Case reference

IC-203321-W1K8

Office 365 – Draft DPIA

Data Protection Impact Assessment – Microsoft Office 365

Document Name	Data Protection Impact Assessment – Microsoft Office 365
Author/Owner (name and job title)	Will McLoughlin – Product Owner, Platforms
Department/Team	Digital & IT, Product and Architecture
Document Status (draft, published or superseded)	Draft
Version Number	V0.1
Release Date	
Approver (if applicable)	
Review Date	
Distribution (internal or external)	Internal

Privacy by design at the ICO

Welcome to our privacy by design process. You should use this every time you want to implement or change a product or process at the ICO. It is essential to managing your own project risks but also to managing the corporate risks of the ICO.

Responsibilities

It is your responsibility to ensure that data protection impact is taken into account during the design and build of your product or service. To do this successfully, you will need to be able to explain what your proposal is, and map out how data is used. This includes, amongst other things, where data might sit at any time geographically, but also the purpose of its use at different points in time.

Remember the basics. Key to a good assessment is knowing at all points in the process: what data you are collecting and why, where it will be stored, for how long will you keep it, who will access it and for what purpose, how it will be kept secure and whether it's being transferred to any other country.

Your Information Asset Owner (your Director) is ultimately responsible for managing any residual risk once you have completed any mitigations to the risks you identify.

The Information Management Service, working on behalf of our DPO, can help complete the paperwork, provide compliance advice and spot risks. It is not the Service's responsibility to own, manage or mitigate the risks identified during the process.

Getting advice

You might also need advice from subject matter experts in other teams to make sure that you understand how something works or risks resulting from what you're proposing to do. This is particularly likely if it involves new, or changing, technologies. Getting this advice will help to provide your IAO with assurance that you have understood and identified the risks.

You might well be working on a contract or agreement and a Security Opinion Report at the same time – these are also ways that you can mitigate risks and should be viewed as part of the overall assessment process.

The paperwork

You should think of this as a live document. You might change your plans or new information might come to light that changes the risk profile of your proposal. If

that’s the case, you should revisit the paperwork and update it to reflect any changes. You might also need to inform your IAO of new or changed risks.

The DPIA process

You should review our internal DPIA Process and allow time for this process in your project plans. Start early! How long it takes will depend on what you’re proposing, and how well you can explain it and identify risks. It can take several weeks to get the right advice and risk assessment in place.

Guidance for completing this template – please read.

You only need to complete this Data Protection Impact Assessment (DPIA) template if you have completed a Screening assessment - do I need to do a DPIA? and this indicates a high risk to data subjects. If you are unsure whether you need to complete a DPIA use the screening assessment first to help you decide.

Aim to complete your DPIA as early as possible as the outcome of the assessment could affect the viability of your plans. In extreme cases, you won't be able to continue with your plans without changing them, or at all.

Guidance notes are included within this template to help you - just **hover your mouse over any blue text** for further information.

The Information Management Service is also available for further advice and support. Please keep in mind our service standards if you require advice.

1. Process/system overview

1.1 Ownership

Project Title:	Product Ownership of Microsoft Office 365
Project Manager:	Will McLoughlin
Information Asset Owner:	Mike Fitzgerald
Controller(s)	ICO & Microsoft
Data processor(s)	Microsoft

ICO as controller and Microsoft as our processor

The ICO is controller and determines the purpose(s) of processing data using Office 365 (O365). ICO has control over what we use O365 for as well as its implementation and configuration in our business.

Our use of the services is governed by the Online Services Terms and Data Protection Addendum, and Microsoft, as a data processor, processes our "Customer Data" (defined below in 1.3) to provide us with their Online Services.

Microsoft as controller for their specific legitimate business operations

In addition Microsoft uses personal data to support a limited set of their own legitimate business operations described by them as:

(1) billing and account management;

(2) compensation (for example, calculating employee commissions and partner incentives);
(3) internal reporting and modelling (for example, forecasting, revenue, capacity planning, product strategy);
(4) combatting fraud, cybercrime, or cyber-attacks that may affect Microsoft or Microsoft Products;
(5) improving the core functionality of accessibility, privacy, or energy efficiency; and
(6) financial reporting and compliance with legal obligations (subject to the limitations on disclosure of Customer Data outlined in the Online Service Terms).

Microsoft is controller of this processing of personal data in order to support these operations and, by using their services we must accept that this processing takes place.

Microsoft states it generally aggregates personal data before using it, removing Microsoft's ability to identify specific individuals, and uses personal data in the least identifiable form that will support their processing. Microsoft further states it will not use Customer Data or information derived from it for profiling or for advertising or similar commercial purposes.

1.2 Describe your new service or process

This DPIA covers the ICO's use of the Microsoft Office 365 suite of applications as provided under our E5 licencing arrangement. It seeks to build and update on the PSIA that was produced in December 2016 when Office 365 was being procured by the ICO. Foundational risks, mitigations, security provisions, and rights considerations that were covered in that PSIA are intentionally not duplicated here.

However, this DPIA does build on and support numerous DPIAs that were produced for individual Office 365 applications, addressing all current Office 365 applications available to colleagues through our MMD and Office on the Web offers, as per the following list (current as of September 30 2022):

Bookings
Calendar
Excel
Forms
Kaizala
Lists
OneDrive
OneNote
Outlook
People
Planner
Power Apps
Power Automate

Power BI
PowerPoint
Project
SharePoint
Stream
Sway
Teams
To Do
Visio
Viva Insights
Whiteboard
Word
Yammer

Whilst all applications are available to ICO staff as part of our E5 licence not all are actively used by the ICO. Further detail about applications currently in use and their current deployment can be found in Appendix 3. This appendix will be updated if our application use changes.

It is recognised that it may still be necessary to create exceptional additional DPIAs for some O365 applications, for example if and where the ICO's intended specific use of that application is significantly at odds with the contents of this DPIA or simply where a more in depth assessment of an application will assist with managing risks. In those cases, this master document will be updated to provide reference to the additional documentation, along with the rationale for its creation.

Some Office 365 products include extensibility options that enable, at the controller's choosing, sharing of data with independent third parties. For example, Exchange Online is an extensible platform that allows third-party add-ins or connectors to integrate with Outlook and extend Outlook's feature sets; the same is true for Teams. These third-party providers of add-ins or connectors act independently of Microsoft, and their add-ins or connectors must be enabled by the users or enterprise administrators, who authenticate with their add-in or connector account.

Such third-party add-ins or connectors are disallowed by default at the ICO, and not automatically covered by this DPIA. Each one required or requested would need to be subject of a DPIA Screening Assessment, on a case-by-case basis.

1.3 Personal data inventory - explain what personal data is involved

Category of data	Data subjects	Recipients	Overseas transfers	Retention period
Customer Data: This is all data, including text, sound, video, or image files and software, that ICO provides to Microsoft through use of Microsoft online services. It includes data uploaded for storage or processing, as well as customizations. Examples of Customer Data processed in Office 365 by the ICO will include, but are not limited to: • Email content in Exchange Online • Documents or files stored in SharePoint Online or OneDrive for Business. • Meetings and conversations • Community and channel posts • Chats • Voicemail • Shared files	ICO Staff and all other data subjects whose data the ICO processes as part of it's day to day operations.	Primarily Microsoft but Microsoft also shares data with third parties acting as their sub processors to support functions such as customer and technical support, service maintenance, and other operations. Microsoft states any subcontractors to which Microsoft transfers Customer Data, Support Data, or Personal Data will have entered into written agreements with Microsoft that are no less protective than the Data Protection Terms of the Online Services Terms agreed between ICO and Microsoft.	As described in their Guidance for Data Controllers using Office 365 - Microsoft GDPR | Microsoft Learn and the Online Services Terms, for instances of Office 365 provisioned in the United Kingdom, Microsoft will store the following Customer Data at rest only within the UK: (1) Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments), (2) SharePoint Online site content and the files stored within that site, (3) files uploaded to OneDrive for Business, and (4) project content uploaded to Project	Data is retained by Microsoft for the duration of our use of the service. As a customer ICO at all times during the term of our subscription will have the ability to access, extract, and delete Customer Data stored in the service, subject in some cases to specific product functionality intended to mitigate the risk of inadvertent deletion (for example, Exchange recovered items folder), as further described in product documentation. Except for free trials and LinkedIn services, Microsoft will retain Customer Data stored in the Online Service

• Recordings and transcriptions. • Profile data such as email address, profile picture and phone number • Call history		All third-party subprocessors with which Customer Data from Microsoft's Core Online Services is shared are included in the Online Services Subcontractor list. All third-party sub processors that may access Support Data (including Customer Data that customers choose to share during their support interactions) are included in the Microsoft Commercial Support Contractors list.	Online. For personal data from the United Kingdom, Microsoft will ensure that transfers of personal data to a third country or an international organization are subject to appropriate safeguards as described in Article 46 of UK GDPR. In addition to Microsoft's commitments under the Standard Contractual Clauses for processors and other model contracts, Microsoft continues to abide by the terms of the Privacy Shield framework. In the UK, as of September 2022, the provisions made for restricted international transfer of data under the Privacy Shield framework are covered under International Data Transfer Agreements (IDTA): International data transfer agreement and guidance | ICO	in a limited function account for 90 days after expiration or termination of the our subscription so that we may extract the data. After the 90-day retention period ends, Microsoft will disable a customer's account and delete the Customer Data. ICO retention periods for our data will vary but information within the O365 environment should be managed by Information Asset Owners as per the ICOs Retention and Disposal Policy.
Service-generated Data: This is data that is generated or derived by	ICO staff	As above	Structural transfer of Diagnostic Data to the USA	This data is retained for a default period of up to 180

Microsoft through operation of the service, such as use or performance data. Most of these data contain pseudonymous identifiers generated by Microsoft.			until December 2022. Microsoft is developing and will apply the EU Data Boundary to all diagnostic data by the end of 2022.(source: EU Data Boundary for the Microsoft Cloud: A progress report - EU Policy Blog)	days from collection, subject to longer retention periods where required for security of the services or to meet legal or regulatory obligations.
Diagnostic Data: This data is collected or obtained by Microsoft from software that is locally installed by Customer in connection with the Online Service and may also be referred to as telemetry. This data is commonly identified by attributes of the locally installed software or the machine that runs that software.	ICO staff	As above	Structural transfer of Diagnostic Data to the USA until December 2022. Microsoft is developing and will apply the EU Data Boundary to all diagnostic data by the end of 2022.	This data is retained for a default period of up to 180 days from collection, subject to longer retention periods where required for security of the services or to meet legal or regulatory obligations.
Support Data/Feedback data Information related to troubleshooting tickets or feedback submission to Microsoft. This is data provided to Microsoft by ICO through an engagement with Microsoft to obtain technical support for Online Services	ICO Staff	As above	Structural transfer of Diagnostic Data to the USA until December 2022. Microsoft is developing and will apply the EU Data Boundary to all diagnostic data by the end of 2022.	This data is retained for a default period of up to 180 days from collection, subject to longer retention periods where required for security of the services or to meet legal or regulatory obligations.

1.4 Identify a lawful basis for your processing

Office 365 is core business technology at the ICO essential for delivering our statutory functions and ICO has invested in Enterprise (E5) licencing for all colleagues. Our lawful basis for using O365 to process personal data is Article 6(e) public task. For the processing of special category data the further basis for processing are Article 9(2)(g) – substantial public interest and DPA 2018 schedule 1 part 1 paragraph 6 – statutory etc and government purposes.

1.5 Explain why it is both necessary and proportionate to process the personal data you've listed in your data inventory

The data processing listed in 1.3 is effectively a set of conditions that enable Microsoft to provide the ICO with the Office 365 service we have chosen. It's necessary for the ICO to use O365 in order to deliver our statutory functions effectively or pursue our legitimate business interests. As detailed in the standard Online Services Terms and Data Protection Addendum, Microsoft also uses Personal Data to support a limited set of their own legitimate business operations as outlined in 1.1 above. They are the controller for this processing and are also required to consider necessity and proportionality themselves, as well as comply more widely with relevant data protection legislation in the jurisdictions in which they operate.

1.6 Outline your approach to completing this DPIA

Throughout the inception and drafting of this DPIA, I have consulted with Steven Johnston, Team Manager, Information Management. I have also been guided and closely advised by Mike Fitzgerald as Information Asset Owner. Since this DPIA is designed to supplement multiple previous DPIAs, and not to cover any specific new usage of data, it is not anticipated that additional consultation of data subjects is required. If such a requirement emerges, that consultation will accordingly be reflected in later updates.

2.0 Personal Data Lifecycle

Guidance: You must provide a systematic description of your processing from the point that personal data is first collected through to its disposal.

You should explain the source of the data, how it is obtained, what technology is used to process it, who has access to it, where it is stored and how and when it is disposed of.

If your plans involve the use of any new technology you should explain how this technology works and outline any 'privacy friendly' features that are available.

You can use the headings provided below to help you construct your lifecycle. Also include a flow diagram if it helps your explanation.

Data source and collection:

Customer data will be collected in a variety of ways by the ICO for processing within O365 applications. Most of the personal data we process is provided directly to us by data subjects. But we also receive personal data indirectly. Further information about how we typically obtain personal data is contained in our customer privacy notice and staff privacy notice.

Some additional categories of personal data are processed as a direct result of our staff using O365 applications. Microsoft systematically collects Telemetry Data about the use of its software. There are three levels at which this data can be set to be collected: Required (Lowest), Enhanced, and Optional (Highest). ICO devices are set to provide **Enhanced** diagnostic data to Microsoft under a known commercial identifier. As part of Microsoft Managed Desktop, IT admins cannot change these settings. As outlined in this DPIA for MMD, the Enhanced setting enables Advanced Threat Protection through use of the diagnostic data collected.

In Office for the Web, the default level is set to the (lowest) level of required data. Microsoft states it has limited the amount of telemetry events to a minimum, and has contractually agreed to never include any Content Data in these events.

In addition, Microsoft collects detailed personal information about the usage of Teams, OneDrive, SharePoint and the Azure Active Directory. Microsoft makes some of these Diagnostic Data available through audit logs and reports for admins.

Personal data related to troubleshooting tickets or feedback submissions to Microsoft is data provided to Microsoft by ICO through an engagement with Microsoft in order to obtain technical support.

Technology used for the processing:

O365 suite of applications as provided under our E5 licencing arrangement (see 1.2 above).

O365 Telemetry Data is collected via a built-in telemetry client built into installed apps on desktops/laptops, on mobile devices and in the browser version of the apps.

O365 Usage Data is collected in log files of Microsoft's cloud servers, in so-called system-generated event logs.

Storage location:

Customer data is typically stored at rest only withing in the UK (See 1.3 above).

Telemetry Data is currently sent regularly, in batches, to Microsoft's servers in the United States. The Diagnostic Data are sent in an undocumented binary format. However this is only the case until December 2022. Microsoft is developing and will apply the EU Data Boundary to all personal data by the end of 2022. Provisions under IDTA for restricted transfer of data apply to EEA and third countries.

Usage Data is hosted in Microsoft's UK and/or EMEA data centres.

Access controls and data sharing:

Access is controlled through Azure Active Directory Single Sign On. This is made available to all ICO colleagues from the moment a New Starter request sent by People Services is processed by IT Help – their Azure Identity is set up and they are allocated to various security groups, which automatically provisions an O365 E5 licence to the user.

Data may be shared with recipients as detailed in 1.3.

Microsoft states it will not disclose Customer Data outside of Microsoft or its controlled subsidiaries and affiliates except (1) as Customer directs, (2) as described in the OST, or (3) as required by law.

Disposal:

Customer Data: Throughout the duration of our contract we are able to dispose of customer data as we see fit by implementing retention and disposal rules within the O365 suite. For Office 365 subscriptions, Microsoft will retain Customer Data stored in the Online Service in a limited function account for 90 days after expiration or termination of the customer's subscription so that the customer may extract the data. After the 90-day retention period ends, Microsoft will disable the customer's account and delete the Customer Data.

Service-generated (Diagnostic/Telemetry) Data: This data is retained for a default period of up to 180 days from collection, subject to longer retention periods where required for security of the services or to meet legal or regulatory obligations.

3.0 Key principles and requirements

Purpose & Transparency

1. Will you need to update our privacy notices?

Yes ☐ No ☒

2. If you are not updating our privacy notices how do you intend to communicate information about your processing to the data subjects?

Microsoft already included in the Staff Privacy Notice. As with a number of other processors there is no clear place in our Global PN to list Microsoft. Where specific applications are used for clearly defined processing activities Microsoft is listed as a processor. For example our use of Microsoft services is referenced in relation to our chatbot, Forms use is referenced for responding to ICO consultations and surveys, website hosting in Azure and use of Teams for delivering webinars and broadcast events.

3. If consent is your lawful basis for processing personal data are you maintaining appropriate records of the data subjects consent?

Yes ☐ No ☐ N/a ☒

4. If legitimate interests is your lawful basis for processing have you completed a legitimate interest assessment?

Yes ☐ No ☐ N/a ☒

If applicable please provide a link to your completed assessment.

Accuracy

5. Are you satisfied the personal data you are processing is accurate?

Yes ☒ No ☐

6. How will you ensure the personal data remains accurate for the duration of your processing?

Customer data can typically be edited by ICO staff if it becomes inaccurate within O365 applications such as Word, Forms, Excel etc. This won't be the case for data such as chats, voicemail and call history which will be an accurate record of events. Similarly service generated data, diagnostic data and support data will be accurate reflections of events and there should be no issues with accuracy

7. If the personal data isn't being obtained directly from the data subject what steps will you take to verify accuracy?

ICO privacy information explains how we get personal data: How do we get information? | ICO

Minimisation, Retention & Deletion

8. Have you done everything you can to minimise the personal data you are processing?

Yes ☒ No ☐

9. How will you ensure the personal data are deleted at the end of the retention period?

Automated retention and disposal is enabled through the O365 Compliance Center. Currently configured for Outlook, Teams, Yammer – currently 12 months on these solutions. Work is ongoing to define and apply retention schedules throughout SharePoint Online.

10. Will you need to update the retention and disposal schedule?

Yes ☐ No ☒

Integrity and confidentiality

11. Where will the personal data be stored?

Office 365, within our Microsoft Azure Tenant, on UK located servers.

12. Are there appropriate access controls to keep the personal data secure?

Yes ☒ No ☐

13. Have you contacted the cyber security team for a security assessment of your plans?

Yes ☒ No ☐ N/a ☐

14. Please explain the policies, training or other instructions you intend to put in place to enable staff to operate the new system or process securely.

Usage policies and how to guides created and maintained for O365; in-house and external training provided for all colleagues.

Accountability

15. Who will be the Information Asset Owner for this personal data?

Mike Fitzgerald, Director of Digital, IT and Business Services

16. Will you need to update our Article 30 record of processing activities?

Yes ☐ No ☒

17. If you are using a data processor have you agreed, or will you be agreeing, a written contract with them?

Yes ☒ No ☐ N/a ☐

Online Services Terms govern ICO use of the Microsoft Office 365 suite.

Individual Rights

Guidance: UK GDPR provides a number of rights to data subjects where their personal data is being processed. As some rights are not absolute and only apply in limited circumstances we may have grounds to refuse a specific request from an individual data subject. However you need to be sure your new service or process can facilitate the exercise of these rights by the data subject i.e. it should be technically feasible for us to action a request if required.

18. Is there a means of providing the data subjects with access to the personal data being processed?

Yes ☒ No ☐

19. Can inaccurate or incomplete personal data be updated on receipt of a request from a data subject?

Yes ☒ No ☐

20. Can we restrict our processing of the personal data on receipt of a request from a data subject?

Yes ☒ No ☐

21. Can we stop our processing of the personal data on receipt of a request from a data subject?

Yes ☒ No ☐ N/a ☐

22. Can we extract and transmit the personal data in a structured, commonly used and machine readable format if requested by the data subject?

Yes ☒ No ☐ N/a ☐

23. Can we erase the personal data on receipt of a request from the data subject?

Yes ☒ No ☐

4.0 Risk assessment

	Risk Description	Response to Risk	Risk Mitigation	Expected Risk Score		
				I	P	Total
				See Appendix 1 – Risk Assessment Criteria		
	Example: *Access controls are not implemented correctly and personal data is accessible to an unauthorised third party.*	*Reduce*	*Existing mitigation: We have checked that the system we intend to procure allows us to set access permissions for different users.* *Expected mitigation: We will appoint and train a system administrator who will be responsible for implementing access controls and monitoring access. The system administrator will also audit the system periodically to review access permissions.*	*3*	*1*	*3 - low*
1.	Excessive personal data shared with Microsoft and third parties as controllers.	Reduce	Existing mitigations: Additional Optional Connected Experiences Disabled. Third Party Apps in Teams Disabled. Usage policies created to guide	3	1	3 - Low
2.	Colleagues overshare personal data on open forums such as Teams, Yammer, SharePoint.	Reduce	Existing mitigations: Training, usage policies, and How-to/etiquette guides produced for all systems to remind staff about appropriate use.	1	1	1 - Low
3.	Personal information is disclosed to unauthorized third-party organization during diagnostic/fault resolution activities.	Reduce	Existing mitigation: Usage data is only accessible via o365 administrators, it is not shared with 3rd party organisations. O365 user feature lockbox is active. Microsoft support engineers requiring	2	1	2 - Low

			access to user data must first submit a lockbox data request. This can only be approved by O365 administrators.			
4.	Personal information is disclosed to unauthorized third-party applications (in e.g. Teams, Outlook, Power BI).	Reduce	Existing Mitigation: Apps policy restricts access to only approved Microsoft applications with known functionality. Expected Mitigation: All new third-party apps will be individually assessed before becoming available to ICO staff.	3	1	3 - Low
5.	Unauthorised disclosure of customer data by Microsoft to a third party	Accept	Existing Mitigations: Agreed Online service terms provide that Microsoft will not disclose Customer Data outside of Microsoft or its controlled subsidiaries and affiliates except (1) as Customer directs, (2) as described in the OST, or (3) as required by law. Microsoft will not disclose Customer Data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for Customer Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose Customer Data to law	4	1	4 - low

			enforcement, Microsoft will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so. Upon receipt of any other third-party request for Customer Data, Microsoft will promptly notify Customer unless prohibited by law. Microsoft will reject the request unless required by law to comply. If the request is valid, Microsoft will attempt to redirect the third party to request the data directly from Customer. Microsoft will not provide any third party: (a) direct, indirect, blanket or unfettered access to Customer Data; (b) platform encryption keys used to secure Customer Data or the ability to break such encryption; or (c) access to Customer Data if Microsoft is aware that the data is to be used for purposes other than those stated in the third party's request. In support of the above, Microsoft may provide Customer's basic contact information to the third party.			
6.	Microsoft security controls are not adequate resulting in a loss of confidentiality,	Accept	Existing Mitigation:	4	1	4- low

	integrity or availability of data.		Agreed Online service terms provide that Microsoft will implement and maintain appropriate technical and organizational measures to protect Customer Data and Personal Data. These measures are set forth in a Microsoft Security Policy. Microsoft make that policy available to ICO as Customer, along with descriptions of the security controls in place for the Online Service and other information reasonably requested by Customer regarding Microsoft security practices and policies. In addition, those measures shall comply with the requirements set forth in ISO 27001, ISO 27002, and ISO 27018. Further detail about Security measures is available in the online service terms.			
7.	ICO unable to communicate details of any personal data breach resulting from our use of O365 to data subjects.	Accept	Existing Mitigation: Agreed Online service terms provide that if Microsoft becomes aware of a breach of security Microsoft will promptly and without undue delay (1) notify ICO of the Security Incident; (2) investigate the Security Incident and provide ICO with detailed information about the Security Incident; (3) take reasonable steps to mitigate the effects and to minimize any	4	1	4 - low

			damage resulting from the Security Incident. Notification(s) of Security Incidents will be delivered to one or more of ICO's administrators Microsoft will make reasonable efforts to assist ICO in fulfilling our obligations under UK GDPR Article 33 and 34 to notify the relevant supervisory authority and data subjects about such Security Incident.			
8.	Data transferred overseas to a country without equivalent data protection laws	Accept	Existing Mitigation: All transfers of Customer Data out of the European Union, European Economic Area, and Switzerland by the Core Online Services shall be governed by the Standard Contractual Clauses/IDTA.	3	1	3 - low
9.	Personal data retained for longer than necessary	Accept	Existing Mitigation At all times during the term of ICO subscription we will have the ability to access, extract and delete Customer Data stored in each Online Service. Except for free trials and LinkedIn services, Microsoft will retain Customer Data that remains stored in Online Services in a limited function account for 90 days after expiration or termination of our subscription so that we may extract	2	3	6 - medium

			the data. After the 90-day retention period ends, Microsoft will disable Customer's account and delete the Customer Data and Personal Data within an additional 90 days. Microsoft retains service generated and diagnostic data for a default period of up to 180 days from collection, subject to longer retention periods where required for security of the services or to meet legal or regulatory obligations. ICO retention periods for our data will vary but information within the O365 environment should be managed by Information Asset Owners as per the ICOs Retention and Disposal Policy.			

5.0 Consult the DPO

Guidance: Once you have completed all of the sections above you should submit your DPIA for consideration by the DPIA Forum who will provide recommendations on behalf of our DPO. The process to follow is here.

Any recommendations from the DPOs team will be documented below and your DPIA will then be returned to you. You must then record your response to each recommendation and proceed with the rest of the template.

	Recommendation	Date and project stage	Project Team Response
1.			
2.			
3.			

6.0 Integrate the DPIA outcomes back into your plans

Guidance: Completing sections 1 to 5 of your DPIA should have helped you identify a number of key actions you now need to take to meet UK GDPR requirements and minimise risks to your data subjects. For example, you may now need to draft a suitable privacy notice for your data subjects; or you could have risk mitigations that you need to go and implement. You should also consider whether any additional actions are required as a result of any recommendations from the DPO.

Use the table below to list the actions you now need to take and to track your progress with implementation. Most actions will typically need to be completed *before* you can start your processing.

Action	Date for completion	Responsibility for Action	Completed Date

7.0 Expected residual risk and sign off by IAO

Guidance: Summarise the expected residual risk below for the benefit of your IAO. This is any remaining risk ***after*** you implement all of your mitigation measures and complete all actions. It is never possible to remove all risk so this section shouldn't be omitted or blank.

Note: If the expected residual risk remains high (i.e. red on the traffic light scoring in the Appendix) then you will need to consult the ICO as the regulator by following the process used by external organisations.

7.1 IAO sign off

Guidance: Your IAO owns the risks associated with your processing and they have final sign off on your plans. You **must** get your IAO to review the expected residual risk and confirm their acceptance of this risk before you proceed.

IAO (name and role)	Date of sign off	Project Stage

8.0 DPIA Change history

Guidance: To be completed by the person responsible for completing the DPIA and delivering the system, service or process.

Version	Date	Author	Change description

V0.1	30/09/2022	Will McLoughlin / Steven Johnston	First Draft

Appendix 1: Risk Assessment Criteria

The following criteria are aligned with our corporate risk assessment criteria.

Impact

Impact is the consequence of a risk to the rights and freedoms of individuals being realised. Factors to consider include the financial harm or emotional distress that can be expected to occur.

Impact	Scoring criteria
Very low (1)	No discernible impact on individuals.
Low (2)	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc).
Medium (3)	Individuals may encounter significant inconveniences, which they will overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc)
High (4)	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc).
Very high (5)	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Probability

Probability is the likelihood of a risk to the rights and freedoms of individuals being realised. Factors to consider include the expected frequency of occurrence, and the motivation and capability of threat sources (eg does the threat require insider knowledge and/or significant technical resources to exploit any vulnerability?).

Probability	Scoring criteria
Very low (1)	0-5% - extremely unlikely or improbable

	For example, the risk has not occurred before or is not expected to occur within the next three years.
Low (2)	6-20% - low but not improbable For example, the risk is expected to occur once a year.
Medium (3)	21-50% - fairly likely to occur For example, the risk is expected to occur several times a year.
High (4)	51-80% - more likely to occur than not For example, the risk is expected to occur once a month.
Very high (5)	81-100% - almost certainly will occur For example, the risk is expected to occur once a week.

Risk level

Risk level is a function of impact and probability, and is represented by a RAG rating.

Probability / Impact	Very low (1)	Low (2)	Medium (3)	High (4)	Very high (5)
Very high (5)	Amber (5)	Amber (10)	Red (15)	Red (20)	Red (25)
High (4)	Green (4)	Amber (8)	Amber (12)	Red (16)	Red (20)
Medium (3)	Green (3)	Amber (6)	Amber (9)	Amber (12)	Red (15)
Low (2)	Green (2)	Green (4)	Amber (6)	Amber (8)	Amber (10)
Very low (1)	Green (1)	Green (2)	Green (3)	Green (4)	Amber (5)

Risk acceptance criteria

These criteria are guidelines only, and any risk treatment decisions should be made on a case-by-case basis. For example, it may be prudent to reduce a low risk because of legal and regulatory requirements.

Risk level	Acceptance criteria
Low (Green)	Within this range risks can be routinely accepted.
Medium (Amber)	Within this range risks can occasionally be accepted but shall be kept under regular review.

High (Red)	Within this range risks shall not be accepted and immediate action is required to reduce, avoid or transfer the risk.

Appendix 2: example risks to data subjects

Guidance: The following are examples of common risks associated with the processing of personal data to assist with your risk assessment. Not all of them will apply to your processing and the list is not exhaustive – you should consider specific risks that are relevant to your plans.

- Data is processed for unspecified / unlawful purposes/ not within expectations of data subjects
- Excessive data is processed
- Data is not kept up to date
- Data is kept for longer than is necessary by us
- Data is kept for longer than is necessary by data processor
- Data processed in contravention of data subject rights
- Data subjects unable to exercise their rights
- Data stolen or modified in transit
- Data stolen or modified at rest in our premises
- Data stolen or modified at rest in data processor premises
- Data transferred overseas to a jurisdiction that does not adequately protect data subject rights
- Re-identification of pseudonymised data by data processor or third party
- Unauthorised destruction or loss of data
- Data processor network / system / online portal not secure
- Data processor fails to process data in accordance with our instructions
- Personal data of children processed without appropriate safeguards / parental authority
- Consent of data subject not freely given (for example employer / employee processing)
- The data subject is particularly vulnerable (elderly or disabled) or is there a potential imbalance of power between the individual and the controller (employee/employer)
- Source of data poses risks re accuracy (obtained from a unverified or old list)
- Risk to accuracy of data due to matching / combining data from different sources
- Use of new technology, e.g. fingerprinting, face recognition
- Monitoring or recording individuals
- Using profiling according to characteristics or behavior
- Non-compliance with DP principles

Appendix 3

Whilst all O365 applications are technically available to ICO staff as part of our E5 licence some aren't actively being used. The table below summarises our current use of the O365 applications suite along with any specific steps taken to implement each application in a privacy friendly way.

When considering the deployment of a particular application consideration will always be given to deploying in the most privacy friendly way that still allows us to achieve our purpose and the table below will be updated.

Where the ICO's intended use of an application is significantly at odds with the contents of this DPIA or simply where a more in depth assessment of an application will assist with managing risks this will be completed.

Applications	**Currently actively used by ICO staff Y/N**	**Any additional DPIA or similar risk assessments**	**Notes on deployment of any privacy friendly features**
Bookings	N	N	N/A
Calendar	Y	N	Calendars and individual appointments can be set to Private by all users.
Excel	Y	N	
Forms	Y	N	
Kaizala	N	N	N/A
Lists	Y	N	

OneDrive	Y	0097 - Core cloud - One Drive - DPIA.docx	
OneNote	Y	N	
Outlook	Y	N	
People	Y	N	
Planner	Y	N	
Power Apps	Y	N	Individual apps should be subject to DPIA Screening as a minimum.
Power Automate	Y	N	Only Standard 365 Connectors enabled for all users. Third Party connectors would need to be fully assessed on their individual merits.
Power BI	Y	N	Governance and request process around access to: Desktop version; Workspaces; Datasets; ability to Publish to Web. Tight restrictions on external sharing, direct queries, export of data to csv/xls. No third party apps or use of APIs by default.
PowerPoint	Y	N	
Project	Y	N	
SharePoint	Y	Intranet Upgrade Data Protection Impact	Group based permissions management, retention labelling.

		Assessment v0.2.docx	
Stream	Y	Teams Live Events and Stream - DPIA.DOCX	Ability to use recording functionality, live events and Stream controlled by IT and limited to preapproved members of staff on request.
Sway	Y	N	
Teams	Y	Team main DPIA 30-09-2020.docx	Teams apps policy restricts access to only approved Microsoft applications with known functionality. All new apps in Teams are first fully assessed before becoming available to ICO staff.
To Do	Y	N	
Visio	Y	N	
Viva Insights	Y	N	Only individuals can view personal data and insights based on work patterns in their emails, meetings, calls, and chats. Individual employees choose the insights and experiences they want to receive. Item insights and people insights disabled at tenant level via Powershell.
Whiteboard	Y	N	
Word	Y	N	

Case reference

IC-203321-W1K8

Convene in Teams – Draft DPIA

Data Protection Impact Assessment – Convene in Teams

Document Name	Data Protection Impact Assessment – Convene in Teams
Author/Owner (name and job title)	Aimee Smith (Assurance and Corporate Compliance Manager)
Department/Team	COO/Corporate Governance
Document Status (draft, published or superseded)	Draft
Version Number	V0.1
Release Date	
Approver (if applicable)	
Review Date	
Distribution (internal or external)	Internal

Privacy by design at the ICO

Welcome to our privacy by design process. You should use this every time you want to implement or change a product or process at the ICO. It is essential to managing your own project risks but also to managing the corporate risks of the ICO.

Responsibilities

It is your responsibility to ensure that data protection impact is taken into account during the design and build of your product or service. To do this successfully, you will need to be able to explain what your proposal is, and map out how data is used. This includes, amongst other things, where data might sit at any time geographically, but also the purpose of its use at different points in time.

Remember the basics. Key to a good assessment is knowing at all points in the process: what data you are collecting and why, where it will be stored, for how long will you keep it, who will access it and for what purpose, how it will be kept secure and whether it's being transferred to any other country.

Your Information Asset Owner (your Director) is ultimately responsible for managing any residual risk once you have completed any mitigations to the risks you identify.

The Information Management Service, working on behalf of our DPO, can help complete the paperwork, provide compliance advice and spot risks. It is not the Service's responsibility to own, manage or mitigate the risks identified during the process.

Getting advice

You might also need advice from subject matter experts in other teams to make sure that you understand how something works or risks resulting from what you're proposing to do. This is particularly likely if it involves new, or changing, technologies. Getting this advice will help to provide your IAO with assurance that you have understood and identified the risks.

You might well be working on a contract or agreement and a Security Opinion Report at the same time – these are also ways that you can mitigate risks and should be viewed as part of the overall assessment process.

The paperwork

You should think of this as a live document. You might change your plans or new information might come to light that changes the risk profile of your proposal. If that's the case, you should revisit the paperwork and update it to reflect any changes. You might also need to inform your IAO of new or changed risks.

The DPIA process

You should review our internal DPIA Process and allow time for this process in your project plans. Start early! How long it takes will depend on what you're proposing, and how well you can explain it and identify risks. It can take several weeks to get the right advice and risk assessment in place.

Guidance for completing this template – please read.

You only need to complete this Data Protection Impact Assessment (DPIA) template if you have completed a Screening assessment - do I need to do a DPIA? and this indicates a high risk to data subjects. If you are unsure whether you need to complete a DPIA use the screening assessment first to help you decide.

Aim to complete your DPIA as early as possible as the outcome of the assessment could affect the viability of your plans. In extreme cases, you won't be able to continue with your plans without changing them, or at all.

Guidance notes are included within this template to help you - just **hover your mouse over any blue text** for further information.

The Information Management Service is also available for further advice and support. Please keep in mind our service standards if you require advice.

1. Process/system overview

1.1 Ownership

Project Title:	Convene for Teams
Project Manager:	Laura Bendall
Information Asset Owner:	Louise Byers, Director of Corporate Planning, Risk and Governance
Controller(s)	ICO and Azeus Convene
Data processor(s)	Azeus Convene

1.2 Describe your new service or process

Convene is an add-on to Team which will improve meeting, particularly Board meeting, functionality.

The current process of providing a secretariat service to SLT and ET Boards and working groups involves the creation and maintenance of a number of different documents (agendas, action boards etc.). These are currently stored on SP EDRM and sent out via email to Board attendees. These documents can change frequently which means multiple email to Board members, which risks members referring to outdated information.

Convene is an app that operates within Teams. Instead of emailing documents to members, the secretariat would upload the agenda and other documents to Convene, which all members would have access to. Members would be able to upload reports they are presenting/discussing in the meeting to Convene. If any documents needed to be changed, all members would be able to access

the most recent version of the document. Accessing and presenting documents during meetings would be more streamlined.

Convene, provided by Azeus, can also provide voting functions, accommodate the review and sign-off of draft minutes and allows for announcements to be made to Board members, which would reduce email volume and ensure all essential messaging is in one place. This will enhance the secretariat offer to Boards and allow for more efficient, streamlined governance.

It is envisioned that around 3 members of staff will have administrative access to Convene, who will be the Corporate Governance Officer, Corporate Governance Manager and Corporate Governance and Secretariat Group Manager. All Board members (all SLT and ET) and those that provide support (Corporate Governance, POC, Private Secretaries, Executive Assistants and Directors Admin)

Convene are a data controller when setting up accounts and providing customer support to ICO staff. Convene are a data processor when storing and providing access to information that ICO staff upload to it, in this case the ICO will be the data controller.

The information processed within Convene is already processed by the ICO. This DPIA solely considers the processing that takes place in Convene, both when Convene is a data controller and a data processor.

1.3 Personal data inventory - explain what personal data is involved

Category of data	Data subjects	Recipients	Overseas transfers	Retention period
ICO to Convene as data controller				
Basic personal identifiers (name, username, job title, company name) Contact details (email address, phone number)	ICO Staff	Azeus Convene	Yes Data stored in Singapore. Data accessed (for customer support) in Philippines.	30 days from subscription end or account deletion (for ICO leavers.) Deleted via cryptoshredding.
Device information (username, IP address, device ID)	ICO Staff	Azeus Convene	Yes Data stored in Singapore. Data accessed (for customer support) in Philippines.	30 days from subscription end or account deletion (for ICO leavers.) Deleted via cryptoshredding.
ICO to Convene as a data processor				
Basic personal identifiers (name, job title, signature)	ICO Staff	Azeus Convene	No	30 days from ICO deletion. ICO internal procedures will require information to be deleted from Convene no more than 2 working days after the date of the meeting. Deleted via cryptoshredding.

1.4 Identify a lawful basis for your processing

Public task – Convene will be used for facilitating reporting for SLT Boards. We currently do this already, but are now intending to use Convene in order to streamline the process.

1.5 Explain why it is both necessary and proportionate to process the personal data you've listed in your data inventory

The information being processed by the ICO, and Convene as the processor, is limited to what is necessary in form of contact details and reports. Users cannot access Convene if they do not have an account, which requires the basic details for set up. Reports that are provided to a Board, and Convene as the processor, will contain the name and potentially job title of the author, consultees and approver of the report. Reports seldom contain personal data beyond this and will usually contain anonymised MI data.

1.6 Outline your approach to completing this DPIA

We have conducted a trial session with Convene to understand the use of the software but to also understand how information is processed. Staff that will use Convene took part in the trial and have had the opportunity to consult on it's effectiveness and use of personal information. We have reviewed Convene's privacy information, which provides information about purpose limitation, data collection and international transfers. We have also asked them further questions about retention and storage where we required greater detail.

2.0 Personal Data Lifecycle

Guidance: You must provide a systematic description of your processing from the point that personal data is first collected through to its disposal.

You should explain the source of the data, how it is obtained, what technology is used to process it, who has access to it, where it is stored and how and when it is disposed of.

If your plans involve the use of any new technology you should explain how this technology works and outline any 'privacy friendly' features that are available.

You can use the headings provided below to help you construct your lifecycle. Also include a flow diagram if it helps your explanation.

Data source and collection:
When Convene is the controller and processor, personal information about staff is provided to Convene by the ICO.

Technology used for the processing:
MS Teams and Convene

Storage location:
Convene as a controller: Singapore
Convene as a processor: UK

Access controls and data sharing:
Convene as a controller: Convene are the controller when setting up user accounts and providing customer support. Convene have confirmed they do not share information obtained for this purpose with any third parties.

Convene as a processor: Only ICO staff who have access to Convene will be able to access the papers (and any personal information held within them).

Disposal:

Convene dispose of the information, which is only held electronically, via cryptoshredding.

3.0 Key principles and requirements

Purpose & Transparency

1. Will you need to update our privacy notices?

Yes ☒ No ☐

2. If you are not updating our privacy notices how do you intend to communicate information about your processing to the data subjects?

3. If consent is your lawful basis for processing personal data are you maintaining appropriate records of the data subjects consent?

Yes ☐ No ☐ N/a ☒

4. If legitimate interests is your lawful basis for processing have you completed a legitimate interest assessment?

Yes ☐ No ☐ N/a ☒

If applicable please provide a link to your completed assessment.

Accuracy

5. Are you satisfied the personal data you are processing is accurate?

Yes ☒ No ☐

6. How will you ensure the personal data remains accurate for the duration of your processing?

The information that could change would be limited to name. If a name were to change the system would be automatically updated as per usual process.

7. If the personal data isn't being obtained directly from the data subject what steps will you take to verify accuracy?

n/a

Minimisation, Retention & Deletion

8. Have you done everything you can to minimise the personal data you are processing?

Yes ☒ No ☐

9. How will you ensure the personal data are deleted at the end of the retention period?

Convene as a controller: Convene delete the information 30 days from when the ICOs subscription/contract with Convene ends. Convene have confirmed this is the case. Convene as a processor: When the ICO delete information from Convene, the data held in Convene is marked for deletion and then retained for 30 days to facilitate individual rights. We could conduct compliance checks on Convene to ensure deletion, should the risk warrant it.

10. Will you need to update the retention and disposal schedule?

Yes ☐ No ☒

Integrity and confidentiality

11. Where will the personal data be stored?

Convene

12. Are there appropriate access controls to keep the personal data secure?

Yes ☒ No ☐

13. Have you contacted the cyber security team for a security assessment of your plans?

Yes ☒ No ☐ N/a ☐

14. Please explain the policies, training or other instructions you intend to put in place to enable staff to operate the new system or process securely.

Staff responsible for preparing papers will be given training on how to operate the system, there will be no additional training in relation to data handling as it is minimal and staff do this already on a regular basis. Although Convene staff can access the information uploaded to it, they would only to do to provide technical support at our request.

Accountability

15. Who will be the Information Asset Owner for this personal data?

Louise Byers, Director of Corporate Planning, Risk and Governance

16. Will you need to update our Article 30 record of processing activities?

Yes ☒ No ☐

17. If you are using a data processor have you agreed, or will you be agreeing, a written contract with them?

Yes ☒ No ☐ N/a ☐

Individual Rights

Guidance: UK GDPR provides a number of rights to data subjects where their personal data is being processed. As some rights are not absolute and only apply in limited circumstances we may have grounds to refuse a specific request from an individual data subject. However you need to be sure your new service or process can facilitate the exercise of these rights by the data subject i.e. it should be technically feasible for us to action a request if required.

18. Is there a means of providing the data subjects with access to the personal data being processed?

Yes ☒ No ☐

19. Can inaccurate or incomplete personal data be updated on receipt of a request from a data subject?

Yes ☒ No ☐

20. Can we restrict our processing of the personal data on receipt of a request from a data subject?

Yes ☒ No ☐

21. Can we stop our processing of the personal data on receipt of a request from a data subject?

Yes ☒ No ☐ N/a ☐

22. Can we extract and transmit the personal data in a structured, commonly used and machine readable format if requested by the data subject?

Yes ☐ No ☐ N/a ☒

23. Can we erase the personal data on receipt of a request from the data subject?

Yes ☒ No ☐

4.0 Risk assessment						
Risk Description		**Response to Risk**	**Risk Mitigation**	**Expected Risk Score**		
				I	**P**	**Total**
				See Appendix 1 – Risk Assessment Criteria		
Example: *Access controls are not implemented correctly and personal data is accessible to an unauthorised third party.*		*Reduce*	*Existing mitigation: We have checked that the system we intend to procure allows us to set access permissions for different users.* *Expected mitigation: We will appoint and train a system administrator who will be responsible for implementing access controls and monitoring access. The system administrator will also audit the system periodically to review access permissions.*	*3*	*1*	*3 - low*
1.	Personal information of ICO staff is transferred to third countries (Singapore and the Philippines) and does not receive the same level of protection	Reduce	Existing mitigation: Singapore and the Philippines do not have a finding of adequacy. This transfer will be restricted. We will establish an IDTA to provide appropriate safeguards. The personal information that will be send to Singapore and the Philippines is limited to basic personal identifiers and (work) contact details.	2	2	4 – very low
2.	Access controls implemented by Convene are not implemented correctly and	Reduce	Existing mitigation: We have received assurance from Convene that although they can access the information we upload	4	1	4 – very low

	sensitive corporate information is accessible to Convene staff, or a third party.		to Convene, they do not access it as a practice. It is intended that the information would only be accessed to provide technical support on the instruction of ICO staff. Expected mitigation: Staff responsible for managing documents on Convene to ensure that Board meeting documents are removed from Convene (and stored in SP EDRM) no more than one working day after the meeting. This will minimise the amount of information held in Convene, and time it is held for.			
3.	As Convene store ICO data for 30 days after the ICO delete/remove it from Convene, personal information may be kept for longer than is necessary, outside of retention periods.	Reduce	Existing mitigation: The personal data held by Convene is limited to basic personal identifiers and work contact details. The right to erasure does not apply as this information is processed for the performance of a task carried out in the public interest. The ICO has a retention and disposal policy which provides for the deletion of this information. Expected mitigation: Information uploaded to Convene for the purpose of creating board packs only contains basic person identifiers, this information will be removed from Convene when no longer required, no later than 3 working days after the date of the	1	1	2 – very low

			meeting. This will ensure adherence to the retention schedule. Information provided by staff to Convene for the purpose of account creation and support will be instructed to be deleted when the staff member no longer requires access to Convene. This will be written into guidance for the administrators of Convene (Corporate Governance). This will ensure adherence to the retention schedule.			
4.						
5.						

5.0 Consult the DPO

Guidance: Once you have completed all of the sections above you should submit your DPIA for consideration by the DPIA Forum who will provide recommendations on behalf of our DPO. The process to follow is here.

Any recommendations from the DPOs team will be documented below and your DPIA will then be returned to you. You must then record your response to each recommendation and proceed with the rest of the template.

	Recommendation	**Date and project stage**	**Project Team Response**
1.	DPIA section/s: **1.1, 1.3 and 4.0** Recommendation: The Privacy Policy and GDPR Overview | Azeus Convene indicates Convene may only be a data processor for the data stored in 'content' which we understand to be the documents the ICO uploads to convene. Personal data about ICO staff is being processed for the purpose of setting up accounts to provide access to the service and for customer support. It is likely Convene are a controller for such data processing rather than the ICO. Similarly their privacy policy also indicates for UK customers 'content' only will be stored in the UK and	10/11/2022 – project design	Clarification sought from Convene about location of processing: Convene response: "Setting up of new accounts (actually new Convene environments to be precise) and Customer Support (i.e. our Convene helpdesk) are handled by our Philippines office, and such information is mainly stored in an internal system Jira which is only accessible by the teams responsible for the said duties. Our Jira is hosted in Amazon Web Services (AWS) in Singapore. If they are sent by users to our helpdesk via emails, they are stored securely in our email system which is provided by Microsoft Office 365 and hosted in Asia Pacific by Microsoft**"** Updated DPIA sections 1.1, 1.2, 1.3 and 4.0.

	states "we may store and process personal information and content in the United States and other countries or cities which include but are not limited to the United Kingdom (UK), Australia, Hong Kong, Singapore and Philippines." Whilst it may be possible for us to specify ICO content remains within the UK as part of contracting the above indicates there may be a need for ICO to authorise the international transfer of ICO staff data in order to provide access to the services and deliver customer support. Any international transfer of data is a risk requiring mitigation via an appropriate safeguard as the countries mentioned above are not currently covered by adequacy regulations. Suggested action: Contact Convene for clarification on any international transfers and update DPIA accordingly.		
2.	DPIA section/s: **1.2** Recommendation: The description of the service is very limited and more detail should be provided about what Convene is as a product and what it's intended use is at the ICO. For	10/11/2022 – project design	Updated to provide more detail about Convene and how the ICO will use it.

	example consider what features of Convene will be used to improve board meeting functionality? How many ICO users do you anticipate will need Convene accounts? Who will be the administrator of the solution? Suggested action: Provide further detail about planned processing so IAO is aware of what is involved.		
3.	DPIA section/s: **1.3 and 4.0** Recommendation: The Privacy Policy and GDPR Overview | Azeus Convene indicates there are additional recipients of ICO staff personal data: • "We may provide your personal information to companies that provide services to help us with our business activities such as offering customer service" • certain information concerning use of your individual account may become accessible to that organization's administrator Suggested action: Clarify recipients with Convene, update data inventory and consider any risks in your risk assessment so the IAO is aware of these recipients.	10/11/2022 – project design	Clarification sought from Convene about data sharing: Convene response: "We confirm that no third party organizations will be in receipt of the information the ICO provides to us about its staff or the content it uploads to Convene." Updated 1.3 and 4.0 to confirm no further recipients.

4.	DPIA section/s: **1.3 and 4.0** Recommendation: The Privacy Policy and GDPR Overview | Azeus Convene and Convene product descriptions indicate there may be additional categories of personal data processed through use of the services which are not detailed in the data inventory: • When you use our Services, we collect data to make the Services work better for you. This can include, for example, usage of the features and modules, and data about the performance of the Services. We may also collect data including log information and the devices you use to access the Services, to optimize and remedy your technical concern related to the use of the Services It was further queried whether ICO staff signatures would be processed	22/11/2022 – project design	**Sought additional clarification from Convene:** "We may collect data about usage of different features and modules of Convene by customers. But such data is collected and analysed in aggregate and does not include any personal information and has no linkage to any individual end users. In providing our 24/7 Support, some support requests may require us to get log information relevant to the specific problem reported in order to troubleshoot and fix the issue. The log information may include very limited personal information which is usually the username, IP address and device ID of the end users concerned. The username can be linked back to the user but it is strictly and exclusively used for support purposes only. IP address and device ID are specific to the end user but they do not include personally identifiable information. We may also collect the device ID used by end users to understand for example the models or versions in order to optimize the services, and/or to troubleshoot a reported problem. Again, such data is specific to an end user but the data itself does not include personally identifiable data." Aggregate data, not PD, is collected for this processing. Limited information is collected for the provision of support – updated DPIA.

	for document sign off as this was noted as a feature of Convene. Suggested action: Update DPIA to include additional data processing and consider any risks so IAO is aware.		
5.	DPIA section/s: 1.2, 1.3, 2.0 and 3.0 Recommendation: There are references throughout to Sharepoint EDRM being a storage location and some indication that you're attempting to consider EDRM content as part of this DPIA. We'd recommend you clarify your scope in 1.2 as being processing within the Convene application as this is the new processing being proposed. Your focus can then exclusively be on what data is processed as a result of ICO using Convene and you will be better able to consider things like overseas transfers, retention and disposal, access controls and risk for the Convene application. Suggested action: Clearly define the scope of this DPIA and remove irrelevant content.	10/11/2022 – project design	Clarified and updated 1.2, 1.3, 2.0 and 3.0
6.	DPIA section/s: 4.0	10/10/22 – project design	Updated 4.0 in line with recommendations

	Recommendation: This statement in your risk assessment should be removed and a more thorough risk assessment should be carried out: *"Note – there is very little, if any, inherent risk in the processing of personal data in this processing activity. The risk is related to the management of our corporate information and for transparency have been documented below."* There is always some risk associated with any personal data processing and the purpose of your risk assessment is to assess how significant this is. It's never possible to completely eliminate all risk, but it is usually possible to mitigate risks to an acceptable level. Suggested action: Delete statement and consider as part of your risk assessment the following risks as a minimum • Any risk of personal data transfer to the USA, Australia, Hong Kong, Singapore and Philippines. • External Stakeholder access if they are meeting attendees as indicated in 1.3.		

	• Data sharing with third parties by Convene as described in their privacy notice (see recommendation 3 above) • Data being kept for longer than necessary • Integrity, confidentiality or availability of data being compromised as a result of inadequate security controls		
7.	DPIA section/s: **3.0 Q21** Recommendation: It was queried why your response to this question is N/A. Please reconsider your response as we should be able to stop processing if required. Suggested action: reconsider response to key requirement. If there is any issue with being unable to stop processing this should be added as a risk to your risk assessment.	10/11/2022 – project design	Updated to Yes, apologies this must have been a typo.

6.0 Integrate the DPIA outcomes back into your plans

Guidance: Completing sections 1 to 5 of your DPIA should have helped you identify a number of key actions you now need to take to meet UK GDPR requirements and minimise risks to your data subjects. For example, you may now need to draft a suitable privacy notice for your data subjects; or you could have risk mitigations that you need to go and implement. You should also consider whether any additional actions are required as a result of any recommendations from the DPO.

Use the table below to list the actions you now need to take and to track your progress with implementation. Most actions will typically need to be completed *before* you can start your processing.

Action	Date for completion	Responsibility for Action	Completed Date
Update Privacy Notice		AS / IM Service	
Implement Access Controls		AS / Convene Admin	
Update ROPA		AS / IM Service	

7.0 Expected residual risk and sign off by IAO

Guidance: Summarise the expected residual risk below for the benefit of your IAO. This is any remaining risk ***after*** you implement all of your mitigation measures and complete all actions. It is never possible to remove all risk so this section shouldn't be omitted or blank.

Note: If the expected residual risk remains high (i.e. red on the traffic light scoring in the Appendix) then you will need to consult the ICO as the regulator by following the process used by external organisations.

RE_ Convene DPIA - IAO comments.msg

7.1 IAO sign off

Guidance: Your IAO owns the risks associated with your processing and they have final sign off on your plans. You **must** get your IAO to review the expected residual risk and confirm their acceptance of this risk before you proceed.

IAO (name and role)	Date of sign off	Project Stage
Louise Byers, Director of Corporate Planning, Risk and Governance	22/11/2022	Planning

8.0 DPIA Change history

Guidance: To be completed by the person responsible for completing the DPIA and delivering the system, service or process.

Version	Date	Author	Change description
V0.1	6/10/22	Aimee Smith	First Draft
V0.1	26/10/22	Steven Johnston	DPIA forum recommendations added to 5.0.
V0.2	10/11/22	Aimee Smith	Final amendments made as a result of DPIA Forum recommendations prior to IAO review and sign-off.

Appendix 1: Risk Assessment Criteria

The following criteria are aligned with our corporate risk assessment criteria.

Impact

Impact is the consequence of a risk to the rights and freedoms of individuals being realised. Factors to consider include the financial harm or emotional distress that can be expected to occur.

Impact	Scoring criteria
Very low (1)	No discernible impact on individuals.
Low (2)	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc).
Medium (3)	Individuals may encounter significant inconveniences, which they will overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc)
High (4)	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc).
Very high (5)	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Probability

Probability is the likelihood of a risk to the rights and freedoms of individuals being realised. Factors to consider include the expected frequency of occurrence, and the motivation and capability of threat sources (eg does the threat require

insider knowledge and/or significant technical resources to exploit any vulnerability?).

Probability	Scoring criteria
Very low (1)	0-5% - extremely unlikely or improbable For example, the risk has not occurred before or is not expected to occur within the next three years.
Low (2)	6-20% - low but not improbable For example, the risk is expected to occur once a year.
Medium (3)	21-50% - fairly likely to occur For example, the risk is expected to occur several times a year.
High (4)	51-80% - more likely to occur than not For example, the risk is expected to occur once a month.
Very high (5)	81-100% - almost certainly will occur For example, the risk is expected to occur once a week.

Risk level
Risk level is a function of impact and probability, and is represented by a RAG rating.

Probability / Impact	Very low (1)	Low (2)	Medium (3)	High (4)	Very high (5)
Very high (5)	Amber (5)	Amber (10)	Red (15)	Red (20)	Red (25)
High (4)	Green (4)	Amber (8)	Amber (12)	Red (16)	Red (20)
Medium (3)	Green (3)	Amber (6)	Amber (9)	Amber (12)	Red (15)
Low (2)	Green (2)	Green (4)	Amber (6)	Amber (8)	Amber (10)
Very low (1)	Green (1)	Green (2)	Green (3)	Green (4)	Amber (5)

Risk acceptance criteria
These criteria are guidelines only, and any risk treatment decisions should be made on a case-by-case basis. For example, it may be prudent to reduce a low risk because of legal and regulatory requirements.

Risk level	Acceptance criteria

Low (Green)	Within this range risks can be routinely accepted.
Medium (Amber)	Within this range risks can occasionally be accepted but shall be kept under regular review.
High (Red)	Within this range risks shall not be accepted and immediate action is required to reduce, avoid or transfer the risk.

Appendix 2: example risks to data subjects

Guidance: The following are examples of common risks associated with the processing of personal data to assist with your risk assessment. Not all of them will apply to your processing and the list is not exhaustive – you should consider specific risks that are relevant to your plans.

- Data is processed for unspecified / unlawful purposes/ not within expectations of data subjects
- Excessive data is processed
- Data is not kept up to date
- Data is kept for longer than is necessary by us
- Data is kept for longer than is necessary by data processor
- Data processed in contravention of data subject rights
- Data subjects unable to exercise their rights
- Data stolen or modified in transit
- Data stolen or modified at rest in our premises
- Data stolen or modified at rest in data processor premises
- Data transferred overseas to a jurisdiction that does not adequately protect data subject rights
- Re-identification of pseudonymised data by data processor or third party
- Unauthorised destruction or loss of data
- Data processor network / system / online portal not secure
- Data processor fails to process data in accordance with our instructions
- Personal data of children processed without appropriate safeguards / parental authority
- Consent of data subject not freely given (for example employer / employee processing)
- The data subject is particularly vulnerable (elderly or disabled) or is there a potential imbalance of power between the individual and the controller (employee/employer)
- Source of data poses risks re accuracy (obtained from a unverified or old list)

- Risk to accuracy of data due to matching / combining data from different sources
- Use of new technology, e.g. fingerprinting, face recognition
- Monitoring or recording individuals
- Using profiling according to characteristics or behavior
- Non-compliance with DP principles

9.0 Template Change History (for Information Management Service only)

Version	Date	Author	Change description
v0.1	01/06/2020	Steven Johnston	First draft
v1.0	07/10/2020	Steven Johnston	First release
v1.1	07/01/2021	Iman Elmehdawy	Amendment to guidance note page 2.
v1.2	18/03/2021	Helen Ward	Addition of Privacy by design at the ICO (pages 2 and 3)
v1.3	24/06/2021	Steven Johnston	Section 3.0 Q13 amended. Removed request for link to security assessment.
v2.0	07/03/2022	Steven Johnston	Full document review. Simplified privacy by design explanation on page 3 and made minor format changes throughout. Guidance note for 2.0 was updated and flow headings inserted to the text box. Next review date set to 31/1/2023.
V2.1	11/05/2022	Ben Cudbertson	Amended title of section 2 from 'data flows' to 'personal data lifecycle'

Case reference

IC-203321-W1K8

Core Cloud Services – Document Storage - DPIA

ico.
Information Commissioner's Office

Data Protection Impact Assessment (DPIA) template

You should complete this template where there is a new (or significant change to an existing) service or process that involves the storage/processing of personal data (whether digital or hardcopy). When dealing with an existing process, service or system **only the change should be impact assessed.**

The DPO's team is available to assist and advise on completing this template.

The template should be submitted to the DPSIA Committee for their recommendations and approval.

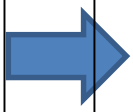
You should start to complete the template as soon as you decide to implement a new system or process. How frequently the DPIA is reviewed and the governance required will vary with the risk of the system or process. At a **minimum**:

Projects: you should produce an initial DPIA prior to finalising your requirements, complete it before finalising your design and review & update the DPIA at least once more prior to go-live. In an Agile project, you should update the DPIA in each sprint. Each update should be submitted to the DPSIA Committee.

Non-projects: you should complete the DPIA prior to designing the service or seeking suppliers and update it whenever there are material changes to the planned system or process.

Screening: Determine what to complete:

1. **GDPR DPIA**: Complete all sections if you meet 2+ questions in section 2.1
2. **Full DPIA**: Complete everything but section 6.2 if you meet 2+ screening questions in any section
3. **Compliance Checklist**: Complete sections 1, 2 and 4, plus signoff, if you don't meet the screening questions



Approval: Consult the DPO's team and select an option for the approvers based on your risk:

1. **DPSIA Committee**: including Senior Information Risk Officer, Head of Cyber Security, DPO
2. **DPSIA Committee**: including DPO and Head of Cyber Security
3. Representatives of DPO and Cyber Security, who will also send it to the DPSIA Committee for their information

Regardless of the option chosen, **the DPIA should be submitted together with your SIA**.

1. Process / System Overview

1.1 Summary

For projects please provide the following key details. Non-projects should provide a key contact who is responsible for delivering the system or process.

Project ID:	0097
Project Title:	Core Cloud Services – Document Storage
Project Manager:	Ray Wong

1.2 Synopsis

In January 2017 a PSIA was agreed covering the migration of services, currently provided within ICO's core network, to an externally hosted service, Office 365. The PSIA covered its underlying technologies, baseline functionality and secure connectivity to the ICO core network.

This DPIA covers the implementation of one of the core capabilities within Office 365; Document Storage. It will consider the additional privacy considerations that arise from the use of Office 365 for storage of ICO documents classified at official (inc. official sensitive).

Document storage offerings within Office 365, such as Sharepoint or OneDrive, have the same underlying technology, security and usage characteristics and are therefore considered together.

1.3 Legitimate Interest

There is a business need for secure, robust and accessible storage of ICO documents. Currently, this is provided primarily using various on-premise network shares or document management systems.

In order to progress the ICO strategy in support of a growing organisation and flexible ways of working a more scalable & flexible solution is required, however, the scope of any legitimate interests around document storage are unchanged.

1.4 Lawful Basis

Under GDPR article 6 we believe that section f) legitimate interests applies. It is in the legitimate interest of ICO staff that we allow access to ICO documents, as it is in line with people's reasonable expectations and wouldn't have an unwarranted impact on them.

1.5 Mandatory Requirements

The following requirements will be added to the backlog for any project implementing document storage in Office 365.

Data Accuracy

a) There must be a means to update inaccurate or incomplete personal data

Retention & Deletion

b) All data collected will have a retention period in line with ICO policies
c) Data must be deleted at the end of its retention period
d) There must be a means to search for and erase personal data upon receipt of a lawful request from the data subject

Information & Transparency

e) The data subjects shall be provided with:
    - the identity and contact details of the data controller;
    - the contact details of the Data Protection Officer;
    - the purposes of the processing, including the legal basis and legitimate interests pursued
    - details of the categories of personal data collected
    - details of the recipients of personal data

Objection & Restriction

f) There must be means to restrict the processing of data on receipt of a lawful request from the data subject
g) There must be means to stop the processing of data on receipt of a lawful request from the data subject

Security

h) Appropriate training and instructions will be put in place to enable staff to operate the new system / process securely
i) Identify an Information Asset Owner
j) Update the Information Asset Register

Data storage location:

k) The storage for all documents must be within the UK or EEA.

Is the data being transferred to or through another organisation? If so:

l) There must be controls to ensure or monitor compliance by external organisations.

Is consent or pursuit of a contract the lawful basis for an automated processing operation? If so:

m) There must be a means to extract and transmit the data in a structured, commonly used and machine-readable format on receipt of a lawful request from the data subject
n) The consent must be recorded in some manner to serve as evidence

Does our Privacy Notice need to be updated? If so:

o) Update the Privacy Notice

2. Data Protection Assessment Screening

The purpose of the initial assessment is to determine the risk profile and whether further assessment is required to identify, assess and manage risks.

2.1. GDPR Required Screening Questions

ID	Screening question	Yes/No
1.	Does the system/process use systematic and extensive profiling or automated decision-making to make significant decisions about people?	No
	Comments: The system does not use systematic and extensive profiling or automated decision-making to make significant decisions about people	
2.	Does the system/process involve large scale processing of data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, data concerning a person's sex life or sexual orientation or data relating to criminal convictions or offences?	No
	Comments: The system does not involve large scale processing of data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, data concerning a person's sex life or sexual orientation or data relating to criminal convictions or offences	
3.	Will you be systematically monitoring a publicly accessible place on a large scale?	No
	Comments: The system will not systematically monitoring a publicly accessible place on a large scale	
4.	Will you be implementing novel technologies or new applications of existing technologies?	Yes
	Comments: Where data was previously stored on-premise, it will now be held in secure UK-based cloud data centres	
5.	Will the system / process help to make decisions about access to services, opportunities or benefits using automated decision-making, profiling or special category data (see list in question 2)?	No
	Comments: The system will not help to make decisions about access to services, opportunities or benefits using automated decision-making, profiling or special category data as listed in Q2	
6.	Will you be profiling using personal data on a large scale, taking into account the number of individuals involved, the volume and range of personal data, the duration of the processing and the geographical area covered?	No
	Comments: The system will not be profiling using personal data on a large scale, taking into account the	

	number of individuals involved, the volume and range of personal data, the duration of the processing and the geographical area covered	
7.	Will you be processing biometric or genetic data?	No
	Comments: The system will not be processing biometric or genetic data	
8.	Will you be matching or combining data from sources collected for other purposes or by other data controllers?	No
	Comments: The system will not be matching or combining data from sources collected for other purposes or by other data controllers	
9.	Will the system / process include 'invisible processing' of personal data (processing without providing a privacy notice to the individual)?	No
	Comments:	
10.	Will you be processing personal data in a way which involves tracking individuals' location or behaviour?	No
	Comments: The system will not be processing personal data in a way which involves tracking individuals' location or behaviour	
11.	Will you be processing children's personal data for profiling, automated decision-making or marketing purposes or to offer them a service directly?	No
	Comments: The system will not be processing children's personal data for profiling, automated decision-making or marketing purposes or to offer them a service directly	
12.	Will the system / process involve personal data which could result in a risk of physical harm in the event of a security breach?	Yes
	Comments: The solution may be used to store any and all ICO document up to official (inc. official sensitive). This could include casework, operational or personal documents/data. So where such sensitive information was shared with ICO, it might then be stored within Office 365.	

If you answer "Yes" to **one or more** of the screening questions in section 2.1 then complete the full assessment.

2.2. GDPR Advised Screening Questions

ID	Screening question	Yes/No
13.	Will the system/process include the profiling or scoring of individuals?	No
	Comments: The system will not include the profiling or scoring of individuals	
14.	Will the system/process result in you making automated decisions or taking automated action against individuals	No

	in ways which could have a legal or similarly significant impact on them?	
	Comments: The system will not result in us making automated decisions or taking automated action against individuals in ways which could have a legal or similarly significant impact on them	
15.	Will the system/process involve the systematic monitoring of individuals or publicly accessible areas?	No
	Comments: The system will not involve the systematic monitoring of individuals or publicly accessible areas	
16.	Does the system/process involve data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, data concerning a person's sex life or sexual orientation, data relating to criminal convictions / offences or other sensitive or highly personal data?	Yes
	Comments: The solution may be used to store any and all ICO document up to official (inc. official sensitive). This could include casework, operational or personal documents/data. This may therefore include documents related to matters such as TU meetings, HR records, etc.	
17.	Will you be processing personal data on a large scale, taking into account the number of individuals involved, the volume and range of personal data, the duration of the processing and the geographical area covered?	No
	Comments: The system will not be processing personal data on a large scale, taking into account the number of individuals involved, the volume and range of personal data, the duration of the processing and the geographical area covered	
18.	Will you be processing information about children or other vulnerable individuals or individuals over whom you hold a position of power (e.g. employees)?	No
	Comments: The system will not be processing information about children or other vulnerable individuals or individuals over whom you hold a position of power	
19.	Will you be implementing technological or organisational solutions which are new to the organisation? Updated or alternative versions of technologies currently in use are not to be considered new unless they include changes with considerable privacy implications (e.g. adding cloud storage to a previously local application).	No
	Comments: We will be adding cloud storage to a previously local application (files held in the MS cloud, rather than on-prem)	
20.	Will the system/process result in individuals being denied access to a service or contract or prevent them from exercising their rights?	No

	Comments: The system will not result in individuals being denied access to a service or contract or prevent them from exercising their rights	

If you answer yes to any of the questions in Section 2.2 then you may wish to consider completing the full DPIA. As a general guideline, you should complete the full assessment if you answer "Yes" to **two or more** questions, then you should complete the full assessment.

Otherwise, you may wish to complete Section 2, 4 & 6.3 onwards and either select other sections on a risk basis or partially complete some sections by focusing only on the risk factors identified in Section 2.2.

2.3. Screening Questions based on Risk Appetite

ID	Screening question	Yes/No
21.	Are you using existing information about individuals for a purpose it is not currently used for and would not have been reasonably expected when the information was provided?	No
	Comments: The system does not use existing information about individuals for a purpose it is not currently used for and would not have been reasonably expected when the information was provided	
22.	Will you disclose to external organisations information about individuals which is currently held internally or result in a material increase in the people with access internally?	No
	Comments: The system will not disclose to external organisations information about individuals which is currently held internally or result in a material increase in the people with access internally.	
23.	Will the system/process require you to contact individuals in ways which they may find intrusive?	No
	Comments: The system will not require us to contact individuals in ways which they may find intrusive	

If you answer "Yes" to **one or more** of the screening questions in Section 2.3 then complete Section 2.4, Section 4 and Section 6.3 onwards. You may choose to complete other sections where the risk requires it.

If you have not answered "Yes" to any of the screening questions in any section then there is no need to complete the remainder of the DPIA, but you **must** ensure that you add the mandatory requirements to your project backlog / requirements and consult representatives of the DPO throughout the delivery of the system / process. You should still complete a Security Impact Assessment.

2.4. DPIA Approach and Consultation

We have previously carried out a PSIA which covered the entire hosted Office 365 environment and the secure connectivity which links to the ICO's Core network. This was reviewed by Auriga consulting who provided a detailed realistic assessment of the privacy and security implications of the implementation of Microsoft Office 365 Core Cloud Product.

Therefore, as tools like Sharepoint and One Drive use the same secure transfer mechanism to connect ICO infrastructure to the cloud, and the One Drive data centres are based in the UK[1] in Durham or London, we do not intend to carry out any further external consultation for this DPIA.

We will consult both the Head of Cyber Security and the DPO prior to proceeding with One Drive.

As there is no change to the data being collected, only the location of its storage, we do not intend to consult ICO staff more widely.

[1] https://products.office.com/en-us/where-is-your-data-located?geo=UnitedKingdom#UnitedKingdom

3. Data Inventory

3.1. Information Flows

The data in scope of this DPIA could be any documents currently created, received and stored within ICO. This might include documents that contain personal data about employees or external parties.

The source of the documents could be any currently valid means of receiving or generating a document. For example, office applications (word, powerpoint, oneNote, etc) created by employees.

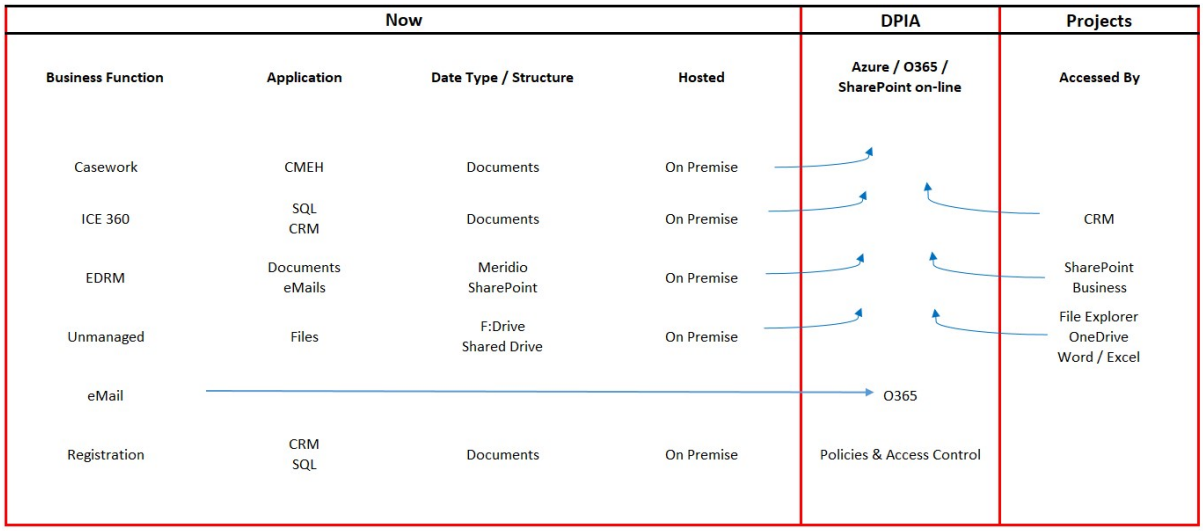
People will interact with Office 365 storage using windows or any of the office desktop tools in use within ICO today. It can also be used by future applications that depend upon Office 365 such as OneDrive, Teams, Sharepoint online, etc.

The transfer and storage of data utilises the same authentication and encrypted transfer and storage mechanisms previously covered in the Office 365 platform PSIA. The underlying platform connectivity and security is common to all applications and all uses of Office 365.

High level responsibilities over the documents, such as overall security and retention/disposal would be managed by Office 365 administrators.

At the lower level people would have control over the adding, removing, editing and sharing of individual documents within their document stores.

The high level diagram below illustrates what types of data we currently store on premise, and what will be moved to the document storage solution. Please note, we will not be collecting any new data or using it for new purposes. The project will simply change where the data lives.



3.2. Data Inventory

Identify the personal data to be held, the recipients (those with access to the data), the retention period and the necessity of the data collection, processing and retention.

Data Type	**Recipients**	**Retention Period**	**Necessity**
[Description of the data held (e.g. dates of birth, addresses etc.)] All Official personal data within our care.	[Who will have access to the data?] Access to document storage will be limited to ICO staff on a least privilege basis. File permissions (eg read, write, delete, etc) will be restricted by the document owner.	[How long will the data be held for?] See Corporate Retention Schedule for details of retention and disposition.	[Is the collection, processing and retention of this data necessary for the purpose pursued? You should always aim to minimise your data collection.] The processing will be limited to any Official personal data that is necessary to meet our specified and lawful purposes as a data controller.

4. Compliance Measures

Use this section to record your compliance with the requirements in section 1.5. Fill in the details of how the requirements have been met or list the requirement as N/A. The requirement source is a reference to GDPR unless otherwise stated.

Requirement	**Implementation Details**
Data Accuracy	
a) Data must be kept up to date	N/A. Outside scope of data storage DPIA.
b) There must be means to validate the accuracy of any personal data collected	
c) Inaccurate or incomplete personal data must be updated on receipt of a lawful request from the data subject	
Retention & Deletion	
d) All data collected will have a retention period	Existing retention policies are reproduced within Office 365.
e) Data must be deleted at the end of its retention period	Policy will delete data in line with existing policies.
f) Personal data must be erased upon receipt of a lawful request from the data subject	O365 tools to search and remove personal data will be configured in line with existing policies.
Information & Transparency	
g) The data subjects shall be provided with: ● the identity and contact details of the data controller; ● the contact details of the Data Protection Officer; ● the purposes of the processing, including the legal basis and legitimate interests pursued ● details of the categories of personal data collected ● details of the recipients of personal data	Information is published in our global privacy notice.
Objection & Restriction	
h) There must be means to restrict the processing of data on receipt of a lawful request from the data subject	
i) There must be means to stop the processing of data on receipt of a lawful request from the data subject	
Security	

j) Appropriate training and instructions will be put in place to enable staff to operate the new system / process securely	Users will access the system following the existing processes and procedures. Admin staff will have training to permit deletion of personal data etc.
k) Identify an Information Asset Owner	The Head of Digital and IT Services will own the supporting asset: the cloud-based document storage solution. Information assets will continue to be owned by the relevant IAO of each business function.
l) Update the Information Asset Register	IAOs are responsible for reviewing and, where appropriate, updating the corporate Information Asset Register.
<u>Conditional Requirements</u>	
m) The data subjects must be provided with information on where to obtain details of any safeguards over data transferred to non-GDPR compliant countries	The document storage solution will not store or process data outside the EEA (and we will use UK based data centres wherever possible).
n) Consult the DPO for additional requirements to ensure the processing is GDPR compliant.	
o) There must be controls to ensure or monitor compliance by external organisations.	External organisations do not have access to ICO data. Temporary access for maintenance tasks can be supplied under ICO admin oversight.
p) There must be a means to extract and transmit the data in a structured, commonly used and machine-readable format on receipt of a lawful request from the data subject	
q) The consent must be recorded in some manner to serve as evidence	
r) Update the Privacy Notice	The DPO's team will be responsible for reviewing and, where appropriate, updating the global privacy notice.

5. Data Protection Risk Assessment

Identify and assess the risks to subjects' rights, the actions you could take to reduce the risks and any future steps that will be necessary (e.g. the production of new guidance or security testing for new systems). Some example risk sources have been listed to aid you. This list is not comprehensive and will not necessarily apply to your system or process.
See Appendix for guidance on quantifying impact and likelihood.

Risks should be considered from the data subject's perspective not the ICO's, i.e. a reputational risk to the ICO should not be recorded here. Some example threats to consider include:

- Discrimination
- Identity theft and fraud
- Financial loss
- Damage to data subjects' reputation
- Loss of confidentiality of professional secrets
- Unauthorised reversal of pseudonymisation
- Social or economic disadvantage
- Deprivation of legal rights or freedoms
- Data subjects losing control over their data
- Loss of privacy or intrusion into private life
- Prevention from accessing services

Please note, the document storage solution will not involve the collection of new categories of data, or the use of data for new purposes. We will simply be changing where the data lives, and applying existing controls and processes to any processing operations.

Risk Details	**Impact**	**Likelihood**	**Response**
(1) **Collection and use** Collection and use of data is unfair and unlawful.	Low (2)	Medium (3)	There are established processes to collect and use data for specified and lawful purposes. Response will reduce the impact to very low. Residual risk is low.
(2) **Data quality** Collection and use of excessive or poor quality data.	High (2)	Medium (3)	There are established processes to collect and use the minimum data required to fulfil our purposes. Response will reduce the impact to very low. Residual

			risk is low.
(3) **Data retention** Retention of data for longer than is necessary.	Low (2)	Medium (4)	There are established processes to keep data for no longer than is required for our purposes. Make sure doc storage applies pour defined retention schedules. Response will reduce likelihood to very low. Residual risk is low.
(4) **Individual rights** Data processed without regard for statutory rights.	Low (2)	Medium (3)	There are established processes to recognise and respond to individuals' requests to exercise their rights. Response will reduce likelihood to very low. Residual risk is low.
(5) **Data security** Confidentiality, integrity and availability of data compromised.	High (4)	High (4)	Data processed by service shall be protected in line with NCSC's cloud security principles (see SIA for details, eg data protection in transit, access controls, etc.). Response will reduce impacts and/or likelihood. Overall residual risk is low.
(6) **Overseas transfers** Data transferred to jurisdiction that doesn't adequately protect statutory rights and freedoms.	High (4)	High (4)	Data shall be stored and processed in UK locations only. Response will reduce likelihood to very low. Residual risk is low.

6. Residual Risk and Sign Off

6.1. Residual Risk

Record details of the remaining risk. It is never possible to remove all risk so this section should not be omitted or blank.

If the residual risk remains high (e.g. red on the traffic light scoring in the Appendix) then you will need to consult the ICO by following the process used by external organisations.

The overall residual risk is low.

6.2. Necessity and Proportionality

If you answered "Yes" to two of the legally required screening questions in Section 2.1 (not 2.2) you should discuss the necessity and proportionality of the collection, processing and retention of this data here, weighing the impact on data subjects rights and freedoms against the benefits of the processing activity. You should also consider whether there are other reasonable ways to achieve the same result with less impact on data subjects.
If you have not answered "Yes" to two questions in Section 2.1, leave this section blank.

6.3. DPO Recommendations

Record any recommendations from the DPO or their delegates and responses here. This serves as useful tool when reconsidering a rejected DPIA or in recording the justification if the organisation rejects the DPO's advice.

No	Recommendation	Project Team Response
1	[Record any changes recommended by the DPO here]	[Record the actions taken as a result of the recommendation]

6.4. Sign Off

Send this to the DPSIA Committee to approve the privacy and security risks involved in the project, the solutions to be implemented and the residual risk.

Approved by	Role	Date	Project Stage
Louise Byers	DPO	10/9/18	Initiation
David Wells	Group Manager Cyber Security	10/9/18	Initiation

7. Integrate the outcomes back into the plan

Who is responsible for integrating the DPIA outcomes back into any project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any data protection concerns which may arise in the future?

Action to be taken	Date for completion	Responsibility for Action	Completed Date
(4) Ensure defined retention periods are applied to all datasets migrated to document storage solution.	TBC	Project lead	
(5) SIA actions to be carried into the project backlog.	TBC	Group manager Cyber Security	

Contact point(s) for future data protection concerns	

8. Change history

To be completed by the person responsible for delivering the system, service or process (in a project this will be the project manager).

Version	Date	Author	Change description
0.1	17/6/18	E Deen	First draft
0.2	01/08/18	P Lee	Draft
1.0	10/9/18	D Wells	Approved at DPSIA forum 10/9/18

9. Document control

Title	Data Protection Impact Assessment Template
Version	0.3.1
Status	Draft
Owner	DPSIA Committee
Approved by	DPO and Head of Cyber Security to be used to pilot DPIAs
Release date	02/07/18
Review date	31/12/18

Appendix – Risk Assessment Guidelines

Risk Probability setting

Probability	Criteria
Very low (1)	0-5% - extremely unlikely or virtually impossible
Low (2)	6-20% - low but not impossible
Medium (3)	21-50% - fairly likely to occur
High (4)	51-80% - more likely to occur than not
Very high (5)	81-100% - almost certainly will occur

Risk Impact setting

Impact	Criteria
Very low (1)	Likely to have minor impact to a small minority of data subjects. For example, minor inconveniences which will be overcome (e.g. time spent re-entering information, short delays, recoverable costs, needing to use alternative services, stress).
Low (2)	Likely to have minor impact to a significant number of data subjects. For example, minor inconveniences which will be overcome (e.g. time spent re-entering information, short delays, recoverable costs, needing to use alternative services, stress).
Medium (3)	Likely to have significant impact, such as significant inconveniences or minor detriment (e.g. misappropriation of funds, temporary loss of access to services, temporary change to credit rating, minor physical ailments or temporary injury, recoverable damage to property), to a small minority of data subjects.
High (4)	Likely to have significant impact, such as significant inconveniences or minor detriment (e.g. misappropriation of funds, temporary loss of access to services, minor physical ailments), on a significant number of data subjects or a major impact to a small minority of data subjects. A major impact would include significant or irreversible consequences (loss of employment, legal consequences, loss of access to services, long term psychological or physical ailments).
Very high (5)	Likely to have major impact to a significant number of data subjects or an irreparable impact to any number of data subjects. A major impact would include significant consequences (loss of employment, legal consequences, loss of access to services, long term psychological or physical ailments). Irreparable impacts would include inability to work, death etc.

Traffic light scoring

Probability						
Very Low (1)	Low (2)	Medium (3)	High (4)	Very High (5)		
Amber (5)	Amber (10)	Red (15)	Red (20)	Red (25)	Very High (5)	**Impact**
Green (4)	Amber (8)	Amber (12)	Red (16)	Red (20)	High (4)	
Green (3)	Amber (6)	Amber (9)	Amber (12)	Red (15)	Medium (3)	
Green (2)	Green (4)	Amber (6)	Amber (8)	Amber (10)	Low (2)	
Green (1)	Green (2)	Green (3)	Green (4)	Amber (5)	Very Low (1)	

Case reference

IC-203321-W1K8

Enabling Teams for Civil Interviews – Draft DPIA

ico.
Information Commissioner's Office

Data Protection Impact Assessment Enabling Teams for Civil Interviews

Document Name	Data Protection Impact Assessment Enabling Teams for Civil Interviews
Author/Owner (name and job title)	Jo Stones, Group Manager Civil Investigations Team
Department/Team	Civil Investigations Team, Regulatory Strategy Service
Document Status (draft, published or superseded)	Draft
Version Number	v0.1
Release Date	
Approver (if applicable)	n/a
Review Date	
Distribution (internal or external)	Internal

Guidance for completing this template

Complete this Data Protection Impact Assessment (DPIA) template if your DPIA screening assessment indicates a high risk to individuals. If you are unsure whether you need to complete a DPIA use the **DPIA Screening Assessment** to help you decide.

Aim to complete your DPIA as early as possible as the outcome of the assessment could affect the viability of your plans. In extreme cases, you will not be able to continue with your plans without changing them, or at all.

Guidance notes are included within the template to help you with its completion- just hover your mouse over any blue text for further information.

The Information Management Service is also available for further advice and support. Please keep in mind our service standards if you require advice.

1. Process/system overview

1.1 Ownership

Project Title:	Using Teams for Civil Interviews
Project Manager:	Jo Stones
Information Asset Owner:	Director of Investigations, currently Stephen Eckersley
Data controller(s)	ICO
Data processor(s)	Microsoft

1.2 Describe your new service or process

This DPIA covers the use of Microsoft (MS) Teams for conducting voluntary interviews with witnesses and significant witnesses in connection with Civil investigations. Witnesses are indivuduals whom have information of relevance to the ICO, usually in the context of the ICO's investigative work. A significant witness is usually someone who has directly seen or heard events believed by the investgating officer to be of direct relevance to the matter under investigation. A witness is usually someone who also has knowledge of an event, but may not be directly involved in the event itself.

The ICO already conducts face to face interviews, usually as part of the criminal investigation process. The change covered by this DPIA is to use MS teams for remote interviews within the Civil Team, whereas previously the use of MS Teams in this context has been for interviews conducted by the Criminal Investigation Team. The existing process used by the Criminal Investigation Team will be amended to cover the minor procedural changes for using MS

Teams for voluntary witness interviews conducted by the Civil Investigation Team.

It is considered unlikely that interviews of this kind will be regulary carried out by the Civil Team. Whilst it is not possible to confirm specific volumes, it is aniticpated that recording of interviews in this way would be necessary is very few cases, and less than one or two occasions per case per year.

The Civil Investigation Team are responsible for the investigation and progression of alleged infringements of the DPA 2018.

Key responsibilities of the Civil Team include:
• conducting enquiries to establish the facts of an alleged infringement;
• gathering evidence and producing exhibits;
• where necessary, taking witness statements;
• where necessary, conducting witness interviews;
• producing recommendation reports for the delegated authority detailing what, if any, regulatory action should be taken in response to any identified infringements.

Occasionaly, an interview with a witness may be required in order to progress civil cases to a conclusion. Unless the invitation to interview is declined by a witness, the account they provide may identify additional lines of enquiry, or otherwise assist the ICO in reaching a decision on a case.

During the current Covid-19 pandemic it is not always possible or appropriate to hold face to face interviews with witnesses. It is not clear how long these restrictions will last and this could have a detrimental impact on the ability to progress investigations to a conclusion.

There is minimal impact on the interviewee through the use of Teams for the following reasons:

- The PD and SCD is processed in accordance with the ICO Privacy Notice and policy document 'Our processing of special categories of personal data and criminal offence data.
- Interviews are not expected to be undertaken with suspects in relation to Civil cases. However, in the event that a witness should make an omission that may lead the investigation team to determine that they are a suspect in relation to an offence, any subsequent interview would be carried out in accordance with Code C of the Police and Criminal Evidence Act (PACE 1984).
- The ability to conduct civil interviews through the use of Teams will expedite investigations and, in the event that a witness becomes a suspect, be compliant with the Criminal Procedures and Investigations Act (CPIA 1996), thus reducing the potential for interviews to suffer from undue stress/anxiety due to prolonged investigations.
- Interviewees would be invited for interview irrespective as to whether that is via a face to face interview or through the use of Teams.
- The intereviewee can decline to be interviewed.

1.3 Personal data inventory - explain what personal data is involved

Categories of data	Data subjects	Recipients	Overseas transfers	Retention period
Name (always captured)	**Witness** – this could be a current or former staff member of a controller or processor, an indidivdual associated with the controller or processor's work or a member of public **Legal Representative** – the intervieewes legal representative. **ICO Investigators**	Witness Controller Processor Legal Representative ICO Investigators ICO Legal Team Barristers Tribunal	Not Applicable	Up to six years in the event of a formal regulatory action case, unless suitable for National Archives.
Date of Birth (may be captured)	**Witness**	Witness Controller Processor Legal Representative ICO Investigators ICO Legal Team Barristers Tribunal	Not Applicable	Up to six years in the event of a formal regulatory action case, unless suitable for National Archives.

Contact Details (always captured)	**Witness** – this could be a current or former staff member of a controller or processor, an indidivdual associated with the controller or processor's work or a amember of public **Legal Representative** – the intervieewes legal representative. **ICO Investigators**	Witness Controller Processor Legal Representative ICO Investigators ICO Legal Team Barristers Tribunal	Not Applicable	Up to six years in the event of a formal regulatory action case, unless suitable for National Archives.
IP Address (always captured)	**Witness** – this could be a current or former staff member of a controller or processor, an indidivdual associated with the controller or processor's work or a member of public **Legal Representative** – the intervieewes legal representative. **ICO Investigators**	ICO Microsoft	Not Applicable	Up to six years in the event of a formal regulatory action case, unless suitable for National Archives.
Cookies (always captured)	**Witness** – this could be a current or former staff member of a controller or processor, an indidivdual associated with the controller or processor's	Microsoft	Not Applicable	Up to six years in the event of a formal regulatory action case, unless suitable for National Archives.

	work or a amember of public **Legal Representative** – the intervieewes legal representative. **ICO Investigators**			
Race (Image) (possible for visually recorded interviews)	**Witness** – this could be a current or former staff member of a controller or processor, an indidivdual associated with the controller or processor's work or a amember of public **Legal Representative** – the intervieewes legal representative. **ICO Investigators**	Witness Controller Processor Legal Representative ICO Investigators ICO Legal Team Barristers Tribunal	Not Applicable	Up to six years in the event of a formal regulatory action case, unless suitable for National Archives.
Ethnic Origin (Image) (possible for visually recorded interviews)	**Witness** – this could be a current or former staff member of a controller or processor, an indidivdual associated with the controller or processor's work or a amember of public **Legal Representative** – the intervieewes legal representative. **ICO Investigators**	Witness Controller Processor Legal Representative ICO Investigators ICO Legal Team Barristers Tribunal	Not Applicable	Up to six years in the event of a formal regulatory action case, unless suitable for National Archives.

Political Opinions (Possible where context of interview has relevance)	**Witness** – this could be a current or former staff member of a controller or processor, an indidivdual associated with the controller or processor's work or a amember of public **Legal Representative** – the intervieewes legal representative. **ICO Investigators**	Witness Controller Processor Legal Representative ICO Investigators ICO Legal Team Barristers Tribunal	Not Applicable	Up to six years in the event of a formal regulatory action case, unless suitable for National Archives.
Religious Beliefs (Possible where context of interview has relevance)	**Witness** – this could be a current or former staff member of a controller or processor, an indidivdual associated with the controller or processor's work or a amember of public **Legal Representative** – the intervieewes legal representative. **ICO Investigators**	Witness Controller Processor Legal Representative ICO Investigators ICO Legal Team Barristers Tribunal	Not Applicable	Up to six years in the event of a formal regulatory action case, unless suitable for National Archives.
Trade Union Membership (Possible where context of interview has relevance)	**Witness** – this could be a current or former staff member of a controller or processor, an indidivdual associated with the controller or processor's	Witness Controller Processor Legal Representative ICO Investigators ICO Legal Team	Not Applicable	Up to six years in the event of a formal regulatory action case, unless suitable for National Archives.

	work or a amember of public **Legal Representative** – the intervieewes legal representative. **ICO Investigators**	Barristers Tribunal		
Health Data (Possible where context of interview has relevance)	**Witness** – this could be a current or former staff member of a controller or processor, an indidivdual associated with the controller or processor's work or a amember of public **Legal Representative** – the intervieewes legal representative. **ICO Investigators**	Witness Controller Processor Legal Representative ICO Investigators ICO Legal Team Barristers Tribunal	Not Applicable	Up to six years in the event of a formal regulatory action case, unless suitable for National Archives.
Criminal Convictions (Possible where context of interview has relevance)	**Witness** – this could be a current or former staff member of a controller or processor, an indidivdual associated with the controller or processor's work or a amember of public **Legal Representative** – the intervieewes legal representative. **ICO Investigators**	Witness Controller Processor Legal Representative ICO Investigators ICO Legal Team Barristers Tribunal	Not Applicable	Up to six years in the event of a formal regulatory action case, unless suitable for National Archives.

1.4 Identify a lawful basis for your processing

Article 6 of the UK GDPR.

Article 6 (1) (a) provides that processing shall be lawful if the data subject has given consent to the processing of his or her personal data for one or more specific purposes, the specific purpose in this case being their attendance at interview. This is confirmed in written communications with the witness and/or their legal advisor prior to interview. This is also clarified verbally at the commencement of an interview.

Once the interview has taken place any information moved from Teams will be processed under Article 6(1)(e) - public task.

Where the processing relates to sensitive personal data as outlined in Article 9 of the UK GDPR, the witness, and if applicable their legal representative, will have consented as outlined above, for their participation in, and contribution to the interview.

Personal data and sensitive personal data gathered during the course of the interview will be processed as necessary for the purposes of the Commissioner's investigative functions (Section 115 of the DPA18 & Article 57 (tasks), and Article 58 of the GDPR (powers)).

In the event that a witness should make an omission of a criminal offence, the Information Commissioner is named as a competent authority for the purpose of Part 3 of the DPA 2018 which applies to the processing of personal data by such authorities for law enforcement purposes as follows:

Section 35 DPA 2018.

The processing of personal data for the facilitation of a criminal interview is based upon consent. No interview will take place unless the suspect agrees to their participation in the interview. This is confirmed in written communications with the suspect and/or their legal advisor prior to interview. This is also clarified verbally at the commencement of an interview.

Where the processing relates to sensitive personal data as outlined in s35(4) DPA 2018, the suspect, and if applicable their legal representative, will have consented as outlined above, for their participation in, and contribution to the interview.

Personal data and sensitive personal data gathered during the course of the interview will be processed as necessary for the law enforcement process.

The ICO Privacy Notice outlines the use of personal data for law enforcement processes:

https://ico.org.uk/global/privacy-notice/investigations-for-law-enforcement-purposes/

The ICO Safeguards Policy details sensitive processing for law enforcement purpose:

https://ico.org.uk/about-the-ico/our-information/safeguards-policy/

1.5 Explain why it is necessary to process this personal data

In order to exercise the Commissioner's functions under section 115 of the DPA18 & Article 57 (tasks), and Article 58 of the GDPR (powers), and in particular to monitor and enforce the application the legislation, it is necessary for the ICO to undertake investigation of alleged non-compliance with the DPA18 and the GDPR. This includes gathering all relevant evidence from all relevant sources, including witnesses.

ICO investigators conduct investigations in accordance with all current legislation including the CPIA.

The CPIA codes of practice state "in conducting an investigation the investigator should pursue all reasonable lines of inquiry, whether these point towards or away from the suspect. What is reasonable in each case will depend on the particular circumstances". Interviews with suspects form part of that process and all investigators are required to undertake good quality and timely investigations.

During the current Covid-19 pandemic it may not be possible to hold face to face interviews. It is not clear how long these restrictions will last.

1.6 Outline your approach to completing this DPIA

Consultation has previously taken place in relation to the DPIA produced by the Criminal Investigation Team regarding the recording of interviews via Teams with:

Regulatory Legal
Information Management
Business Development
Digital and IT Services
Business Architect
Information Security

Where required, each witness in a civil investigation will be offered the opportunity to subject to a voluntary interview via Teams. They may decline to do so, and any queries they may have can be addressed with them at that time. If they have concerns regarding the process then they would be offered the opportunity to be interviewed in a conventional setting when Covid-19 restrictions are lifted, or Op Volta grants approval for a conventional interview to take place.

Whilst any refusal to be interviewed via Teams would delay the progression of the case, this would be the witneses decision and would assist the ICO in defending abuse of process arguments at a later stage.

There is a restricted, dedicated site on EDRM for the storage of the recordings. Extensive testing has taken place to identify any issues/mitigate risk.

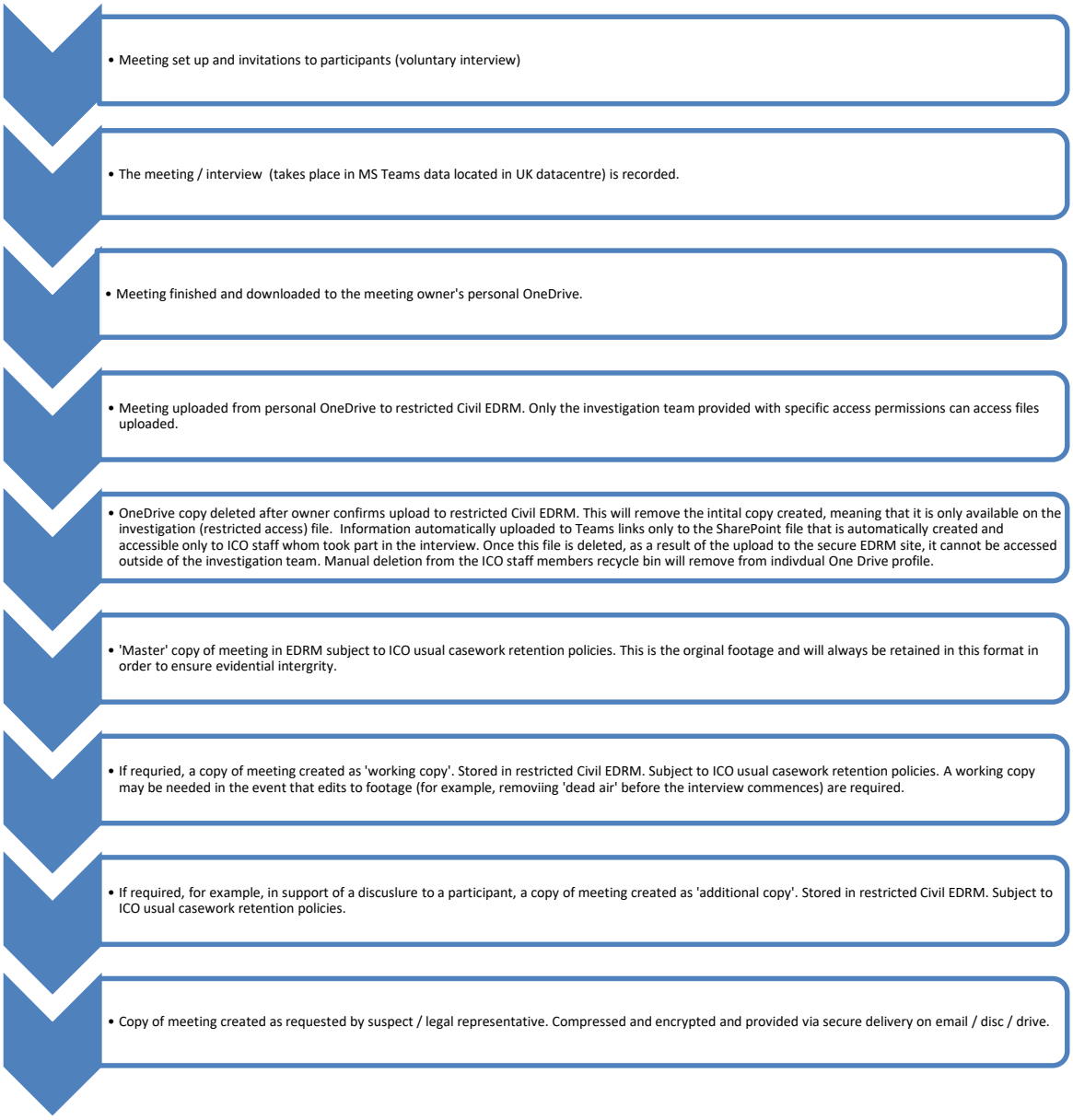
2.0 Data flows

2.1 Provide a systematic description of your processing, from the point that the data is first collected through to its destruction.

If your plans involve the use of new technology you should explain how this technology works and outline any 'privacy friendly' features that are available.

The process guidance and narrative on data flow has been moved to Appendix 1 on the advice of the DPIA panel on 21.12.20.

This is the simple data flow of the process:



3.0 Key principles and requirements

Purpose & Transparency

1. Will you need to update our privacy notices?

Yes ☐ No ☒

2. If you are not updating our privacy notices how do you intend to communicate information about your processing to the data subjects?

Civil interviews are not spefiically covered in the ICO's privacy notice, although Criminal interview are. The witness and if applicable their legal advisor will be advised by the lead investigator of the requirement to use Teams, and provided with bespoke fair processing information included in our standard letters. The process is detailed in Section 2.1 of the DPIA.

3. If consent is your lawful basis for processing personal data are you maintaining appropriate records of the data subjects consent?

1. Yes ☒ No ☐ N/a ☐

4. If legitimate interests is your lawful basis for processing have you completed a legitimate interest assessment?

Yes ☐ No ☐ N/a ☒

If applicable please provide a link to your completed assessment.

N/A

Accuracy

5. Are you satisfied the personal data you are processing is accurate?

Yes ☒ No ☐

6. How will you ensure the personal data remains accurate for the duration of your processing?

This is a live recording that is not subject to any digital interference. The suspect and if applicable their legal advisor are entitled to a copy of the recording, and the recording may later be used in Tribunal proceedings.

7. If the personal data isn't being obtained directly from the data subject what steps will you take to verify accuracy?

Not applicable with regards to the witness.

Minimisation, Retention & Deletion

8. Have you done everything you can to minimise the personal data you are processing?

Yes ☒ No ☐

9. How will you ensure the personal data are deleted at the end of the retention period?

As per current ICO policy.

10. Will you need to update the retention and disposal schedule?

Yes ☐ No ☒

Integrity and confidentiality

11. Where will the personal data be stored?

ICO systems: EDRM Interviewer OneDrive until deleted.

12. Are there appropriate access controls to keep the personal data secure?

Yes ☒ No ☐

13. Have you contacted the cyber security team for a security assessment of your plans?

Yes ☐ No ☒ N/a ☐

If applicable please provide a link to any assessment.

n/a

14. Please explain the policies, training or other instructions you intend to put in place to enable staff to operate the new system or process securely.

Civil Team staff are already familiar with the use of Crimson (the ICO's case management platform as in use for Investigations) and EDRM. A guide has been prepared as outlined in part at s2.1. A full copy will be supplied with the DPIA. A number of the Civil Team staff will be involved in the testing of the system (which has in any event, already been sucessfuly used by Criminal Team staff) and all staff will be briefed prior to using Teams for the first time for civil interviews.

For clarity, no footage will be stored on Crimson – EDRM is the only location in which permanent copies of Teams' recordings will be stored (as per the details set out in this DPIA).

Accountability

15. Who will be the Information Asset Owner for this personal data?

Director of Investigations

16. Will you need to update our Article 30 record of processing activities?

Yes ☐ No ☒

17. If you are using a data processor have you agreed, or will you be agreeing, a written contract with them?

Yes ☒ No ☐ N/a ☐

Individual Rights

18. Is there a means of providing the data subjects with access to the personal data being processed?

Yes ☒ No ☐

19. Can inaccurate or incomplete personal data be updated on receipt of a request from a data subject?

Yes ☒ No ☐

Note: the interview recording will be an accurate record of the interview and will not need any rectification.

20. Can we restrict our processing of the personal data on receipt of a request from a data subject?

Yes ☒ No ☐

21. Can we stop our processing of the personal data on receipt of a request from a data subject?

Yes ☒ No ☐ N/a ☐

Note: The lawful basis for the use of Microsoft Teams as a means of carrying out an interview is consent. Data subjects can withdraw consent before the interview. Withdrawal of consent during or after the interview for the use of Teams has an implication on anything saved on Teams. So if the recording has

not been uploaded or there is a chat history this should not be processed once consent has been withdrawn.

Any information moved from Teams will be processed under public task so if data subjects object to this process any objection will be considered by the Information Access Team following existing processes.

22. Can we extract and transmit the personal data in a structured, commonly used and machine readable format if requested by the data subject?

Yes ☒ No ☐ N/a ☐

23. Can we erase the personal data on receipt of a request from the data subject?

Yes ☒ No ☐

Risk Description	Response to Risk	Risk Mitigation	Expected Risk Score		
			I	P	Total
			See Appendix 1 – Risk Assessment Criteria		
Example: *Access controls are not implemented correctly and personal data is accessible to an unauthorised third party.*	*Reduce*	*Existing mitigation: We have checked that the system we intend to procure allows us to set access permissions for different users.* *Expected mitigation: We will appoint and train a system administrator who will be responsible for implementing access controls and monitoring access. The system administrator will also audit the system periodically to review access permissions.*	*3*	*2*	*6 - medium*
Access to recording facilities on Teams. Copying, storage and onward distribution of all copies of the interview.	Accept	Access is restricted to staff from the Civil Team. Only the lead interviewer who starts the recording will be able to access the recording on their OneDrive before they upload it to EDRM. The interviewee will not be able to record the interview on Teams. If any issues are encountered IThelp would be able to provide OneDrive access to a specific member of the team. IThelp would then be able to upload the data to EDRM on behalf of the Civil Team. In the event of copying, only authorised Civil Team members, whom form part of	1	1	1

		the investigation team, can copy a file and this must be carried out in accordance with the very limited circumstances set out in the DPIA (for example, to create a working copy. In relation to onward distribution, where the recipient facilities allow, this must be achieved in a secure manner via encrypted disk or portable device. If this is not possible, consultation with the ICO's IT Dept must take place to confirm a secure means of electronic disclosure that provides appropriate controls.			
Chat function within Teams may result in admissions from attending parties that contain personal data	Accept	The chat function is to be disabled when sending out the Teams' invite.	1	1	1
MS drop cookies without consent when users land on the Teams page on a browser. This includes dropping tracking, analytics and advertising cookies. People are unable to consent to their data being used in this way	Accept	Existing: It is understood that in response to previous use of Teams within the ICO, an email has been sent to Microsoft to inform them that their platform is not compliant and request they look at rectifying this. Expected: Inform users of the activity on the site before sending them to it so they can make an informed (albeit not ideal) decision.	2	5	10
An attendee might share additional personal data, including SCD that may not be related to the civil investigation.	Accept	The attendees will have agreed to the interview in the expectation that they will be sharing personal data and SCD.	1	5	5

		Clear fair processing information should be shared with all attendees so they aware what will happen to any PD shared.			
Staff do not follow procedures when undertaking interviews	Reduce	Expected: IT will limit the recording functionality to members of the civil team. Procedures have been drawn up on how to conduct interviews using Teams and will include instructions to provide fair processing information to attendees. The completed interview will be subject to management review. I.T. have the capability to retrieve the recording if necessary from the Lead Investigators OneDrive.	2	2	4
Unauthorised people attending interviews	Reduce	Whilst there is limited access to the ICO offices, all interviews by ICO staff will be conducted within the office environment. In the event of no ICO office access, measures to be taken to prevent identification of domestic premises including use of 'blurred' backgrounds. When the meeting organiser creates a Microsoft Live Event, they can choose to limit it to only specified people or groups. Only the suspect and where appropriate the legal advisor will be invited to the event.	3	2	6

		After invite for a team meeting has been sent to specific individual(s), the civil team meeting organiser will perform a manual check that attendee is the correct person and no others are on call. If anyone else attempts to join meeting, the civil meeting organiser will be notified. Attendees will be advised to join via web browser or teams application and not join anonymously via Dial in feature which can be revoked. The interviewer can request to see photo identification before proceedings with the interview. As per the process guidance, we will use the 'Lobby' function to hold people in a virtual waiting area while ICO investigators check who is attending the interview, and then permit them entry to the interview once identification is confirmed.			
There is a risk that information may be shared inadvertently through the screen share function by ICO officers.	Reduce	Mitigation for this risk is the advice on screen sharing for investigators in the process and guidance document.	2	2	4

5.0 Consult the DPO

Guidance: Submit your DPIA for consideration by the DPIA Forum. The process to follow is here.
Any recommendations from the DPOs team will be documented below and your DPIA will be returned to you. You should then record your response to each recommendation.

	Recommendation	**Date and project stage**	**Project Team Response**
1.	Section 1.2 – some explanation of the difference between witness and significant witness would be useful. What is the significance of this distinction?	Planning	**Explanatory text added to section 1.2 on 19/01/2022**
2.	Section 1.3 (Data inventory) - For data categories marked as "Possible" do we seek this information as a matter of course. Can it be made clearer what we will always need to process vs what might be incidental?	Planning	**Explanatory text added to section 1.3 on 19/01/2022**
3.	Lawful basis – update 1.4 to confirm public task lawful basis.	Planning	**Confirmed amendment/accepted change on 19/01/2022**
4.	Section 1.5 – review content about criminal investigations. Is this still relevant to this DPIA as it seems to mostly relate to suspects?	Planning	**Section related to Criminal suspect interviews removed on 19/01/2022**
5.	Section 2.0 (data flows) - Elaborate on restrictions for recordings. Is the recording restricted to the investigating team once uploaded to Civil EDRM or is it the wider department?	Planning	**Explanatory text, confirming investgiatin team only access, added to section 2.0 on 19/01/2022**
6.	Section 2.0 (data flows) – *"meeting finished and downloaded to the meeting owners personal one drive".* Can you add some clarification about where this is downloaded from as we need to ensure there isn't another copy floating around. All procedures indicate		**Explanatory text, confirming investgiatin team only access, added to section 2.0 on 19/01/2022**

	staff should delete from their onedrive but we need to be sure this primary source is deleted too.		
7.	Delete the recording from the device Recycle Bin should be written into process as we've recently discovered that there is no automated deletion of device recycle bins. OneDrive recycle bin is automatic but an additional manual deletion will need to take place to remove the file from the device.	Planning	**Additional text added to section 2.0 on 19/01/2022**
8.	Data flow – Please define master, working and additional copy. For what purpose are multiple copies created and how do you distinguish between them and ensure integrity of master? Please include more detail in data flow to explain.	Planning	**Additional text added to section 2.0 on 19/01/2022**
9.	Section 3 Q1- Bespoke privacy information will likely need an update. Your privacy notices should be reviewed to ensure the fair processing information is suitable for civil teams use and covers processing taking place in relation to all data subjects (witnesses, legal representatives and ICO investigators).	Planning	**Query raised with Information Management on 19/01/2022.**
10.	Q14- Can you clarify why Crimson is mentioned in response to Q14. Are recordings also added to Crimson? If so please update data flows and risk assessment to reflect this or remove reference.	Planning	**Additional text added to section 2.0 on 19/01/2022**
11.	Risk 1 – broaden the risk to include all stages of recording, copying, storage and onward distribution of all copies of the interview.	Planning	**Additional text added to section 2.0 on 19/01/2022**
12.	Recommend bespoke privacy information includes a link to advice on ICO website about on removing cookies. We can't stop these being dropped but we can provide advice in PN on how to remove after interview.	Planning	**Query raised with Information Management on 19/01/2022.**
13.	1.2 (description of processing) – DPIA could be improved with some estimation of the scale of processing. How frequently will Teams be used for	Planning	**Additional text added to section 1.2 on 19/01/2022**

	interviews by civil per annum, roughly how many data subjects?		
14.	Add risk of using chat function to risk assessment for completeness. Mitigation is advising against use as per your Appendix.	Planning	**Additional text added to section risk on 19/01/2022**

6.0 Integrate the outcomes back into your plans

Guidance: Identify who is responsible for integrating the DPIA outcomes. The outcomes include any expected mitigation you need to take as identified in your risk assessment and any further actions resulting from the DPOs recommendations.

Action	**Date for completion**	**Responsibility for Action**	**Completed Date**

7.0 Expected residual risk and sign off

Guidance: Summarise the expected residual risk below. This is any remaining risk *after* you implement all of your mitigation measures and complete all actions. It is never possible to remove all risk so this section shouldn't be omitted or blank. If the expected residual risk remains high (e.g. red on the traffic light scoring in the Appendix) then you will need to consult the ICO as the regulator by following the process used by external organisations.

Cookies is recorded as the highest residual risk. This appears to be an anomaly because

7.1 IAO sign off

IAO (name and role)	Date	Project Stage
Stephen Eckersley, Director of Investigations		Final

8.0 Change history

Guidance: To be completed by the person responsible for delivering the system, service or process (in a project this will be the project manager).

Version	Date	Author	Change description
V0.1	16/12/2021	Jo Stones	First Draft

Appendix 1: Risk Assessment Criteria

The following criteria are aligned with our corporate risk assessment criteria.

Impact

Impact is the consequence of a risk to the rights and freedoms of individuals being realised. Factors to consider include the financial harm or emotional distress that can be expected to occur.

Impact	Scoring criteria
Very low (1)	No discernible impact on individuals.
Low (2)	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc).
Medium (3)	Individuals may encounter significant inconveniences, which they will overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc)
High (4)	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc).
Very high (5)	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Probability

Probability is the likelihood of a risk to the rights and freedoms of individuals being realised. Factors to consider include the expected frequency of occurrence, and the motivation and capability of threat sources (eg does the threat require insider knowledge and/or significant technical resources to exploit any vulnerability?).

Probability	Scoring criteria
Very low (1)	0-5% - extremely unlikely or improbable For example, the risk has not occurred before or is not expected to occur within the next three years.
Low (2)	6-20% - low but not improbable For example, the risk is expected to occur once a year.
Medium (3)	21-50% - fairly likely to occur

	For example, the risk is expected to occur several times a year.
High (4)	51-80% - more likely to occur than not For example, the risk is expected to occur once a month.
Very high (5)	81-100% - almost certainly will occur For example, the risk is expected to occur once a week.

Risk level
Risk level is a function of impact and probability, and is represented by a RAG rating.

Probability / Impact	Very low (1)	Low (2)	Medium (3)	High (4)	Very high (5)
Very high (5)	Amber (5)	Amber (10)	Red (15)	Red (20)	Red (25)
High (4)	Green (4)	Amber (8)	Amber (12)	Red (16)	Red (20)
Medium (3)	Green (3)	Amber (6)	Amber (9)	Amber (12)	Red (15)
Low (2)	Green (2)	Green (4)	Amber (6)	Amber (8)	Amber (10)
Very low (1)	Green (1)	Green (2)	Green (3)	Green (4)	Amber (5)

Risk acceptance criteria
These criteria are guidelines only, and any risk treatment decisions should be made on a case-by-case basis. For example, it may be prudent to reduce a low risk because of legal and regulatory requirements.

Risk level	Acceptance criteria
Low (Green)	Within this range risks can be routinely accepted.
Medium (Amber)	Within this range risks can occasionally be accepted but shall be kept under regular review.
High (Red)	Within this range risks shall not be accepted and immediate action is required to reduce, avoid or transfer the risk.

Appendix 2: example risks to data subjects

Guidance: The following are examples of common risks associated with the processing of personal data to assist with your risk assessment. Not all of them will apply to your processing and the list is not exhaustive – you should consider specific risks that are relevant to your plans.

- Data is processed for unspecified / unlawful purposes/ not within expectations of data subjects
- Excessive data is processed
- Data is not kept up to date
- Data is kept for longer than is necessary by us
- Data is kept for longer than is necessary by data processor
- Data processed in contravention of data subject rights
- Data subjects unable to exercise their rights
- Data stolen or modified in transit
- Data stolen or modified at rest in our premises
- Data stolen or modified at rest in data processor premises
- Data transferred overseas to a jurisdiction that does not adequately protect data subject rights
- Re-identification of pseudonymised data by data processor or third party
- Unauthorised destruction or loss of data
- Data processor network / system / online portal not secure
- Data processor fails to process data in accordance with our instructions
- Personal data of children processed without appropriate safeguards / parental authority
- Consent of data subject not freely given (for example employer / employee processing)
- The data subject is particularly vulnerable (elderly or disabled) or is there a potential imbalance of power between the individual and the data controller (employee/employer)
- Source of data poses risks re accuracy (obtained from a unverified or old list)
- Risk to accuracy of data due to matching / combining data from different sources
- Use of new technology, e.g. fingerprinting, face recognition
- Monitoring or recording individuals
- Using profiling according to characteristics or behavior
- Non-compliance with DP principles

9.0 Template Document control

Title	Data Protection Impact Assessment Template
Version	1.0
Status	First release
Owner	Information Management Service
Release date	07/10/20
Review date	07/10/22

Appendix 1

Access to Microsoft Teams 'meeting' recording will be provided to all relevant members of the Civil Team (currently three staff members). Controlled tests have previousy taken place by the Criminal Team to ensure the viability of the process.

Those tests have been successful in a variety of circumstances, using combinations of investigators in different locations. The tests have represented one on one interviews, interviews where a suspect is represented by a legal advisor, and where there are two investigators conducting the interview. The interviews are recorded onto the lead investigators OneDrive, from where they have been successfully uploaded into the dedicated SharePoint folder. The recordings in the SharePoint folder have been viewed for accuracy.

Following consultation with the ICO Business Architect for those interviews, the recordings are saved directly to OneDrive. The lead investigator will be responsible for uploading into EDRM and deleting the OneDrive copy after verifying the complete video has been uploaded without corruption.

Where a copy of the interview is requested, these will either be compressed and emailed or provided on an encrypted and password protected disc or pen drive. Where interviews are downloaded onto a disc or pen drive, a master, working and additional (spare) copy will be created. The additional copy will be supplied to the legal adviser or suspect when requested. Pen drives and discs created as a result of this process will be recorded as exhibits as per the current policy, and retained securely in the exhibit store in accordance with current practice, procedure and legislation. The passing of discs or pen drives will be in accordance with current ICO security protocols.

The following is an extract from the guidance document used by the Criminal Team. This will be updated / amended to frame the instructions for the Civil Team:

Teams video conferencing instructions

1. All investigators have access to Microsoft Teams on their MMD. The use of Teams to conduct criminal interviews will not preclude the suspect from having a legal representative present, nor if appropriate a translator. However, attendees for the interview should be kept to a minimum and the interviewee should be made aware of who is permitted to be present during the interview. If there is any deviation from the agreed attendance, this should be addressed at that time, and if the issue cannot be resolved the interview should be terminated, and if possible rescheduled.

2. The success of this approach is dependent on not only the technology available to the interviewer, but also that available to the interviewee. Whilst most people have access to a smart mobile phone, laptop or

desktop computer, that will not be the case for all. The lack of access to a suitable device for the interviewee will not be considered a refusal to attend the interview. If that situation arises further consideration will be given, and if necessary the views of the Legal Team and/or Operation Volta will be sought.

3. Please note, this guidance only applies to the use of Microsoft Teams and not other similar software that may be available. The use of Microsoft Teams has been addressed in a DPIA, an SIA and has been subject to consultation and testing within the ICO.

4. You will arrange the interview by setting up a meeting using your calendar within Teams, adding the interviewees/attendees email address to the 'attendees' field. This will ensure that they receive an invite that includes a link to the Teams meeting.

5. Provide adequate notice of the interview using a formal invitation to interview. This should be also used as an opportunity to explain how the recording of the interview will work, and by providing the standard fair processing information. You will also need to provide details of, or a link to the ICO privacy policy.

6. When creating the invitation to interview please ensure that you use the Virtual Lobby facility in Microsoft Teams. This will ensure you can start recording the meeting before allowing the external attendees entry to the meeting. Details of how to set up the virtual lobby can be found through this link:


20200505
Instructions for Setup

7. Instructions on how to record in Microsoft Teams can be found in the following link:

   https://support.microsoft.com/en-us/office/record-a-meeting-in-teams-34dfbe7f-b07d-4a27-b4c6-de62f1348c24#:~:text=Record%20a%20meeting%20or%20call.%201%20Start%20or,shows%20up%20in%20the%20meeting%20chat%20...%20

8. The person receiving the invitation will then have to click on the link embedded in the email to join the meeting. They will have two options, downloading a windows app or by joining through a webpage. In neither case is there any requirement for the attendee to already have Teams installed.

   - Video rather than audio-only should take place. This not only allows you to see facial expressions and body language of the interviewee but

will prevent any issue of identification should that arise at a later stage. Interviewees may be asked to provide proof of identity by showing a drivers licence, passport or similar documents at the commencement of the interview.

- Ask the individual being interviewed to call from a private and quiet room free of distractions, and request that mobile phones are turned off. You should advise them that they can blur the background if they do not want their wider environment captured during the interview.

- You should close down all non-essential programs on your MMD device. For example, Outlook in circumstances where this is not required for the purposes of the interview process (note below in 'Account').

- If the interviewee wishes to be accompanied, then they will need prior permission from you. Please note that this only extends to persons normally permitted to participate in the interview such as legal advisers, translators and appropriate adults.

- Professional appearance: make sure you are appropriately dressed in accordance with current ICO policy, with a neutral background and an environment free of distractions.

- Whilst there is limited access to the ICO offices, all interviews will be conducted within the office environment. In the event of no ICO office access, interviews can be conducted from domestic premises, but precautionary measures must be taken including mandatory use of 'blurred' or blank backgrounds to prevent identification of domestic premises. NOTE; that the use of 'fun' or interesting vista backgrounds is discouraged for reasons of professionalism.

- It is also important that there is a socially distanced second interviewer present as per current practice and procedure.

- Should there be a loss of connection, wait to see if the connection is re-established, keep recording and if the connection is re-established explain what has occurred and continue with the interview. Should the connection be lost, retain the recording along with all other recordings of interviews with that suspect.

- Be mindful of the health and well-being, both for yourself and the person being interviewed. Investigations are normally very stressful for all involved. Be flexible re scheduling and make sure sufficient breaks are taken.

- Should the interviewee request a short break during the interview including the opportunity to take legal advice, they should be

permitted to do so. It may be necessary for the interviewee to disconnect from the call if they are to take legal advice, however the recording should continue until they re-join the meeting and the interview can recommence.

- Interviews should generally be no longer than 45 minutes, if there is a requirement for a further interview allow time for a comfort break/for the interviewee to take legal advice. A time should be agreed to recommence the interview and on doing so normal procedures should be followed, confirming that a break has been taken and that there were no discussions about the case between the interviewer and the interviewee during that time.

Engage & Explain

- Explain that the interviewee should be alone (unless permission has been granted for a third party to be present). It will be difficult to ensure nobody else is present but what needs to be prevented is any coaching of the witness by a third party.

- Advise the interviewee they should not use the 'Chat' function in Teams. You should not respond to questions that are posed in the chat function, and instead redirect the interviewee to ask their question during the face to face recording process.

- Minimise risk of covert recordings unless agreed. Ask the person to confirm that they are not using recording devices.

- Ask the person to speak clearly and not to rely on body language i.e. nods of head etc.

Account

- Before the actual interview starts inform the interviewee that the interview is being recorded. Prior notification of this should be given in the invite letter/covering email. Microsoft Teams also informs all participants that the meeting is being recorded.

- If they object to the recording at the start or during the interview, clarify the reasons why and try to use your powers of persuasion to convince the person that it necessary to avoid face to face contact. If they continue to object, then the recording must cease and the interview concluded.

- There is no time limit on Microsoft Teams re length of interviews, however we should aim to keep each session no longer than 45 minutes to prevent issues with file size and storage in SharePoint.

- Screen share: You can use this to show the interviewee (and other attendees) any documents that you are referring to. To do this: Click on the box (with the arrow pointing upwards) located on the same bar where the mute / unmute button is. You should then be able to pull up any documents saved. Ensure all other applications and documents on your device are closed to prevent inadvertent disclosure to the participants in the meeting.

Saving Recorded Interviews

9. The recording will be downloaded to the lead investigators OneDrive (It is not uploaded into Stream). The file format will be mp4 and can uploaded onto EDRM. External attendees will not be able to view the recording.

10. The video is only available to download for the person who originated the recording. The video is downloaded to your OneDrive which again is not shared externally before being uploaded to EDRM which is only accessible to ICO staff.

11. It is the responsibility of the lead investigator to ensure that the recording is stored on EDRM in the CRiT SharePoint site at the earliest opportunity. The OneDrive copy must be deleted after the lead investigator has verified that the complete video has been uploaded without corruption. (The entire video should be watched from EDRM to ensure no corruption has taken place and before deleting the OneDrive copy).

12. The upload of a 45 minute recording to EDRM will take approximately fifteen minutes. You will be able to undertake other work on your MMD whilst this is taking place.

ENDS

Case reference

IC-203321-W1K8

Enabling Teams for Criminal Interviews – Draft DPIA

ico.
Information Commissioner's Office

Data Protection Impact Assessment Enabling Teams for Criminal Interviews

Document Name	Data Protection Impact Assessment Enabling Teams for Criminal Interviews
Author/Owner (name and job title)	Mike Shaw, Group Manager Criminal Investigations Team
Department/Team	Criminal Investigations Team, Regulatory Strategy Service
Document Status (draft, published or superseded)	Draft
Version Number	v0.1
Release Date	26.01.21
Approver (if applicable)	Steve Eckersley
Review Date	26.07.21
Distribution (internal or external)	Internal

DRAFT

Guidance for completing this template

Complete this Data Protection Impact Assessment (DPIA) template if your DPIA screening assessment indicates a high risk to individuals. If you are unsure whether you need to complete a DPIA use the **DPIA Screening Assessment** to help you decide.

Aim to complete your DPIA as early as possible as the outcome of the assessment could affect the viability of your plans. In extreme cases, you will not be able to continue with your plans without changing them, or at all.

Guidance notes are included within the template to help you with its completion- just hover your mouse over any blue text for further information.

The Information Management Service is also available for further advice and support. Please keep in mind our service standards if you require advice.

1. Process/system overview

1.1 Ownership

Project Title:	Enabling Teams for Criminal Interviews
Project Manager:	Mike Shaw
Information Asset Owner:	Stephen Eckersley
Data controller(s)	ICO
Data processor(s)	Microsoft

1.2 Describe your new service or process

This DPIA covers the use of Microsoft (MS) Teams for conducting interviews under caution.

The ICO already conducts face to face interviews, as part of the criminal investigation process. The change covered by this DPIA is to use MS teams for remote interviews. The existing process will be amended to cover the procedural changes for using MS Teams and any new information flows.

The Criminal Investigation Team are responsible for the investigation and progression of alleged criminal offences under the DPA 2018 and the FOIA 2000. Offences range in nature and include s170 DPA, the unlawful obtaining of personal data, and s77 FOIA, the concealing or destroying of information to prevent its disclosure.

Key responsibilities of the Criminal Team include:

• conducting enquiries to establish the facts of an alleged criminal offence;
• gathering evidence and producing exhibits;
• taking witness and victim statements;
• conducting suspect and witness interviews;
• producing prosecution case files for review by ICO Legal.

An interview with a suspect may be required in order to progress criminal cases to a conclusion. Unless the invitation to interview is declined by a suspect, the account they provide may identify additional lines of enquiry, or assist the ICO legal team in reaching a decision on a case whether to prosecute or not.

During the current Covid-19 pandemic it is not possible to hold face to face criminal interviews with suspects. It is not clear how long these restrictions will last and this is having a detrimental impact on the ability to progress investigations to a conclusion.

There is minimal impact on the suspect/interviewee through the use of Teams for the following reasons:

- The PD and SCD is processed in accordance with the ICO Privacy Notice and policy document 'Our processing of special categories of personal data and criminal offence data.
- Interviews with suspects are in accordance with Code C of the Police and Criminal Evidence Act (PACE 1984).
- The ability to conduct criminal interviews through the use of Teams will expedite investigations and be compliant with the Criminal Procedures and Investigations Act (CPIA 1996), thus reducing the potential for suspects to suffer from undue stress/anxiety due to prolonged investigations.
- Suspects would be invited for interview irrespective as to whether that is via a face to face interview or through the use of Teams.
- The suspect can decline to be interviewed.

Offences contrary to s77 FOIA have a six month time limit on summonses being issued, therefore there is the potential to lose cases and consequently the support and confidence of the public if we are unable to meet our statutory obligations. The use of Teams in this way also provides long-term flexibility to the ICO in progressing suspect interviews.

Meeting the six month time limit for issuing summonses in s77 FOIA cases is already challenging, as time has usually passed before the matter is referred to the criminal team. Failure to conduct an interview with a suspect will deprive them of an opportunity to provide an account of their actions, and prevent them from presenting any potential defences. It will deprive the investigator of the opportunity to challenge or test accounts, and will present an incomplete case for the ICO legal team to consider. We will be unable to fulfil our statutory responsibilities as a regulator, leading to a reduction in prosecutions and loss of confidence in the service we provide.

This presents a lost opportunity and the potential for reputational damage if the ICO is unable to investigate complaints thoroughly. The use of Teams to conduct interviews will ensure that investigators can progress their

investigations expeditiously and in accordance with the Criminal Procedures and Investigations Act (CPIA 1996).

DRAFT

1.3 Personal data inventory - explain what personal data is involved

Categories of data	Data subjects	Recipients	Overseas transfers	Retention period
Name	Suspect – member of public Legal Representative – member of public ICO Investigators Witnesses – member of public Expert witnesses – member of public	Suspect Legal Representative ICO Investigators ICO Legal Team Barristers Court	Not Applicable	Six Years, duration of sentence unless suitable for National Archives
Date of Birth	Suspect – member of public	Suspect Legal Representative ICO Investigators ICO Legal Team Barristers Court	Not Applicable	Six Years, duration of sentence unless suitable for National Archives
Contact Details	Suspect – member of public Legal Representative – member of publiclo ICO Investigators	Suspect Legal Representative ICO Investigators ICO Legal Team Barristers Court	Not Applicable	Six Years, duration of sentence unless suitable for National Archives

DRAFT

IP Address	Suspect – member of public Legal Representative – member of public ICO Investigators	ICO Microsoft	Not Applicable	Six Years, duration of sentence unless suitable for National Archives
Cookies	Suspect – member of public Legal Representative – member of public ICO Investigators	Microsoft	Not Known	Not Known
Race (Image)	Suspect – member of public Legal Representative – member of public ICO Investigators	Suspect Legal Representative ICO Investigators ICO Legal Team Barristers Court	Not Applicable	Six Years, duration of sentence unless suitable for National Archives
Ethnic Origin (Image)	Suspect – member of public Legal Representative – member of public ICO Investigators	Suspect Legal Representative ICO Investigators ICO Legal Team Barristers Court	Not Applicable	Six Years, duration of sentence unless suitable for National Archives
Political Opinions (Possible)	Suspect – member of public Witnesses – member of public	Suspect Legal Representative ICO Investigators ICO Legal Team Barristers Court	Not Applicable	Six Years, duration of sentence unless suitable for National Archives

DRAFT

Religious Beliefs (Possible)	Suspect – member of public Witnesses – member of public	Suspect Legal Representative ICO Investigators ICO Legal Team Barristers Court	Not Applicable	Six Years, duration of sentence unless suitable for National Archives
Trade Union Membership (Possible)	Suspect – member of public Witnesses – member of public	Suspect Legal Representative ICO Investigators ICO Legal Team Barristers Court	Not Applicable	Six Years, duration of sentence unless suitable for National Archives
Health Data (Possible)	Suspect – member of public Witnesses – member of public	Suspect Legal Representative ICO Investigators ICO Legal Team Barristers Court	Not Applicable	Six Years, duration of sentence unless suitable for National Archives
Criminal Convictions (Possible)	Suspect – member of public	Suspect Legal Representative ICO Investigators ICO Legal Team Barristers Court	Not Applicable	Six Years, duration of sentence unless suitable for National Archives

DRAFT

1.4 Identify a lawful basis for your processing

The Information Commissioner is named as a competent authority for the purpose of Part 3 of the DPA 2018 which applies to the processing of personal data by such authorities for law enforcement purposes.

Section 35 DPA 2018.

The processing of personal data for the facilitation of a criminal interview is based upon consent. No interview will take place unless the suspect agrees to their participation in the interview. This is confirmed in written communications with the suspect and/or their legal advisor prior to interview. This is also clarified verbally at the commencement of an interview.

Where the processing relates to sensitive personal data as outlined in s35(4) DPA 2018, the suspect, and if applicable their legal representative, will have consented as outlined above, for their participation in, and contribution to the interview.

Personal data and sensitive personal data gathered during the course of the interview will be processed as necessary for the law enforcement process.

The ICO Privacy Notice outlines the use of personal data for law enforcement processes:

https://ico.org.uk/global/privacy-notice/investigations-for-law-enforcement-purposes/

The ICO Safeguards Policy details sensitive processing for law enforcement purpose:

https://ico.org.uk/about-the-ico/our-information/safeguards-policy/

DRAFT

1.5 Explain why it is necessary to process this personal data

The Police and Criminal Evidence Act 1984 (PACE) is primarily concerned with the powers and duties of the police, the rights of suspects and the admissibility of evidence. There are several Codes of Practice including Code C – Requirements for the detention, treatment and questioning of suspects not related to terrorism in police custody, and Code E – Revised code of practice on audio recording interviews with suspects. Section 67(9) of PACE places a duty on persons other than police officers "who are charged with the duty of investigating offences or charging offenders" to have regard to any provisions of the Codes of Practice.

There is no express legal requirement that a person suspected of having committed an offence must be interviewed under caution before any decision as to whether to prosecute is taken. However, investigators do have a duty to allow a suspect the opportunity to answer the allegations against them and give their own account before a decision on prosecution is made. An interview under caution may provide:

- Important evidence against the suspect, which the investigator would otherwise be unable to obtain;
- Important information revealing further lines of enquiry;
- Relevant information to be considered in the prosecution decision

Criminal interviews form part of the investigative process. Section 22 of the Criminal Procedure and Investigations Act 2003 (CPIA) defines an investigation as an investigation conducted by police officers with a view to it being ascertained:

- Whether a person should be charged with an offence, or
- Whether a person charged with an offence is guilty of it.

ICO investigators conduct investigations in accordance with all current legislation including the CPIA.

The CPIA codes of practice state "in conducting an investigation the investigator should pursue all reasonable lines of inquiry, whether these point towards or away from the suspect. What is reasonable in each case will depend on the particular circumstances". Interviews with suspects form part of that process and all investigators are required to undertake good quality and timely investigations.

During the current Covid-19 pandemic it is not possible to hold face to face criminal interviews with suspects. It is not clear how long these restrictions will last and this is having a detrimental impact on the ability to progress investigations to a conclusion.

DRAFT

1.6 Outline your approach to completing this DPIA

Consultation has taken place with:

Regulatory Legal
Information Management
Business Development
Digital and IT Services
Business Architect
Information Security

Each suspect in a criminal investigation will be offered the opportunity to subject to a criminal interview via Teams. They may decline to do so, and any queries they may have can be addressed with them at that time. If they have concerns regarding the process then they would be offered the opportunity to be interviewed in a conventional setting when Covid-19 restrictions are lifted, or Op Volta grants approval for a conventional interview to take place.

Whilst any refusal to be interviewed via Teams would delay the progression of the case, this would be the suspect's decision and would assist the ICO in defending abuse of process arguments at a later stage.

There is a restricted, dedicated site on EDRM for the storage of the recordings. Extensive testing has taken place to identify any issues/mitigate risk.

DRAFT

2.0 Data flows

2.1 Provide a systematic description of your processing, from the point that the data is first collected through to its destruction.

If your plans involve the use of new technology you should explain how this technology works and outline any 'privacy friendly' features that are available.

The process guidance and narrative on data flow has been moved to Appendix 1 on the advice of the DPIA panel on 21.12.20.

This is the simple data flow of the process:

3.0 Key principles and requirements

Purpose & Transparency

1. Will you need to update our privacy notices?

Yes ☐ No ☒

2. If you are not updating our privacy notices how do you intend to communicate information about your processing to the data subjects?

Criminal interviews are covered in the privacy notice. The suspect and if applicable their legal advisor will be advised by the lead investigator of the requirement to use Teams, and provided with bespoke fair processing information included in our standard letters. The process is detailed in Section 2.1 of the DPIA.

3. If consent is your lawful basis for processing personal data are you maintaining appropriate records of the data subjects consent?

1. Yes ☒ No ☐ N/a ☐

4. If legitimate interests is your lawful basis for processing have you completed a legitimate interest assessment?

Yes ☐ No ☐ N/a ☒

If applicable please provide a link to your completed assessment.

N/A

Accuracy

5. Are you satisfied the personal data you are processing is accurate?

Yes ☒ No ☐

6. How will you ensure the personal data remains accurate for the duration of your processing?

This is a live recording that is not subject to any digital interference. The suspect and if applicable their legal advisor are entitled to a copy of the recording, and the recording may later be used in Court proceedings.

7. If the personal data isn't being obtained directly from the data subject what steps will you take to verify accuracy?

Not applicable with regards to the suspect.

DRAFT

Minimisation, Retention & Deletion

8. Have you done everything you can to minimise the personal data you are processing?

Yes ☒ No ☐

9. How will you ensure the personal data are deleted at the end of the retention period?

As per current ICO policy.

10. Will you need to update the retention and disposal schedule?

Yes ☐ No ☒

Integrity and confidentiality

11. Where will the personal data be stored?

ICO systems: EDRM Interviewer OneDrive until deleted.

12. Are there appropriate access controls to keep the personal data secure?

Yes ☒ No ☐

13. Have you contacted the cyber security team for a security assessment of your plans?

Yes ☒ No ☐ N/a ☐

If applicable please provide a link to any assessment.

The assessment is being completed separately.

14. Please explain the policies, training or other instructions you intend to put in place to enable staff to operate the new system or process securely.

DRAFT

Criminal Team staff are already familiar with the use of Crimson and EDRM. A guide has been prepared as outlined in part at s2.1. A full copy will be supplied with the DPIA. A number of the Criminal Team staff have been involved in the testing of the system and all staff will be briefed prior to using Teams for the first time for criminal interviews.

Accountability

15. Who will be the Information Asset Owner for this personal data?

Director of Investigations

16. Will you need to update our Article 30 record of processing activities?

Yes ☐ No ☒

17. If you are using a data processor have you agreed, or will you be agreeing, a written contract with them?

Yes ☒ No ☐ N/a ☐

Individual Rights

18. Is there a means of providing the data subjects with access to the personal data being processed?

Yes ☒ No ☐

19. Can inaccurate or incomplete personal data be updated on receipt of a request from a data subject?

Yes ☒ No ☐

Note: the interview recording will be an accurate record of the interview and will not need any rectification.

20. Can we restrict our processing of the personal data on receipt of a request from a data subject?

Yes ☒ No ☐

21. Can we stop our processing of the personal data on receipt of a request from a data subject?

Yes ☒ No ☐ N/a ☐

DRAFT

22. Can we extract and transmit the personal data in a structured, commonly used and machine readable format if requested by the data subject?

Yes ☒ No ☐ N/a ☐

23. Can we erase the personal data on receipt of a request from the data subject?

Yes ☒ No ☐

DRAFT

Risk Description	Response to Risk	Risk Mitigation	Expected Risk Score		
			I	P	Total
			See Appendix 1 – Risk Assessment Criteria		
Example: *Access controls are not implemented correctly and personal data is accessible to an unauthorised third party.*	*Reduce*	*Existing mitigation: We have checked that the system we intend to procure allows us to set access permissions for different users.* *Expected mitigation: We will appoint and train a system administrator who will be responsible for implementing access controls and monitoring access. The system administrator will also audit the system periodically to review access permissions.*	*3*	*2*	*6 - medium*
Access to recording facilities on Teams	Accept	Access is restricted to staff from the Criminal Team. Only the lead interviewer who starts the recording will be able to access the recording on their OneDrive before they upload it to EDRM. The interviewee will not be able to record the interview on Teams. If any issues are encountered IThelp would be able to provide OneDrive access to a specific member of the team. IThelp would then be able to upload the data to EDRM on behalf of the Criminal Team.	1	1	1

DRAFT

MS drop cookies without consent when users land on the Teams page on a browser. This includes dropping tracking, analytics and advertising cookies. People are unable to consent to their data being used in this way	Accept	Existing: Email Microsoft to inform them that their platform is not compliant and request they look at rectifying this. Expected: Inform users of the activity on the site before sending them to it so they can make an informed (albeit not ideal) decision.	2	5	10
An attendee might share additional personal data, including SCD that may not be related to the criminal investigation.	Accept	The attendees will have agreed to the interview in the expectation that they will be sharing personal data and SCD. Clear fair processing information should be shared with all attendees so they aware what will happen to any PD shared.	1	5	5
Staff do not follow procedures when undertaking interviews	Reduce	Expected: IT will limit the recording functionality to members of the criminal team. Procedures have been drawn up on how to conduct interviews using Teams and will include instructions to provide fair processing information to attendees. The completed interview will be subject to management review. I.T. have the capability to retrieve the recording if necessary from the Lead Investigators OneDrive.	2	2	4
Unauthorised people attending interviews	Reduce	Whilst there is limited access to the ICO offices, all interviews by ICO staff will be	3	2	6

DRAFT

		conducted within the office environment. In the event of no ICO office access, measures to be taken to prevent identification of domestic premises including use of 'blurred' backgrounds. When the meeting organiser creates a Microsoft Live Event, they can choose to limit it to only specified people or groups. Only the suspect and where appropriate the legal advisor will be invited to the event. After invite for a team meeting has been sent to specific individual(s), CRIT team meeting organiser will perform a manual check that attendee is the correct person and no others are on call. If anyone else attempts to join meeting, CRIT meeting organiser will be notified. Attendees will be advised to join via web browser or teams application and not join anonymously via Dial in feature which can be revoked. The interviewer can request to see photo identification before proceedings with the interview. As per the process guidance, we will use the 'Lobby' function to hold people in a virtual waiting area while ICO investigators check who is attending the			

DRAFT

		interview, and then permit them entry to the interview once identification is confirmed.			
There is a risk that information may be shared inadvertently through the screen share function by ICO officers.	Reduce	Mitigation for this risk is the advice on screen sharing for investigators in the process and guidance document.	2	2	4

DRAFT

5.0 Consult the DPO

Guidance: Submit your DPIA for consideration by the DPIA Forum. The process to follow is here. Any recommendations from the DPOs team will be documented below and your DPIA will be returned to you. You should then record your response to each recommendation.

	Recommendation	**Date and project stage**	**Project Team Response**
1.	Clearly state the purpose of the DPIA in the opening paragraph	17/12/2020 Planning	**AC. Added to Introduction to DPIA on 21.12.20**
2.	Review lawful basis for sensitive processing in section 1.4. Is schedule 8 relevant here if processing is based on consent? (i.e. DPA s.35(4) only rather than s.35(5)).	17/12/2020 Planning	**RH. Considered section 1.4 and basis for sensitive processing in line with recommendation. All Interviews under caution are consented to by interviewee who maintains right to provide no answer to any questions put to them. With this in mind reliance in DPA s.35(4) only sufficient. Amendment made to s 1.4**
3.	Confirm with digital architect what happens to the original recording in Teams. What is the process for deletion of the recording from original Teams location once it is downloaded by Lead Investigator to their OneDrive. Clarify where it has been downloaded from and does a copy remain in this original location? Who deletes it? Update section 2.0 to clarify.	17/12/2020 Planning	**RH. Digital Architect confirms no copy held in Teams, download made automatically to OneDrive of Lead Investigator.** **Section 2.0 updated.**
4.	Add risk of accidentally sharing incorrect ICO information via screen share to section 4.0 Risk Assessment. The	17/12/2020 Planning	**AC. Added to Risk Assessment section on 21.12.20**

DRAFT

	mitigation for this risk is the advice on screen sharing for investigators in the guidance document.		
5.	Privacy Notice and compliance with Article 13 GDPR - The answer to Q1 in section 3.0 is no update to PN required however the mitigation for two identified risks is to provide fair processing information to DS. This must be completed by either an update to existing ICO PN on our website or a bespoke PN created by Investigations that is provided to DS as part of pre interview bundle.	17/12/2020 Planning	**See section 6.0 for completed action. Fair processing information included in Notice to Interviewed Persons template and to be provided to all persons invited to interview.**
6.	Add that we will use the lobby function to the mitigation measures for the risk of 'Unauthorised people attending'. Reconsider the current impact score of 1 for this risk as we think this is too low.	17/12/2020 Planning	**AC. Added to Risk Assessment section on 21.12.20. Scoring revised upwards to 6 AMBER.**
7.	Consider moving teams video conferencing instructions to an appendix in this document and include a clear data flow in section 2.0.	17/12/2020 Planning	**AC. Moved to Appendix 1 on 21.12.20. Simple data flow created at 2.0.**

6.0 Integrate the outcomes back into your plans

Guidance: Identify who is responsible for integrating the DPIA outcomes. The outcomes include any expected mitigation you need to take as identified in your risk assessment and any further actions resulting from the DPOs recommendations.

Action	**Date for completion**	**Responsibility for Action**	**Completed Date**
Fair processing information to be prepared and communicated to data subjects	By 31.1.21	RH	Draft version completed – provided to AC 13/01/21
Further consultation with digital architect regarding recommendation 3.	By 11.1.21	RH	05/01/2020. Digital Architect confirms no copy of recording held in Teams. Download made

DRAFT

			automatically to OneDrive of Lead Investigator as meeting owner. This copy is deleted following upload to EDRM.

DRAFT

7.0 Expected residual risk and sign off

Guidance: Summarise the expected residual risk below. This is any remaining risk *after* you implement all of your mitigation measures and complete all actions.

It is never possible to remove all risk so this section shouldn't be omitted or blank. If the expected residual risk remains high (e.g. red on the traffic light scoring in the Appendix) then you will need to consult the ICO as the regulator by following the process used by external organisations.

Cookies is recorded as the highest residual risk. This appears to be an anomaly because of the high probability of it happening (across all ICO MS systems) but the assessed impact is low. It is not possible to reduce this risk further without ceasing the use of MS products.

There is a residual risk the meeting could be recorded by a participant. This would be done outside the ICO controlled environment as all recording facilities have been disabled as part of the mitigation measures. The risk to the participant is assessed as low because it is their personal data, and they would be choosing to participate in the interview.

There is a residual risk that participants may share personal data not connected to the investigation during the interview. This has been assessed as medium probability but with a low impact on the participant. The risk is mitigated by providing clear fair processing information to participants in advance of the interview.

There is a residual risk that ICO staff do not follow procedures. This is mitigated, but cannot be eliminated entirely, by having a clear, accessible policy and process in place, with regular reminders forming part of the pre-interview management controls.

There is a residual risk that unintended participants attend the interviews. This is mitigated by the process requiring confirmation of identification pre and during the interview process, as well as the meeting controls in place for the lobby and meeting itself. This risk will be kept under review to assess whether additional mitigating measures are possible, and can be introduced in the light of operational experience.

There is a residual risk that ICO officers unintentionally share documents, or excerpts of documents, via screen share with participants. This is mitigated through the clear accessible process guidance on pre-interview checks, advice on screen sharing and advice on closure of other programs during interviews.

DRAFT

7.1 IAO sign off

IAO (name and role)	Date	Project Stage
Stephen Eckersley, Director of Investigations	26 January 2021	Final

8.0 Change history

Guidance: To be completed by the person responsible for delivering the system, service or process (in a project this will be the project manager).

Version	Date	Author	Change description
V0.1	24/11/2020	Mike Shaw	First Draft
V0.1	17/12/2020	Steven Johnston	DPIA Forum Recommendations added to section 5.0

Appendix 1: Risk Assessment Criteria

The following criteria are aligned with our corporate risk assessment criteria.

Impact

Impact is the consequence of a risk to the rights and freedoms of individuals being realised. Factors to consider include the financial harm or emotional distress that can be expected to occur.

Impact	Scoring criteria
Very low (1)	No discernible impact on individuals.
Low (2)	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc).
Medium (3)	Individuals may encounter significant inconveniences, which they will overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc)
High (4)	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc).
Very high (5)	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

DRAFT

Probability
Probability is the likelihood of a risk to the rights and freedoms of individuals being realised. Factors to consider include the expected frequency of occurrence, and the motivation and capability of threat sources (eg does the threat require insider knowledge and/or significant technical resources to exploit any vulnerability?).

Probability	Scoring criteria
Very low (1)	0-5% - extremely unlikely or improbable For example, the risk has not occurred before or is not expected to occur within the next three years.
Low (2)	6-20% - low but not improbable For example, the risk is expected to occur once a year.
Medium (3)	21-50% - fairly likely to occur For example, the risk is expected to occur several times a year.
High (4)	51-80% - more likely to occur than not For example, the risk is expected to occur once a month.
Very high (5)	81-100% - almost certainly will occur For example, the risk is expected to occur once a week.

Risk level
Risk level is a function of impact and probability, and is represented by a RAG rating.

Probability / Impact	Very low (1)	Low (2)	Medium (3)	High (4)	Very high (5)
Very high (5)	Amber (5)	Amber (10)	Red (15)	Red (20)	Red (25)
High (4)	Green (4)	Amber (8)	Amber (12)	Red (16)	Red (20)
Medium (3)	Green (3)	Amber (6)	Amber (9)	Amber (12)	Red (15)
Low (2)	Green (2)	Green (4)	Amber (6)	Amber (8)	Amber (10)
Very low (1)	Green (1)	Green (2)	Green (3)	Green (4)	Amber (5)

DRAFT

Risk acceptance criteria
These criteria are guidelines only, and any risk treatment decisions should be made on a case-by-case basis. For example, it may be prudent to reduce a low risk because of legal and regulatory requirements.

Risk level	Acceptance criteria
Low (Green)	Within this range risks can be routinely accepted.
Medium (Amber)	Within this range risks can occasionally be accepted but shall be kept under regular review.
High (Red)	Within this range risks shall not be accepted and immediate action is required to reduce, avoid or transfer the risk.

Appendix 2: example risks to data subjects

Guidance: The following are examples of common risks associated with the processing of personal data to assist with your risk assessment. Not all of them will apply to your processing and the list is not exhaustive – you should consider specific risks that are relevant to your plans.

- Data is processed for unspecified / unlawful purposes/ not within expectations of data subjects
- Excessive data is processed
- Data is not kept up to date
- Data is kept for longer than is necessary by us
- Data is kept for longer than is necessary by data processor
- Data processed in contravention of data subject rights
- Data subjects unable to exercise their rights
- Data stolen or modified in transit
- Data stolen or modified at rest in our premises
- Data stolen or modified at rest in data processor premises
- Data transferred overseas to a jurisdiction that does not adequately protect data subject rights
- Re-identification of pseudonymised data by data processor or third party
- Unauthorised destruction or loss of data
- Data processor network / system / online portal not secure
- Data processor fails to process data in accordance with our instructions
- Personal data of children processed without appropriate safeguards / parental authority
- Consent of data subject not freely given (for example employer / employee processing)

- The data subject is particularly vulnerable (elderly or disabled) or is there a potential imbalance of power between the individual and the data controller (employee/employer)
- Source of data poses risks re accuracy (obtained from a unverified or old list)
- Risk to accuracy of data due to matching / combining data from different sources
- Use of new technology, e.g. fingerprinting, face recognition
- Monitoring or recording individuals
- Using profiling according to characteristics or behavior
- Non-compliance with DP principles

9.0 Template Document control

Title	Data Protection Impact Assessment Template
Version	1.0
Status	First release
Owner	Information Management Service
Release date	07/10/20
Review date	07/10/22

DRAFT

Appendix 1

Access to Microsoft Teams 'meeting' recording has been provided to all members of the Criminal Team. Controlled tests have taken place to ensure the viability of the process.

The tests have been successful in a variety of circumstances, using combinations of investigators in different locations. The tests have represented one on one interviews, interviews where a suspect is represented by a legal advisor, and where there are two investigators conducting the interview. The interviews are recorded onto the lead investigators OneDrive, from where they have been successfully uploaded into the dedicated SharePoint folder. The recordings in the SharePoint folder have been viewed for accuracy.

Following consultation with the ICO Business Architect the recordings are saved directly to OneDrive. The lead investigator will be responsible for uploading into EDRM and deleting the OneDrive copy after verifying the complete video has been uploaded without corruption.

Where a copy of the interview is requested, these will either be compressed and emailed or provided on an encrypted and password protected disc or pen drive. Where interviews are downloaded onto a disc or pen drive, a master, working and additional (spare) copy will be created. The additional copy will be supplied to the legal adviser or suspect when requested. Pen drives and discs created as a result of this process will be recorded as exhibits as per the current policy, and retained securely in the exhibit store in accordance with current practice, procedure and legislation. The passing of discs or pen drives will be in accordance with current ICO security protocols.

The following is an extract from the guidance document:

Teams video conferencing instructions

1. All investigators have access to Microsoft Teams on their MMD. The use of Teams to conduct criminal interviews will not preclude the suspect from having a legal representative present, nor if appropriate a translator. However, attendees for the interview should be kept to a minimum and the interviewee should be made aware of who is permitted to be present during the interview. If there is any deviation from the agreed attendance, this should be addressed at that time, and if the issue cannot be resolved the interview should be terminated, and if possible rescheduled.

2. The success of this approach is dependent on not only the technology available to the interviewer, but also that available to the interviewee. Whilst most people have access to a smart mobile phone, laptop or

desktop computer, that will not be the case for all. The lack of access to a suitable device for the interviewee will not be considered a refusal to attend the interview. If that situation arises further consideration will be given, and if necessary the views of the Legal Team and/or Operation Volta will be sought.

3. Please note, this guidance only applies to the use of Microsoft Teams and not other similar software that may be available. The use of Microsoft Teams has been addressed in a DPIA, an SIA and has been subject to consultation and testing within the ICO.

4. You will arrange the interview by setting up a meeting using your calendar within Teams, adding the interviewees/attendees email address to the 'attendees' field. This will ensure that they receive an invite that includes a link to the Teams meeting.

5. Provide adequate notice of the interview using a formal invitation to interview. This should be also used as an opportunity to explain how the recording of the interview will work, and by providing the standard fair processing information. You will also need to provide details of, or a link to the ICO privacy policy.

6. When creating the invitation to interview please ensure that you use the Virtual Lobby facility in Microsoft Teams. This will ensure you can start recording the meeting before allowing the external attendees entry to the meeting. Details of how to set up the virtual lobby can be found through this link:

20200505
Instructions for Setup

7. Instructions on how to record in Microsoft Teams can be found in the following link:

   https://support.microsoft.com/en-us/office/record-a-meeting-in-teams-34dfbe7f-b07d-4a27-b4c6-de62f1348c24#:~:text=Record%20a%20meeting%20or%20call.%201%20Start%20or,shows%20up%20in%20the%20meeting%20chat%20...%20

8. The person receiving the invitation will then have to click on the link embedded in the email to join the meeting. They will have two options, downloading a windows app or by joining through a webpage. In neither case is there any requirement for the attendee to already have Teams installed.

DRAFT

- Video rather than audio-only should take place. This not only allows you to see facial expressions and body language of the interviewee but will prevent any issue of identification should that arise at a later stage. Interviewees may be asked to provide proof of identity by showing a drivers licence, passport or similar documents at the commencement of the interview.

- Ask the individual being interviewed to call from a private and quiet room free of distractions, and request that mobile phones are turned off. You should advise them that they can blur the background if they do not want their wider environment captured during the interview.

- You should close down all non-essential programs on your MMD device. For example, Outlook in circumstances where this is not required for the purposes of the interview process (note below in 'Account').

- If the interviewee wishes to be accompanied, then they will need prior permission from you. Please note that this only extends to persons normally permitted to participate in the interview such as legal advisers, translators and appropriate adults.

- Professional appearance: make sure you are appropriately dressed in accordance with current ICO policy, with a neutral background and an environment free of distractions.

- Whilst there is limited access to the ICO offices, all interviews will be conducted within the office environment. In the event of no ICO office access, interviews can be conducted from domestic premises, but precautionary measures must be taken including mandatory use of 'blurred' or blank backgrounds to prevent identification of domestic premises. NOTE; that the use of 'fun' or interesting vista backgrounds is discouraged for reasons of professionalism.

- It is also important that there is a socially distanced second interviewer present as per current practice and procedure.

- Should there be a loss of connection, wait to see if the connection is re-established, keep recording and if the connection is re-established explain what has occurred and continue with the interview. Should the connection be lost, retain the recording along with all other recordings of interviews with that suspect.

- Be mindful of the health and well-being, both for yourself and the person being interviewed. Investigations are normally very stressful for all involved. Be flexible re scheduling and make sure sufficient breaks are taken.

DRAFT

- Should the interviewee request a short break during the interview including the opportunity to take legal advice, they should be permitted to do so. It may be necessary for the interviewee to disconnect from the call if they are to take legal advice, however the recording should continue until they re-join the meeting and the interview can recommence.

- Interviews should generally be no longer than 45 minutes, if there is a requirement for a further interview allow time for a comfort break/for the interviewee to take legal advice. A time should be agreed to recommence the interview and on doing so normal procedures should be followed, confirming that a break has been taken and that there were no discussions about the case between the interviewer and the interviewee during that time.

Engage & Explain

- Explain that the interviewee should be alone (unless permission has been granted for a third party to be present). It will be difficult to ensure nobody else is present but what needs to be prevented is any coaching of the witness by a third party.

- Advise the interviewee they should not use the 'Chat' function in Teams. You should not respond to questions that are posed in the chat function, and instead redirect the interviewee to ask their question during the face to face recording process.

- Minimise risk of covert recordings unless agreed. Ask the person to confirm that they are not using recording devices.

- Ask the person to speak clearly and not to rely on body language i.e. nods of head etc.

Account

- Before the actual interview starts inform the interviewee that the interview is being recorded. Prior notification of this should be given in the invite letter/covering email. Microsoft Teams also informs all participants that the meeting is being recorded.

- If they object to the recording at the start or during the interview, clarify the reasons why and try to use your powers of persuasion to convince the person that it necessary to avoid face to face contact. If they continue to object, then the recording must cease and the interview concluded.

- There is no time limit on Microsoft Teams re length of interviews, however we should aim to keep each session no longer than 45 minutes to prevent issues with file size and storage in SharePoint.

- Screen share: You can use this to show the interviewee (and other attendees) any documents that you are referring to. To do this: Click on the box (with the arrow pointing upwards) located on the same bar where the mute / unmute button is. You should then be able to pull up any documents saved. Ensure all other applications and documents on your device are closed to prevent inadvertent disclosure to the participants in the meeting.

Saving Recorded Interviews

9. The recording will be downloaded to the lead investigators OneDrive (It is not uploaded into Stream). The file format will be mp4 and can uploaded onto EDRM. External attendees will not be able to view the recording.

10. The video is only available to download for the person who originated the recording. The video is downloaded to your OneDrive which again is not shared externally before being uploaded to EDRM which is only accessible to ICO staff.

11. It is the responsibility of the lead investigator to ensure that the recording is stored on EDRM in the CRiT SharePoint site at the earliest opportunity. The OneDrive copy must be deleted after the lead investigator has verified that the complete video has been uploaded without corruption. (The entire video should be watched from EDRM to ensure no corruption has taken place and before deleting the OneDrive copy).

12. The upload of a 45 minute recording to EDRM will take approximately fifteen minutes. You will be able to undertake other work on your MMD whilst this is taking place.

ENDS

DRAFT

Case reference

IC-203321-W1K8

Enabling Teams Live Broadcast and Stream - DPIA

ico.
Information Commissioner's Office

Data Protection Impact Assessment (DPIA) template

You should complete this template where there is a new (or significant change to an existing) service or process that involves the processing of personal data (whether digital or hardcopy). When dealing with an existing process, service or system **only the change should be impact assessed.**

You should start to complete the assessment at the very start of your work and plan to revisit it throughout the lifecycle. Please note that the outcome of the assessment could affect the viability of what you are planning to do. In extreme cases, you will not be able to continue with your plans without changing them, or at all.

The Information Management and Compliance team is available to assist and advise on completing this template. If required this template should be submitted to the DPSIA forum for their consideration and recommendations. For assistance or to submit a DPIA for consideration email informationmanagement@ico.org.uk.

Determining what to complete:

You should complete all aspects of **sections 1 and 2** of this form to determine if a DPIA is required.

If you answer **no** to all screening questions in section 2 a full DPIA isn't required and there is no need to complete the additional sections of this assessment (see Approval).

If you answer **yes** to any of the screening questions in section 2 you **must** complete a full DPIA. You should complete all sections of this form except for 6.3 and 6.4 (see Approval).

Approval:

If a full DPIA isn't required. Inform your IAO and retain a copy of the partially completed form (sections 1 and 2) within your department.

If a full DPIA is required, the completed form **must** be submitted to the DPSIA Forum for their consideration and recommendations.

Once complete you should send this to informationmanagement@ico.org.uk

1. Process/system overview

1.1 Summary

Project ID:	BDG 0164
Project Title:	Enabling Teams Live Broadcast and Stream
Project Manager:	Sue Shepherd

1.2 Synopsis

The ICO proposes to use Microsoft 365 additional functionality in Teams Meetings, Live Events, Stream and Forms.

We propose to extend the use of Microsoft Teams to host committee meetings, staff meetings and for training events, for both internal and external stakeholders.

We propose to introduce the use of Microsoft Live Events to broadcast content to larger online audiences, both internal and external. Live Events work best for one-to-many or few-to-many scenarios, such as in an auditorium.

Teams allows for the recording of both 'meetings' and 'live events'. In both cases, only producers of a 'live event' or the host of a Teams 'meeting' would have the ability to record the event. All recordings will automatically be stored in Microsoft Streams. Microsoft Stream is a video service that can be used to upload, view, and share videos securely. Any recording created for ICO internal viewing will be shared via Stream. Recordings of events and meetings for external viewers would be uploaded, stored and shared via YouTube, Vimeo and/or the ICO's website.

Forms may be used in conjunction with Teams 'meeting' and 'live events' to poll the audiences in order to offer a more engaging experience or collect quantitative data. No personal data will be collected through forms as it should only be used, in this context, for undertaking polls or votes.

Staff will be using existing laptop software and hardware to access these additional Microsoft 365 services. External stakeholders will access the services via a browser.

1.3 Definition of processing

Guidance: As a data controller we are required to maintain a "record of processing activities" for which we are responsible (Article 30 refers). The following table is designed to help us define the planned processing operation.

Data controller(s)	ICO
Data processor(s)	Microsoft

Joint data controllers	N/A
Purpose of processing	To deliver video content – both live and recorded – to both internal and external audiences, about the work of the ICO and seek input from delegates.
Categories of data	Email addresses, names, images & audio.
Categories of subjects	Internal viewers, internal producers, internal presenters, external presenters, external viewers
Categories of recipients	ICO, Microsoft
Overseas transfers	Data is hosted in Microsoft's UK and/or EEA data centres. We rely on the privacy shield framework for any transfers of data to Microsoft, Vimeo or Google data centres.

1.4 Purpose for processing

Guidance: State the context and business need being pursued in the processing, including the purposes, aims and the intended benefits for you, data subjects, society or others.

Internal: As an employer the ICO has an obligation to keep staff up to date on the corporate direction and changes. It also has an obligation to deliver staff training and development. As the organisation has grown the need for some of these services to be delivered online has expanded so that it can reach larger audiences and remote audiences. The recent pandemic and subsequent lockdown has meant this need is now a must have not a should have, as without the ability to deliver this information virtually and remotely – it will not be available to staff.

External: A number of the laws the ICO regulates, put an obligation on the ICO to communicate and promote guidance to stakeholders. As we live in a digital world, the expectation from stakeholders is for educational events to be held online. The ability to do this remotely e.g. presenters in separate locations has been a requirement of the ICO for a while with staff located in different areas of the country, our international work expanding and the business working closely with other organisations. The recent pandemic and subsequent lockdown has meant this is now a must have not a should have as all presenters are currently unable to be in the same locations.

1.5 Lawful basis

Guidance: State the basis on which the processing is lawful under GDPR Article 6 (consent, performance of contractual obligations to a data subject, compliance with legal obligations, protecting the vital interests of a natural person, public task or legitimate interests). If you are processing based on legitimate interests you must also complete a legitimate interests assessment.

If you are processing data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, data concerning a person's sex life or sexual orientation or data relating to criminal convictions or offences, you will

also need to state a further basis for that processing –see GDPR Article 9 and 10.

The lawful basis for processing is Article 6(1)(e) – public task.

1.6 Mandatory requirements

Guidance: Add the following requirements to your project backlog unless they do not apply (e.g. data need not be kept up to date in a system for storing old records). Section 4 can be used to check that these have been completed, particularly if delivery is not being managed as a project.

<u>Data Accuracy</u>
a) Data must be kept up to date
b) There must be means to validate the accuracy of any personal data collected
c) Inaccurate or incomplete personal data must be updated on receipt of a lawful request from the data subject

<u>Retention & Deletion</u>
d) All data collected will have a retention period
e) Data must be deleted at the end of its retention period unless required by the National Archives for permanent preservation
f) Data kept beyond the retention period will be pseudonymised
g) Personal data must be erased upon receipt of a lawful request from the data subject

<u>Information & Transparency</u>
h) The data subjects shall be provided with:
(i) The identity and contact details of the data controller;
(ii) The purposes of the processing, including the legal basis and legitimate interests pursued
(iii) Details of the categories of personal data collected
(iv) Details of the recipients of personal data

<u>Objection & Restriction</u>
i) There must be means to restrict the processing of data on receipt of a lawful request from the data subject
j) There must be means to stop the processing of data on receipt of a lawful request from the data subject

<u>Security</u>
k) Appropriate training and instructions will be put in place to enable staff to operate the new system / process securely
l) Identify an Information Asset Owner
m) Update the Information Asset Register
n) Access controls must be in place for both physical and digital records

<u>Is the data being transferred outside the UK and EEA? If so:</u>
o) The data subjects must be provided with information on where to obtain details of any safeguards over data transferred to non-GDPR compliant countries

p) Consult the DPO for additional requirements to ensure the processing is GDPR compliant.

<u>Is the data being transferred to or through another organisation? If so:</u>

q) There must be controls to ensure or monitor compliance by external organisations.

<u>Is consent or pursuit of a contract the lawful basis for an automated processing operation? If so:</u>

r) There must be a means to extract and transmit the data in a structured, commonly used and machine-readable format on receipt of a lawful request from the data subject

s) The consent must be recorded in some manner to serve as evidence

<u>Does our Privacy Notice need to be updated? If so:</u>

t) *Update the Privacy Notice*

u) Update the records of processing activities

v) There must be appropriate contracts in place with data processors / sub-contractors

2. Data protection assessment screening

Guidance: The purpose of the screening questions is to determine if a DPIA is required. As a data controller we are required to perform DPIAs where the processing is likely to result in a high risk to the rights and freedoms of individuals (Article 35 refers).

2.1 Screening questions

ID	Criteria	Y/N
1	Will the processing involve evaluation or scoring, including profiling or predicting, especially in relation to an individual's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements?	N
2	Will the processing involve automated decision making that will have a legal or similar detrimental effect on individuals? For example, decisions that lead to exclusion or discrimination.	N
3	Will the processing involve the systematic monitoring of individuals in a publicly accessible area? For example, surveillance cameras in a shopping centre or train station.	N
4	Will the processing involve sensitive personal data or data of a highly personal nature? For example, special categories of data (Article 9 refers), personal data relating to criminal convictions or offences (Article 10 refers), and personal data linked to household and private activities.	N
5	Does the processing involve large scale processing of data at a regional, national or supranational level, and which could affect a large number of data subjects?	N
6	Does the processing involve matching and combining two or more datasets that have been collected for different purposes and/or by different data controllers?	N
7	Does the processing concern vulnerable individuals who may be unable to easily give consent or object to the processing? For example, children, employees, and others who require special protection (mentally ill persons, asylum seekers, patients, the elderly).	N
8	Does the processing involve the innovative use or application of new technological or organisational solutions? For example, "Internet of Things" applications can have significant impacts on subjects' daily lives and privacy.	N
9	Does the processing prevent individuals from exercising a	N

	rights or using a service or contract? For example, where a bank screens its customers again credit reference database in order to decide whether to offer them a loan.	

*Guidance: If you answer "Yes" to one or more questions you should complete a DPIA. If you answer "No" to all questions a full DPIA is **not** required but you must still keep a record of this document as evidence that you have considered the data processing operation against the screening questions. You can save this locally in your department and it does not need to be submitted for consideration by the DPSIA forum.*

2.2 DPIA approach and consultation

Guidance: Record which parts of the DPIA you will be completing and your rationale (especially if your choices differ from the guidance above).

Explain what practical steps you will take to ensure that you identify and address the data protection risks. Include details of:

- *Who should be consulted, internally and externally? This must include the DPO's team and Cyber Security. You should also consult data subjects or their representatives unless this is not possible or appropriate – e.g. it would be disproportionate, impractical, undermine security or compromise commercial confidentiality.*
- *If data subjects (or their representatives) will not be consulted you must document the reasons for this.*
- *Consider whether consultation with processors or sub-processors is needed.*
- *How you will carry out the consultation. You should link this to the relevant stages of your project management process or delivery plan.*

Although the screening questions indicate a DPIA isn't required we have decided to complete a full DPIA to consider any risks to data subjects associated with our plans.

Consultation:

The project team will consult the Cyber Security and Information Management Services.

The ICO Cyber team has reviewed the security of these platforms and produced a Security Opinion Report – AOR 000026 v1.0 dated 9/6/20, with the Director of Digital, IT and Business Services, and Head of BD and IT accepting outstanding risks.

Microsoft will be consulted if risks, concerns or queries about the software arise during the DPIA process.

Due to the small amount of data being processed and the standard use of well-known technology, it is deemed to be disproportionate to consult with the data subjects.

3. Data inventory

3.1 Information flows

Guidance: Provide a systematic description of the processing, including:
- *What personal data is collected*
- *The specific purpose of your processing*
- *The source of the data (including whether the data subjects are vulnerable, the relationship with the data subjects, the manner of collection and the level of control the data subjects have over the data once collected)*
- *The nature and context of the processing (including whether there are new technological developments or any relevant current issues of public concern)*
- *The scope of the processing (including the nature and volume of data, frequency and duration of processing, sensitivity of the data and the extent of the processing)*
- *The storage and transfer of the data (including details of hardware, software, networks, key people and details of any paper records or transmission channels)*
- *Responsibilities for the data (including the information asset owners, how responsibilities for information change through the data flow and the boundaries of responsibilities in any handover)*

You may find it useful to refer to a flow diagram or other way of explaining information flows. You should also say how many individuals are likely to be affected by the processing of personal data.

General background information on Microsoft Teams

Microsoft Teams 'meeting' functionality is already available to all ICO staff and is used for internal meetings. But the recording feature and 'Live Events' functionality is not currently in use. We intend to make this available but only to a restricted group of staff.

Access to Microsoft Teams 'Live Events' and 'meeting' recording will be controlled by two teams; Communications and Workforce Development and Planning (WD&P). Any member of staff contacting the IT Help team for access will be directed to one of these teams for approval. Any access granted from outside of the nominated staff in these teams will be temporary access for the period required for the task.

When a meeting organiser creates a Microsoft Teams 'Live Event', they can choose for it to be a public event, an internal event (where only ICO colleagues can join), or they can limit it further to only specified people or groups.

When a meeting organiser creates a Teams 'meeting' they can choose to use a lobby function to screen attendees before allowing them to join the meeting. They can also choose to use an attendee report if required. It has not yet been decided if these functions will be used or in what circumstance.

For ‘live events’ external participants may choose to join this anonymously or as an ‘invited person’. If a participant chooses to join anonymously then the event organiser/administrator would only see ‘anonymous’ and if an attendee report was being generated this would only show ‘anonymous’. External participants to Teams ‘meetings’ must either sign in to Teams or join as a guest by providing their name. They cannot join a Teams ‘meeting’ anonymously.

A recording of the audio and visual elements and the Q&A is captured after any Microsoft ‘Live Event’ is held. For live events the audio and visual elements are limited to the presenter as attendees feeds are switched off. However if an attendee engages with the Q&A function their comments will form part of the final recording.

Recordings are stored in both Microsoft Teams (in the post meeting material section of the original event entry) and stored in Microsoft Stream - in an Azure secure environment. A meeting organiser can also choose to record a Microsoft Teams ‘Meeting’, which would also be stored via Stream.

There is currently no automated deletion facility in Microsoft Stream, this will need to be done manually and will be the responsibility of the event organiser. Any recordings created for Communications purposes must be deleted after 12 months by a member of the Digital and Creative team. A member of WD&P must delete recordings created for learning and development purpose. For training purposes this will be six years after it’s superseded. For knowledge sharing purposes it will be 12 months after last action. The IT department will also have access to remove recordings after their designated retention period.

When recording in a Microsoft Team ‘Meeting’ there is functionality to stop and start the video recording, but when in a ‘Live Event’ this functionality is not available as it is recording the live event. Microsoft Streams does allow the editing of the beginning and ending of the video stream, but not in the main body of the video. There is no intention to edit the recordings after the event to remove personal data before sharing on third party platforms like YouTube or Vimeo. This would require additional software which we don’t currently have.

Within the chat function on a Teams ‘meeting’, there is a feature to share documents via OneDrive. If a staff member shares a OneDrive document via the chat function – external candidates can see the document in the chat function but they cannot access it. If the meeting organiser wishes to share a document with external attendees, then the document would be sent out as an attachment to the email containing the invite.

Chat messages are held in a hidden folder in Outlook and will be subject to a 7 day retention period, these are only searchable by IT administrators.

Q&A’s from a Microsoft Teams Live Event are available to the producers and presenters of the event after its conclusion. There is currently no automated

deletion of these Q&A's; they will be retained in line with the recording of the event.

What personal data will be collected

For all meetings and live events we will process the names and email addresses of attendees for the purpose of facilitating access to the meeting or event.

Where recording is taking place this is being carried out for the purpose of sharing the meeting or event more widely. This may be internally for the benefit of ICO staff or we may publish the recording on our website, Youtube or Vimeo channels for public viewing.

In a Teams 'meeting' the recording will capture the attendees audio and image if they choose to have their mic and camera turned on. If they were to disclose any personal information, views or opinions verbally or in the meeting text chat this would also form part of the recording.

For 'Live events' the audio and visual elements are limited to the presenter as attendees audio and video feeds are switched off. Live events may feature a moderated Q&A. If attendees choose to interact with the Q&A their comments can be published by the moderator to others at the event and published comments will also form part of the final recording.

When people access the ICO's live events and meetings via a browser Microsoft set Google Analytics cookies and targeting/advertising cookies. We have no control over what cookies are dropped or how and have no access to the information collected by them.

Source of the data

We already process staff names and email addresses; they will enter a meeting or live event via their organisational MS account. All other personal data will be collected directly from data subjects if they provide it to us.

The scope of the processing

The data is minimal and not sensitive. The data will only be processed when a meeting or event, that the data subject has expressed an interest in attending, is taking place.

Presenters of live events will be expected to have their audio and cameras on when delivering an event and will have their image captured. For attendees at 'meetings' this is optional.

Storage and transfer of data

The data will be processed through Microsoft 365 Teams, live events or Stream. It will be stored via our Azure Secure Environment. All data is hosted in a Microsoft data centre in the UK and/or EEA until it is uploaded to Stream, Youtube or Vimeo for wider sharing. We rely on the privacy shield framework for any transfers of data to Microsoft, Vimeo or Google data centres.

The retention schedules for the data will be varied based on which department in the ICO is responsible for it – however, clear retention schedules will be laid out.

In the case of an external live event, emails will be collected via the ICO's CMS Umbraco and deleted after a link to recording of the event has been sent.

Some recordings will be uploaded to YouTube, Vimeo and/or the ICO's website but will be deleted after 12 months.

Responsibilities for the data

Raymond Wong, Lead Business Development Officer is responsible for the relationship between the ICO and Microsoft.

The Communications and WD&P services will oversee access to live events and the recording functionality in meetings. Hannah Smith will be the lead contact for Communications and Deborah Toone will be the lead contact for WD&P.

3.2 Data inventory

Guidance: Identify the personal data to be held, the recipients (those with access to the data), the retention period and the necessity of the data collection, processing and retention.

Data Type	Recipients	Retention Period	Necessity
Email addresses of attendees	Event organiser(s) and IT support	Variable dependant on event – could be a reoccurring meeting	To invite attendees to event and in the case of a closed meeting validate attendees
Image of attendees or presenters	Event organisers, IT support, attendees, presenters and viewers	Any recording created for the communication teams purposes will be deleted after 12 months. Any recording created for workforce development and planning purposes will be deleted 6 years after superseded. Knowledge sharing purposes will be	Presenters: to deliver a live event Attendees: The attendee can chose not to have their image captured if they chose. They will need to be informed ahead of a meeting if it is going to be recorded and published more widely after the event in order to make an informed decision.

		deleted 12 months after last action	
Additional data shared verbally or in Q&A	Event organisers, IT support, attendees, presenters and viewers	As above.	Before any event attendees should be encouraged not to share personal data in these ways and informed if it will be recorded and shared. In the case of the moderated Q&As – moderators should be briefed to consider carefully whether to share comments with PD in them and instructed never to share comments with SCD in them.
Cookies – data collected by Microsoft from attendees joining via web browser	External attendees	Not known.	Microsoft set Google Analytics cookies and targeting/advertising cookies. We have no control over what cookies are dropped or how and have no access to the information collected by them.

4. Compliance measures

Guidance: Use this section to record your compliance with the requirements in section 1.6. Fill in the details of how the requirements have been met. The requirement source is a reference to GDPR unless otherwise stated.

Requirement	**Implementation Details**
Data Accuracy	
a) Data must be kept up to date	Contact email addresses can be updated with ease. Recordings will not need to be updated as they will be an accurate recording of the meeting or event.
b) There must be means to validate the accuracy of any personal data collected	It is expected that personal data will be limited to name, email address and maybe company name and the attendee will be providing the details themselves so these will be accurate. Recordings will be an accurate recording of the meeting or event.
c) Inaccurate or incomplete personal data must be updated on receipt of a lawful request from the data subject	Email addresses can be updated at any time prior to an event or meeting. It will not be possible to update event recordings.
Retention & Deletion	
d) All data collected will have a retention period	Any recording created for communication purposes will be deleted after 12 months. A recording created for learning and development for: Training purposes will be deleted 6 years after superseded Knowledge sharing purposes will be deleted 12 months after last action
e) Data must be deleted at the end of its retention period unless required by the National Archives for permanent preservation	For events created for communications purposes this is the responsibility of the communications department. For events created for learning and development purposes this is the responsibility of L&D.
f) Data kept beyond the retention period will be pseudonymised	N/A
g) Personal data must be erased upon receipt of a lawful request from the data subject	For events created for communications purposes this is the responsibility of the communications department. For events created for learning and development purposes this is the responsibility of L&D.
Information & Transparency	
h) The data subjects shall be	Covered in the Privacy Notice and we will

provided with: ● the identity and contact details of the data controller; ● the contact details of the Data Protection Officer; ● the purposes of the processing, including the legal basis and legitimate interests pursued ● details of the categories of personal data collected ● details of the recipients of personal data	consider if additional fair processing information is required for each meeting / event.
<u>Objection & Restriction</u>	
i) There must be means to restrict the processing of data on receipt of a lawful request from the data subject	For events created for communications purposes this is the responsibility of the communications department. For events created for learning and development purposes this is the responsibility of L&D.
j) There must be means to stop the processing of data on receipt of a lawful request from the data subject	For events created for communications purposes this is the responsibility of the communications department. For events created for learning and development purposes this is the responsibility of L&D.
<u>Security</u>	
k) Appropriate training and instructions will be put in place to enable staff to operate the new system / process securely	Teams meeting, Live Events and Streaming guidance and training to be created and maintained.
l) Identify an Information Asset Owner	Director of Communications & Director of Resources.
m) Update the Information Asset Register	TBC
n) Access controls must be in place for both physical and digital records	L&D and Communications will be the only departments in the ICO with Streams channels. Only certain members of the relevant teams in those departments will be granted access to add, edit or remove the meeting and event recording. IT Help will have access to all areas of Stream as the owners of the 365 apps. Only members of the communications department have access to the ICO corporate Vimeo and YouTube channels. A policy is in place to update the passwords to these platforms quarterly and/or when a

	member of the team leaves the ICO.
Conditional Requirements	
o) The data subjects must be provided with information on where to obtain details of any safeguards over data transferred to non-GDPR compliant countries	Covered in the Privacy Notice.
p) Consult the DPO for additional requirements to ensure the processing is GDPR compliant.	The DPO's advice shall be sought as part of the DPIA process
q) There must be controls to ensure or monitor compliance by external organisations.	N/A
r) There must be a means to extract and transmit the data in a structured, commonly used and machine-readable format on receipt of a lawful request from the data subject	N/A
s) Any consent must be recorded in some manner to serve as evidence	N/A
t) Update the Privacy Notice	A new Privacy Notice will be drafted.
u) Update the Article 30 Records of Processing Activities	To be updated by the Information Management Service.
v) There must be appropriate contracts in place with data processors / sub-contractors	Contracts are in place with Microsoft for Office 365.

5. Data protection summary risk assessment

Guidance: Record a summary of identified and assessed risks to data subjects' rights, the actions you have taken (existing) and could take (expected) to reduce the risks. Detail any future steps that will be necessary (eg the production of new guidance or security testing for new systems). Some example risk sources have been listed to aid you below and in Appendix 2. The examples are not exhaustive. Equally not all will be relevant to your specific processing activities. See Appendix 1 for guidance on assessing impact and probability.

Risks should be considered from the data subject's perspective not the ICO's (eg a reputational risk to the ICO should not be recorded here). Some example threats to consider include:

- *Discrimination*
- *Identity theft and fraud*
- *Financial loss*
- *Damage to data subjects' reputation*
- *Loss of confidentiality of professional secrets*
- *Unauthorised reversal of pseudonymisation*
- *Social or economic disadvantage*
- *Deprivation of legal rights or freedoms*
- *Data subjects losing control over their data*
- *Loss of privacy or intrusion into private life*
- *Prevention from accessing services*

Risk Description	**Response to Risk**	**Risk Mitigation**	**Expected Risk Score**		
			I	**P**	**Total**
[Guidance: Describe the cause and likelihood of; and the threat to the data subjects rights, and the impact on the data subject should the risk be realised- 3 elements]	*[Guidance: Describe risk treatment (e.g. reduce, avoid, accept or transfer)]*	*[Guidance: Describe existing activity and controls to reduce risk and any further activity or controls to be taken that are expected to reduce the risk- 2 elements]*	*[Guidance: I is impact score and P is probability score and IxP is the Total Score. Probability is the likelihood of the risk being realised after Risk Mitigations have been achieved.*		

MS drop cookies without consent when users land on the Teams page on a browser. This includes dropping tracking, analytics and advertising cookies. People are unable to consent to their data being used in this way	Accept	Existing: Email Microsoft to inform them that their platform is not compliant and request they look at rectifying this. Expected: Inform users of the activity on the site before sending them to it so they can make an informed (albeit not ideal) decision.	2	5	10
An attendee might share personal data, including SCD verbally or via the Q&A function	Reduce	Expected: Producers of live events should be briefed about what to do in instances where PD is shared via Q&As. It should be at the producers discretion as to whether it is shared with the group, unless it is SCD in which case it should always be deleted. Instructions should be sent to presenters and attendees advising them not to share PD. Clear fair processing information should be shared with all attendees and presenters so they aware what will happen to any PD shared.	2	2	4

Data is stolen or mishandled	Reduce	Existing: All data is hosted in Azure Secure environment. Security assessments have been completed of the platforms. Access to the information is limited. L&D and Communications will be the only departments in the ICO with Streams channels. Only certain members of the relevant teams in those departments will be granted access to add, edit or remove the meeting and event recording. IT Help will have access to all areas of Stream as the owners of the 365 apps. Only members of the communications department have access to the ICO corporate Vimeo and YouTube channels. A policy is in place to update the passwords to these platforms quarterly and/or when a member of the team leaves the ICO. The data is minimal and not sensitive	2	1	2
Staff do not follow procedures when undertaking events meaning attendees do not have access the PN, SCD is shared via the Q&A, unauthorised people access the platforms	Reduce	Expected: IT will limit the roll out recording functionality, live events and Stream to preapproved members of staff. Procedures will be drawn up about how to conduct meetings, events etc. and will include instructions to provide fair processing information to attendees.	3	2	6

An ICO staff member asks for people to share additional personal data via a form during an event	Reduce	Expected: IT will limit the roll out of forms to a small number of approved staff. Procedures will be drawn up instructing staff to only use forms to collect non-personal data.	2	1	2
Unauthorised people attending events and meetings	Reduce	Existing mitigation: When meeting organiser creates a Microsoft Live Event, they can choose for it to be a public event, an internal meeting (where only ICO colleagues can join), or they can limited it further to only specified people or groups. When a meeting organiser creates a Microsoft Teams Meeting they can use the Lobby functionality to screen people before allowing them into the meeting. Attendees must sign in to Teams or join as a guest allowing the host to see who is joining.	2	1	2

6. Expected residual risk and sign off

6.1 High and medium level expected residual risk

Guidance: Record details of the remaining risk. It is never possible to remove all risk so this section should not be omitted or blank. If the residual risk remains high (e.g. red on the traffic light scoring in the Appendix) then you will need to consult the ICO by following the process used by external organisations.

Residual risk is mostly assessed as low but there are two medium risks. We are progressing our enquiries with Microsoft regarding the non-essential cookies to try and reduce this risk. The remaining medium risk results from staff not following procedures. The necessary procedures will be drawn up and communicated to relevant staff and should be followed by staff for every meeting / live event.

6.2 Necessity and proportionality

Guidance: If you answered "Yes" to one or more of the screening questions in Section 2.1 you should discuss the necessity and proportionality of the collection, processing and retention of this data here, weighing the impact on data subjects rights and freedoms against the benefits of the processing activity. You should also consider whether there are other reasonable ways to achieve the same result with less impact on data subjects.

Necessity covered at 1.4 & 3.2.

6.3 DPO recommendations

Guidance: Record any recommendations from the DPO or their delegates and responses here. This serves as useful tool when reconsidering a rejected DPIA or in recording the justification if the organisation rejects the DPO's advice.

No	Recommendation	Project Team Response
1	Ensure appropriate measures are used to guard against unauthorised people accessing meetings For example the lobby feature should be used for all meetings.	Where a closed meeting is required, the Lobby feature will be used to only allow access to those who have registered. When only a small number of attendees are present for a meeting it is also possible for the participants list to be viewed. Appropriate measures available for guarding against unauthorised access will be noted in the Policy and Procedures

		documentation.
2	Consider procuring additional software that allows for the editing of videos we intend to publish so we can remove unnecessary personal data from recordings.	Communications team have editing software available if unnecessary personal data needs to be removed.
3	Develop the guidance referenced above as soon as possible so staff are properly trained and are using the additional functionality in a way that minimises risk.	This additional functionality will be limited to a small number of named staff. Policy and Procedures documentation is in progress to assist with guidance.
4	Continue to progress the query with Microsoft about the non-essential cookies and update this DPIA with the conclusion.	Issue has been submitted to the MS privacy portal – ref PRV0032076. Microsoft deployed a correction on May 20, 2020 which has resolved issue on App, still waiting for resolution for desktop.
5	Recordings should be reviewed before publication to check that there is no personal data or other content that it would be unfair to publish.	It will be the responsibility of the Event Producer to review any recordings for their suitability for publication, this will be noted in the Policy and Procedures documentation

6.4 Sign Off

Guidance: Send this to the DPSIA forum to consider the privacy and security risks involved in the processing, the solutions to be implemented and the residual risk.

Considered by	**Date**	**Project Stage**
DPIA Forum	01/07/2020	Planning
IAO - Jen Green, Director of Corporate Communications	15/07/2020	
IAO - Andrew Hubert, Director of Resources	10/07/2020	

7. Integrate the outcomes back into the plan

Guidance: Identify who is responsible for integrating the DPIA outcomes back into any project plan and updating any project management paperwork. Who is responsible for implementing the solutions that have been approved? Who is the contact for any data protection concerns which may arise in the future?

Action to be taken	Date for completion	Responsibility for Action	Completed Date
Policy and Procedures to be drafted	24th July 2020	Sue Shepherd	
Continue to progress with Microsoft the non-compliance cookies issue		Ray Wong	

Contact point(s) for future data protection concerns	Sue Shepherd

8. Change history

Guidance: To be completed by the person responsible for delivering the system, service or process (in a project this will be the project manager).

Version	Date	Author	Change description
0.1	01/07/2020	SS/HS/SJ	First Draft
1.0	10/07/2020	AH	Final release

9. Template Document control

Title	Data Protection Impact Assessment Template
Version	2.0
Status	Final release
Owner	DPSIA Forum
Release date	17/07/19
Review date	17/07/20

Appendix 1: Risk Assessment Criteria
The following criteria are aligned with our corporate risk assessment criteria.

Impact
Impact is the consequence of a risk to the rights and freedoms of individuals being realised. Factors to consider include the financial harm or emotional distress that can be expected to occur.

Impact	Scoring criteria
Very low (1)	No discernible impact on individuals.
Low (2)	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc).
Medium (3)	Individuals may encounter significant inconveniences, which they will overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc)
High (4)	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc).
Very high (5)	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Probability
Probability is the likelihood of a risk to the rights and freedoms of individuals being realised. Factors to consider include the expected frequency of occurrence, and the motivation and capability of threat sources (eg does the threat require insider knowledge and/or significant technical resources to exploit any vulnerability?).

Probability	Scoring criteria
Very low (1)	0-5% - extremely unlikely or improbable For example, the risk has not occurred before or is not expected to occur within the next three years.
Low (2)	6-20% - low but not improbable For example, the risk is expected to occur once a year.
Medium (3)	21-50% - fairly likely to occur For example, the risk is expected to occur several times a year.

High (4)	51-80% - more likely to occur than not For example, the risk is expected to occur once a month.
Very high (5)	81-100% - almost certainly will occur For example, the risk is expected to occur once a week.

Risk level

Risk level is a function of impact and probability, and is represented by a RAG rating.

Probability / Impact	Very low (1)	Low (2)	Medium (3)	High (4)	Very high (5)
Very high (5)	Amber (5)	Amber (10)	Red (15)	Red (20)	Red (25)
High (4)	Green (4)	Amber (8)	Amber (12)	Red (16)	Red (20)
Medium (3)	Green (3)	Amber (6)	Amber (9)	Amber (12)	Red (15)
Low (2)	Green (2)	Green (4)	Amber (6)	Amber (8)	Amber (10)
Very low (1)	Green (1)	Green (2)	Green (3)	Green (4)	Amber (5)

Risk acceptance criteria

These criteria are guidelines only, and any risk treatment decisions should be made on a case-by-case basis. For example, it may be prudent to reduce a low risk because of legal and regulatory requirements.

Risk level	Acceptance criteria
Low (Green)	Within this range risks can be routinely accepted.
Medium (Amber)	Within this range risks can occasionally be accepted but shall be kept under regular review.
High (Red)	Within this range risks shall not be accepted and immediate action is required to reduce, avoid or transfer the risk.

Appendix 2: Common risks to data subjects

The following are examples of common risks associated with the processing of personal data to assist with your risk assessment. Not all of them will apply to your processing and the list is not exhaustive – you should consider any other specific risks that may apply in relation to your intended processing.

- Data is processed for unspecified / unlawful purposes/ not within expectations of data subjects
- Excessive data is processed
- Data is not kept up to date
- Data is kept for longer than is necessary by us
- Data is kept for longer than is necessary by data processor
- Data processed in contravention of data subject rights
- Data subjects unable to exercise their rights
- Data stolen or modified in transit
- Data stolen or modified at rest in our premises
- Data stolen or modified at rest in data processor premises
- Data transferred overseas to a jurisdiction that does not adequately protect data subject rights
- Re-identification of pseudonymised data by data processor or third party
- Unauthorised destruction or loss of data
- Data processor network / system / online portal not secure
- Data processor fails to process data in accordance with our instructions
- Personal data of children processed without appropriate safeguards / parental authority
- Consent of data subject not freely given (for example employer / employee processing)
- The data subject is particularly vulnerable (elderly or disabled) or is there a potential imbalance of power between the individual and the data controller (employee/employer)
- Source of data poses risks re accuracy (obtained from a unverified or old list)
- Risk to accuracy of data due to matching / combining data from different sources
- Use of new technology, e.g. fingerprinting, face recognition
- Monitoring or recording individuals
- Using profiling according to characteristics or behavior
- Non-compliance with DP principles

Case reference

IC-203321-W1K8

Intranet Upgrade - DPIA

ico.
Information Commissioner's Office

Data Protection Impact Assessment - template

Document Name	Intranet Upgrade Data Protection Impact Assessment
Author/Owner (name and job title)	Raymond Wong, Project Manager
Department/Team	PMO
Document Status (draft, published or superseded)	Published
Version Number	V1.1
Release Date	
Approver (if applicable)	
Review Date	
Distribution (internal or external)	Internal

Privacy by design at the ICO

Welcome to the data protection impact assessment process. You should use this every time you want to implement or change a product or process. It is essential to managing your own project risks but also to managing the corporate risks of the ICO.

Responsibilities

It is your responsibility to ensure that data protection impact is taken into account during the design and build of your product or service. To do this successfully, you will need to be able to explain what your proposal is, and map out how data is used. This includes, amongst other things, where data might sit at any time geographically, but also the purpose of its use at different points in time.

Remember the basics. Key to a good assessment is knowing at all points in the process: what data you are collecting/using, why, where it will be stored and for how long, who will access it and why, how it will be kept secure and whether it's being transferred to any other country.

Your Information Asset Owner (your Director) is ultimately responsible for managing any residual risk once you have completed any mitigations to the risks you identify.

The Information Management Service, working on behalf of our DPO, can help complete the paperwork, provide compliance advice and spot risks. It is not the Service's responsibility to own, manage or mitigate the risks identified during the process.

Getting advice

You might also need advice from subject matter experts in other teams to make sure that you understand how something works or risks to what you are proposing to do. This is particularly likely if it involves new, or changing, technologies. Getting this advice will help to provide your IAO with assurance that you have understood and identified the risks.

You might well be working on a contract or agreement and a Security Opinion Report at the same time – these are also ways that you can mitigate risks and should be viewed as part of the overall assessment process.

The paperwork

You should think of this as a live document. You might change your plans or new information might come to light that changes the risk profile of your proposal. If that's the case, you should revisit the paperwork and update it to reflect any changes. You might also need to inform your IAO of new or changed risks.

The process

You should allow time for this process in your project plans. Start early! How long it takes will depend on what you're proposing, and how well you can explain it and identify risks. It can take several weeks to get the right advice and risk assessment in place.

Step 1

- Complete DPIA screening assessment. If you conclude that you do not need to complete a DPIA then you must make a record of your decision.
- If you do need to complete a DPIA then start completing the paperwork and notify the IM Service. Depending on what you're doing, the DPIA might need to be reviewed by the DPIA forum. You need to ensure the paperwork is sufficiently detailed, accurate and thorough before the forum is able to review it. This particularly applies to your descriptions of the processing activities you are proposing and how any associated technology works alongside it.
-

Step 2

- The forum is likely to provide advice and recommendations. You should consider this advice. If you decide not to follow it, then you must document your reasons why. If you do follow it, then most actions will need to be completed before go live. For example, updating privacy information or refining access controls.
- The forum is able to escalate risks to our Data Protection Officer and/or Risk and Governance Board if it is not comfortable with the processing activity being suggested or wants sign-off on advice.

When you have completed the DPIA paperwork and any actions, accepting that you might need to revisit it, you should get sign-off from your IAO before your product or service goes live.

If there are residual risks that your IAO would like to discuss, they can contact dpo@ico.org.uk. That discussion can be escalated to our Data Protection Officer and/or Risk and Governance Board if required.

Guidance for completing this template

Complete this Data Protection Impact Assessment (DPIA) template if your 'Screening Assessment - do I need to carry out a DPIA?' indicates a high risk to individuals. If you are unsure whether you need to complete a DPIA use the **screening assessment** first to help you decide.

Aim to complete your DPIA as early as possible as the outcome of the assessment could affect the viability of your plans. In extreme cases, you will not be able to continue with your plans without changing them, or at all.

Guidance notes are included within the template to help you with its completion- just hover your mouse over any blue text for further information.

The Information Management Service is also available for further advice and support. Please keep in mind our service standards if you require advice.

1. Process/system overview

1.1 Ownership

Project Title:	Intranet Upgrade
Project Manager:	Colin Crawford / Raymond Wong
Information Asset Owner:	Executive Director of Strategic Change and Transformation
Controller(s)	ICO will be the main controller, the SharePoint online intranet will include a page containing Union information only, the UNION will be the controller for this page.
Data processor(s)	Microsoft

1.2 Describe your new service or process

The purpose of the project is to upgrade the ICO ICON Intranet from an on-premise Sharepoint to Sharepoint Online. This will provide a more modern site which will be more visually appealing to colleagues and resolve a number of the current issues such as searching and finding people and information.
The modern site will be accessible, support multiple devices, be easier to maintain and provide tools to enable better management of the intranet.
The purpose of the new Intranet is essentially the same as the current ICON but upgraded to a more modern and accessible platform with the content reviewed, revised and made accessible.

1.3 Personal data inventory - explain what personal data is involved

Categories of data	Data subjects	Recipients	Overseas transfers	Retention period
Staff profiles to include names and contact information, job role profiles, photographs, interests, specialisms.	ICO Staff	All ICO colleagues	None	Profile information will be deleted when staff leave the ICO. News items will have a retention period defined in Internal Communications publishing process which is yet to be confirmed.
General intranet content about staff including information about staff members general interests.	ICO Staff	All ICO colleagues.	None	Articles will have a retention period defined.
Special category data such as data concerning health, sexuality, racial or ethnic origin, religious or philosophical beliefs, trade union membership.	ICO Staff	All ICO colleagues.	None	Articles will have a retention period defined.
Video recordings.	ICO Staff	All ICO colleagues.	None	News items will have a retention period defined.

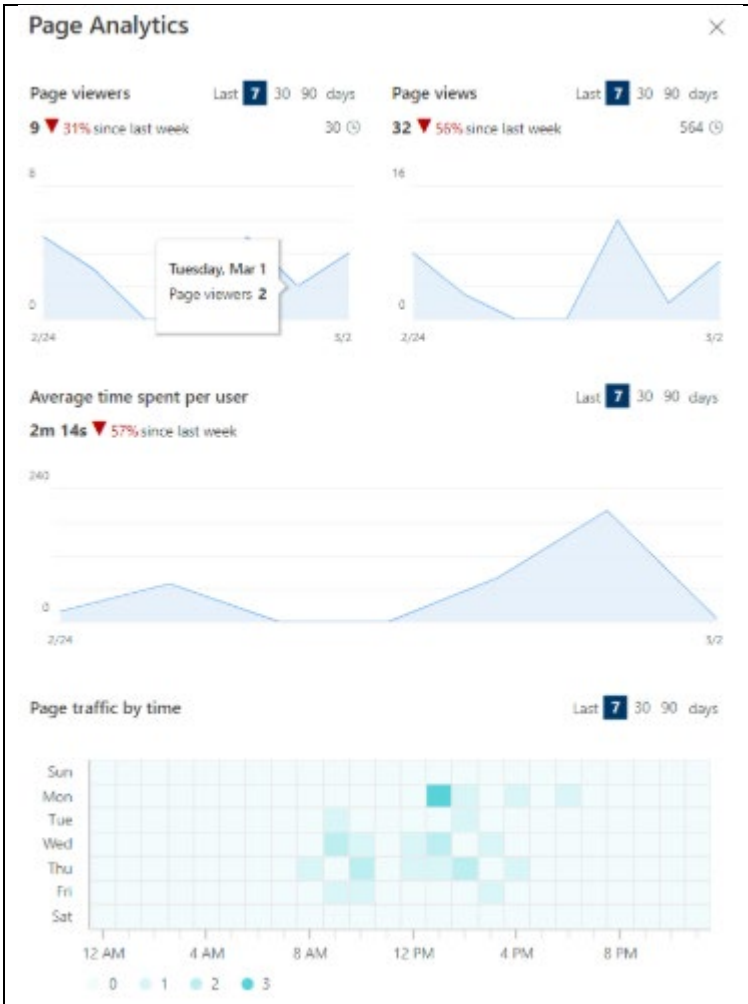
Analytics of pages and user activity is automatically recorded and can be accessed however this isn't linked to individual users (see 2.0).	ICO Staff	All ICO colleagues.	None	Analytics have a defined retention period of 90 days.
Likes, comments and other similar records of staff content interaction.	ICO Staff	All ICO Colleagues	None	This is linked to lifecycle of a page. Information is deleted when the intranet page is deleted.

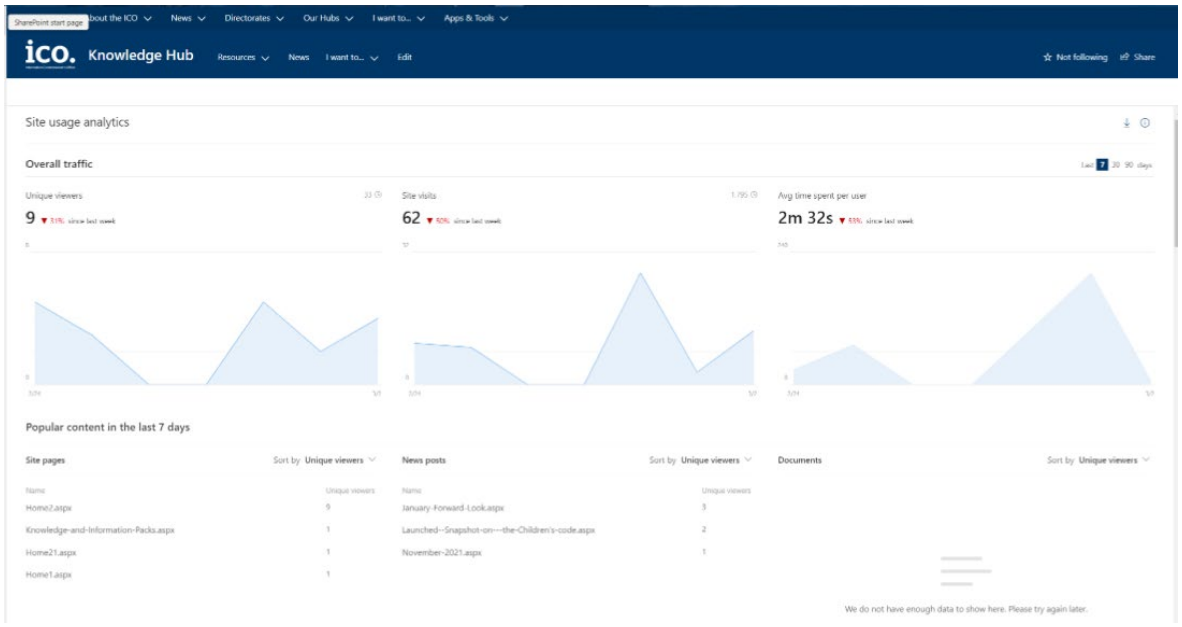
1.4 Identify a lawful basis for your processing

The lawful basis for processing staff profiles, general ICON content about individuals, their general interests, wellbeing type info, EDI content etc. is Article 6(1)(f) legitimate interests. Where this is special category data this is processed under Article 9(2)(a) explicit consent. Consent of staff where required will be collected and recorded in advance of the publication of such content on ICON. The process for this will be included in the Internal Communications publishing guidelines. The lawful basis for video recordings placed on ICON and analytics will be Article 6(1)(e) public task. Necessary for our internal communications and business analysis.

1.5 Explain why it is necessary to process this personal data

A significant element of functionality of the Intranet (from staff research) is a people finder / staff search function where a member of staff would like to find someone to contact about a particular subject. Typically by team, skill or area of expertise. Guidance will be given to staff to ensure that only work related information is stored on the staff profile in Delve. The need to publish information that may contain protected characteristics is to promote equality, diversity and inclusion using articles that may mention individuals in order to raise/increase awareness of a topic. Similarly with wellbeing articles. The purpose of processing video recordings is because they are a useful and successful way for us to promote the ICO's business and increase knowledge of particular topics to staff. In terms of analytics it is primarily site data and data relating to unique visitors rather than specific data for individuals that is gathered No personal identification information is collected for SharePoint analytics or hub usage. Attached is a screen grab of the usage data which include: Number of visits Heatmap Time of date of visits Unique visitors.

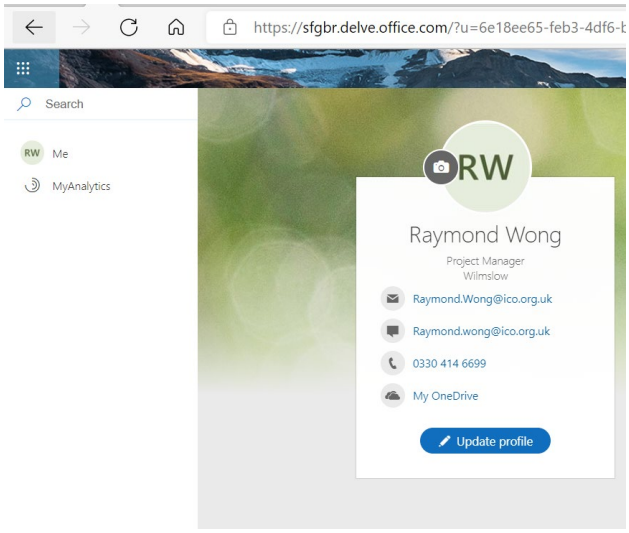




This information is necessary for the ICO to understand how our staff engage with content on our Intranet so that we can measure the success of our internal communications.

Analytic data can be re-identifed.

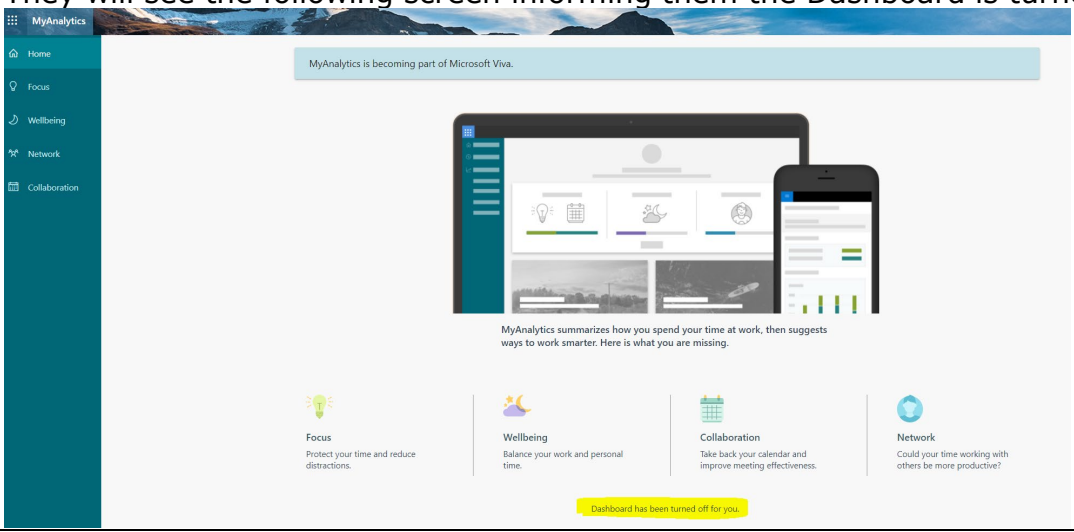
The new intranet will link through to Microsoft Delve feature.



Any images uploaded for the staff profile will NOT be shared externally in emails or any other interactions. The image will only appear for ICO staff members. Staff will be informed with Delve Guidance on usage and best practise.

Dashboard with in the "MyAnalytics" option has been turned off by default for all users.

They will see the following screen informing them the Dashboard is turned off.



1.6 Outline your approach to completing this DPIA

At the start of the project user research was conducted with ICO staff to establish what staff wanted from the intranet and needed to be improved from ICON. The output of this research has informed the requirements for the project and the personal data that will be processed.

Silicon Reef have been engaged as a SharePoint Online design and build consultant and have contributed to the art of the possible regarding our requirement with the SharePoint Online tool.

Drafted full DPIA and issued for review with intranet project team and Information Management.

Cyber security have been consulted.

Unions may need to be consulted about personal data processing if deemed necessary.

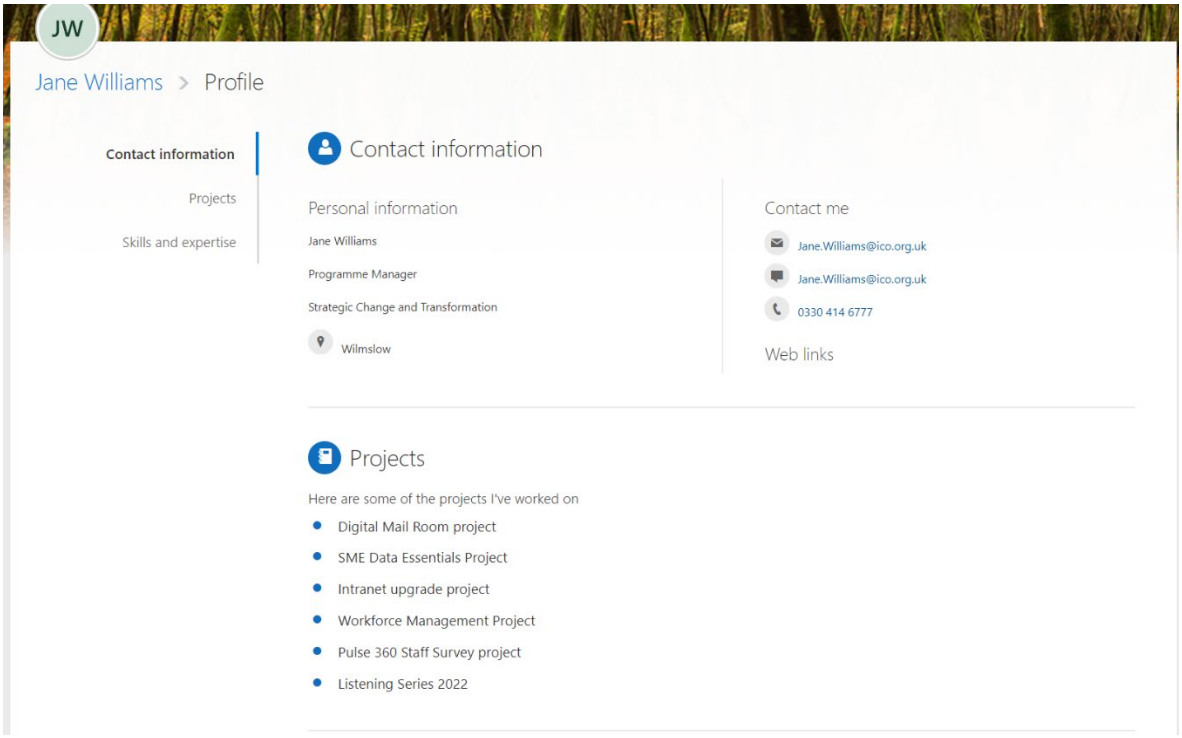
2.0 Data flows

2.1 Provide a systematic description of your processing, from the point that the data is first collected through to its destruction.

If your plans involve the use of new technology you should explain how this technology works and outline any 'privacy friendly' features that are available.

Staff profile data will be created initially in Active Directory on joining. This includes name, email, role information.

This data can be viewed and updated via Delve (and viewed in other 365 tools such as Teams) and staff will be asked to ensure that their profile is kept up to date with skills included and projects worked. An example of a Delve profile is shown below.



The staff profile in Active Directory will also be changed during any organisation changes such as new job role or line manager / direct reports. The staff profile data will be deleted from Active Directory when the individual leaves the organisation.

Content will be created and published on the Intranet, this content will in some cases identify individual staff and may include articles that identify further information including protected characteristics on those staff i.e. stories about religion or equality, diversity or inclusion. In other cases there will be news or video content that will mention individuals.

In these cases the article will be drafted which will include individuals approval where appropriate if personal information is included, the draft article will then go through an approval process before being published.

A process will be written and owned by Internal Communications that will detail the full drafting, publication and retention process using SharePoint Online tools and templates.

There will also be a governance document produced by the project team to ensure content is appropriately created and managed within the SharePoint Online environment.

As outlined above page analytics don't individually identify ICO staff. Access to this data will be managed by permissions to be set out in the governance and other process documents. This data is retained for 90 days.

ICO staff can interact with content published on the Intranet by leaving comments and "likes". This data exists for the duration of the ICON page hosting the content. Once the page is deleted this content is also deleted.

The existing Intranet contains information about members of the public; reasonable adjustments and /or any ICO restrictions on their contact with the office. It is not clear at this stage whether this will be migrated to the new Intranet. We have included this data in 1.3 for now but once this decision is made this DPIA will be revisited to identify suitable controls and compliance requirements for this data.

3.0 Key principles and requirements

Purpose & Transparency

1. Will you need to update our privacy notices?

Yes ☒ No ☐

2. If you are not updating our privacy notices how do you intend to communicate information about your processing to the data subjects?

3. If consent is your lawful basis for processing personal data are you maintaining appropriate records of the data subjects consent?

Yes ☒ No ☐ N/a ☐

4. If legitimate interests is your lawful basis for processing have you completed a legitimate interest assessment?

Yes ☒ No ☐ N/a ☐

If applicable please provide a link to your completed assessment.

https://edrm/sites/corp/im/GovAccount/_layouts/15/DocIdRedir.aspx?ID=CORP-1937519151-532

Accuracy

5. Are you satisfied the personal data you are processing is accurate?

Yes ☒ No ☐

6. How will you ensure the personal data remains accurate for the duration of your processing?

Active Directory data will be maintained by the organisation with joiner, leavers and organisational changes. There will be communications to staff to update their profiles with guidance on what information should and should not be posted. Whilst this data could get out of date over time as a person changes job role, there is an expectation that it will be reasonable accurate in the majority of cases. News items posted that refer to individuals will go through a review prior to being published so there shouldn't be any concerns regarding accuracy and they have a review/deletion date attached. All content can be amended if there is a need.

A Delve guidance document will be produced and will inform staff to periodically update their profile so the content is accurate and up to date.

7. If the personal data isn't being obtained directly from the data subject what steps will you take to verify accuracy?

Checks with individual members of staff if deemed necessary.

Minimisation, Retention & Deletion

8. Have you done everything you can to minimise the personal data you are processing?

Yes ☒ No ☐

9. How will you ensure the personal data are deleted at the end of the retention period?

The Active Directory leavers process. News items posted will have an archive/deletion date. Usage analytics will have a processing lifecycle for the past 90 days.

10. Will you need to update the retention and disposal schedule?

Yes ☒ No ☐

Integrity and confidentiality

11. Where will the personal data be stored?

ICO systems: Active Directory and MS365 Sharepoint Online.

12. Are there appropriate access controls to keep the personal data secure?

Yes ☒ No ☐

13. Have you contacted the cyber security team for a security assessment of your plans?

Yes ☒ No ☐ N/a ☐

14. Please explain the policies, training or other instructions you intend to put in place to enable staff to operate the new system or process securely.

The Intranet Upgrade project will produce guides on maintaining/configuring SharePoint Online as well as guidance on the process to approve and publish content.

Accountability

15. Who will be the Information Asset Owner for this personal data?

Executive Director of Strategic Change and Transformation

16. Will you need to update our Article 30 record of processing activities?

Yes ☒ No ☐

17. If you are using a data processor have you agreed, or will you be agreeing, a written contract with them?

Yes ☒ No ☐ N/a ☐

Note: ICO already has a contract with Microsoft.

Individual Rights

18. Is there a means of providing the data subjects with access to the personal data being processed?

Yes ☒ No ☐

19. Can inaccurate or incomplete personal data be updated on receipt of a request from a data subject?

Yes ☒ No ☐

20. Can we restrict our processing of the personal data on receipt of a request from a data subject?

Yes ☒ No ☐

21. Can we stop our processing of the personal data on receipt of a request from a data subject?

Yes ☒ No ☐ N/a ☐

22. Can we extract and transmit the personal data in a structured, commonly used and machine readable format if requested by the data subject?

Yes ☒ No ☐ N/a ☐

23. Can we erase the personal data on receipt of a request from the data subject?

Yes ☒ No ☐

4.0 Risk assessment						
Risk Description		**Response to Risk**	**Risk Mitigation**	**Expected Risk Score**		
				I	**P**	**Total**
				See Appendix 1 – Risk Assessment Criteria		
1.	Access controls are not implemented correctly where users will have access to areas not required.	Reduce	Existing mitigation: Role based access control will be implemented to ensure users will have restricted access as appropriate.	1	1	1 Low
2.	Access controls not implemented correctly allowing external access to ICO information	Reduce	Intranet is only accessible for ICO staff with security controls implemented using Azure conditional access. Guest users via teams will not be able to access the intranet. Guest accounts are regularly reviewed and access removed when no longer required.	1	1	1 Low
4.	Duplication of documents due to additional storage option for staff	Reduce	During migration from old to new intranet the old intranet will be read only. This will reduce the risk of duplication of corporate content that could impact the business. A governance document is being created to give guidance on what is an appropriate document for storage on the intranet. Staff will be advised to adhere and continue to use EDRM.	1	2	2 Low

5.	Personal data is kept longer than necessary	Reduce	Retention labels to be attached to all content stored in Intranet sites. Clear ownership of content so responsibility for managing information is clear. A governance document will be produced to outline information governance best practice which will be circulated to content / site owners. Content owner user guide will include information of what documents can be stored in SharePoint online. As part of the processed to move content from ICON to new share point online intranet, the documents will be assessed to ensure there is only a single source of that document and not duplicates.	2	2	4 Low

5.0 Consult the DPO

Guidance: Submit your DPIA for consideration by the DPIA Forum. The process to follow is here.
Any recommendations from the DPOs team will be documented below and your DPIA will be returned to you. You should then record your response to each recommendation.

	Recommendation	Date and project stage	Project Team Response
1.	**In section 1.1, the ICO will be controller for most information in the intranet however Union will be controller for Union pages. Please therefore add them as a controller to this section, clarifying that this is for the Union information only.**	Planning 10/03/2022	This has been updated as suggested.
2.	**Section 1.3, confirm whether reasonable adjustments data will be on new Intranet.**	Planning 10/03/2022	**This has been removed from DPIA as intranet will NOT contain this information.**
3.	**Section 1.4, to rely on explicit consent for processing special category data you will need to ensure that records of consent are kept. An email containing conformation from a user that they consent to processing is adequate, this should be stored centrally in EDRM.**	Planning 10/03/2022	Internal comms will include this in their processes and procedures.
4.	**Section 1.5, please add a line confirming that analytics data cannot be re-identified**	Planning 10/03/2022	This has been updated as suggested.

5.	**Section 3.6, there should be some controls put in place to ensure that Delve profiles are regularly updated to ensure that the information remains accurate, e.g. annual reminders for staff to update.**	Planning 10/03/2022	Section 3.6 has been updated with: A Delve guidance document will be produced and will inform staff to periodically update their profile so the content is accurate and up to date.
6.	**There are several sections of this document that can be updated when the governance document is finalised, particularly section 2.0, 3.9 and the risks section. Once the governance document has been signed off, please return to the DPIA and update the relevant sections and link to the governance document from section 2.0 of the DPIA.**	Planning 10/03/2022	Governance document has been completed ref: https://edrm/sites/rs/_layouts/15/DocIdRedir.aspx?ID=RESOURCE-25847047-32
7.	**LIA needs to be completed**	Planning 10/03/2022	Accept – Completed 21/03/2022
8.	**Risk 2 – suggest adding a further mitigation to implement periodic access reviews**	Planning 10/03/2022	IThelp already implement access reviews of Guest accounts. Completed 5/4/2022
9.	**Remove risk 3 – all comments will include personal data (e.g. name) so this is not a risk**	Planning 10/03/2022	Risk 3 has been removed from DPIA - Completed 5/4/2022
10.	**Risk 5 – there is a risk that duplicates of document stored in the Intranet will be stored in EDRM. There should be clear guidance for staff on what needs to be stored in the Intranet.**	Planning 10/03/2022	Mitigating risk action added: Content owner user guide will include information of what documents can be stored in SharePoint online. As part of the processed to move content from ICON to new share point online intranet, the documents will be assessed to

			ensure there is only a single source of that document and not duplicates.- in progress

6.0 Integrate the outcomes back into your plans

Guidance: Identify who is responsible for integrating the DPIA outcomes. The outcomes include any expected mitigation you need to take as identified in your risk assessment and any further actions resulting from the DPOs recommendations.

Action	Date for completion	Responsibility for Action	Completed Date
Make recommended updates to DPIA	30 June 2022	Project team	10/05/2022 - RW
Complete LIA	30 June 2022	Project team (with support from IM)	21/03/2021 - SJ
Finalise governance document and update relevant sections of the DPIA	30 June 2022	Project team (with support from IM)	10/05/2022 - RW
Update Privacy notices	30 June 2022	Project team (with support from IM)	14/04/2022 - SJ
Define retention periods for data and update retention schedule	30 June 2022	Project team (with support from IM)	30/06/2022 – RW Content label retention has been agreed with the following labels attributed to all intranet content

			(pages and documents) at the time of creation: • Corporate news content • General news content • Policy content • Team and Hub content • Project content • Inquiry content Those labels will trigger an email being sent to a designated inbox highlighting that the content needs to be reviewed: • Hub & Team content – 12 months • Policy content – 12 months • Inquiry content – 12 months • Project content – 6 months

			All news content – will have a 12 months retention with no review. The inbox will be overseen by the digital content team. When an email is received a reminder will be sent to the content owner to: • Confirm the accuracy of content. • Confirm the content can be deleted/archived. • Update the content if required.
Produce Delve guidance document	30 June 2022	Project team	05/05/2022 - RW

7.0 Expected residual risk and sign off

Guidance: Summarise the expected residual risk below. This is any remaining risk *after* you implement all of your mitigation measures and complete all actions. It is never possible to remove all risk so this section shouldn't be omitted or blank. If the expected residual risk remains high (e.g. red on the traffic light scoring in the Appendix) then you will need to consult the ICO as the regulator by following the process used by external organisations.

The intranet is built on software as a service SharePoint online. This is a continually changing platform that will offer new and retire old features. There is a small risk that feature changes will be introduced by default or current features are updated with unexpected implications. A intranet product owner is being appointed and a future content team is being considered if management of new features can be done by the ICO. Other options of working with external support service providers exist.

7.1 IAO sign off

IAO (name and role)	Date	Project Stage
Jen Green - Executive Director of Strategic Change and Transformation		Planning

8.0 Change history

Guidance: To be completed by the person responsible for completing the DPIA and delivering the system, service or process)

Version	Date	Author	Change description
V0.1	08/02/2022	C Crawford	First Draft
V0.2	5/04/2022	R.Wong	Reasonable adjustments and contact restrictions – removed from DPIA
V0.1	04/03/2022	C Crawford / R Wong / S Johnston	Amendments to draft and additional content included.
v0.1	10/03/2022	B Cudbertson	Updated sections 5 and 6 following DPIA Forum recommendations
V0.2	21/03/2022	S Johnston	3.0 Q4 changed to yes and LIA link added.
V0.3	23/3/2022	R Wong	Section 1.5 update to Delve profile pictures not appearing externally. Update on MyAnalytics feature being turned off.
V1.0	10/05/2022	R Wong	Included link to governance document and confirm PN updated by information management.
V1.1	22/06/2022	R Wong	Section 6.0 update to retention periods to include agreed content labels and review periods before deletion. All news content will have a default 12month deletion with no review.

Appendix 1: Risk Assessment Criteria

The following criteria are aligned with our corporate risk assessment criteria.

Impact

Impact is the consequence of a risk to the rights and freedoms of individuals being realised. Factors to consider include the financial harm or emotional distress that can be expected to occur.

Impact	Scoring criteria
Very low (1)	No discernible impact on individuals.
Low (2)	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc).
Medium (3)	Individuals may encounter significant inconveniences, which they will overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc)

High (4)	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc).
Very high (5)	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Probability
Probability is the likelihood of a risk to the rights and freedoms of individuals being realised. Factors to consider include the expected frequency of occurrence, and the motivation and capability of threat sources (eg does the threat require insider knowledge and/or significant technical resources to exploit any vulnerability?).

Probability	Scoring criteria
Very low (1)	0-5% - extremely unlikely or improbable For example, the risk has not occurred before or is not expected to occur within the next three years.
Low (2)	6-20% - low but not improbable For example, the risk is expected to occur once a year.
Medium (3)	21-50% - fairly likely to occur For example, the risk is expected to occur several times a year.
High (4)	51-80% - more likely to occur than not For example, the risk is expected to occur once a month.
Very high (5)	81-100% - almost certainly will occur For example, the risk is expected to occur once a week.

Risk level
Risk level is a function of impact and probability, and is represented by a RAG rating.

Probability / Impact	Very low (1)	Low (2)	Medium (3)	High (4)	Very high (5)
Very high (5)	Amber (5)	Amber (10)	Red (15)	Red (20)	Red (25)
High (4)	Green (4)	Amber (8)	Amber (12)	Red (16)	Red (20)

Medium (3)	Green (3)	Amber (6)	Amber (9)	Amber (12)	Red (15)
Low (2)	Green (2)	Green (4)	Amber (6)	Amber (8)	Amber (10)
Very low (1)	Green (1)	Green (2)	Green (3)	Green (4)	Amber (5)

Risk acceptance criteria
These criteria are guidelines only, and any risk treatment decisions should be made on a case-by-case basis. For example, it may be prudent to reduce a low risk because of legal and regulatory requirements.

Risk level	Acceptance criteria
Low (Green)	Within this range risks can be routinely accepted.
Medium (Amber)	Within this range risks can occasionally be accepted but shall be kept under regular review.
High (Red)	Within this range risks shall not be accepted and immediate action is required to reduce, avoid or transfer the risk.

Appendix 2: example risks to data subjects

Guidance: The following are examples of common risks associated with the processing of personal data to assist with your risk assessment. Not all of them will apply to your processing and the list is not exhaustive – you should consider specific risks that are relevant to your plans.

- Data is processed for unspecified / unlawful purposes/ not within expectations of data subjects
- Excessive data is processed
- Data is not kept up to date
- Data is kept for longer than is necessary by us
- Data is kept for longer than is necessary by data processor
- Data processed in contravention of data subject rights
- Data subjects unable to exercise their rights
- Data stolen or modified in transit
- Data stolen or modified at rest in our premises
- Data stolen or modified at rest in data processor premises

- Data transferred overseas to a jurisdiction that does not adequately protect data subject rights
- Re-identification of pseudonymised data by data processor or third party
- Unauthorised destruction or loss of data
- Data processor network / system / online portal not secure
- Data processor fails to process data in accordance with our instructions
- Personal data of children processed without appropriate safeguards / parental authority
- Consent of data subject not freely given (for example employer / employee processing)
- The data subject is particularly vulnerable (elderly or disabled) or is there a potential imbalance of power between the individual and the controller (employee/employer)
- Source of data poses risks re accuracy (obtained from a unverified or old list)
- Risk to accuracy of data due to matching / combining data from different sources
- Use of new technology, e.g. fingerprinting, face recognition
- Monitoring or recording individuals
- Using profiling according to characteristics or behavior
- Non-compliance with DP principles

Case reference

IC-203321-W1K8

Intune Mobile Device Management - DPIA

ico.
Information Commissioner's Office

Data Protection Impact Assessment (DPIA) template

You should complete this template where there is a new (or significant change to an existing) service or process that involves the processing of personal data (whether digital or hardcopy). When dealing with an existing process, service or system **only the change should be impact assessed.**

You should start to complete the assessment at the very start of your work and plan to revisit it throughout the lifecycle. Please note that the outcome of the assessment could affect the viability of what you are planning to do. In extreme cases, you will not be able to continue with your plans without changing them, or at all.

The Information Management and Compliance team is available to assist and advise on completing this template. If required this template should be submitted to the DPSIA forum for their consideration and recommendations. For assistance or to submit a DPIA for consideration email informationmanagement@ico.org.uk.

Determining what to complete:

You should complete all aspects of **sections 1 and 2** of this form to determine if a DPIA is required.

If you answer **no** to all screening questions in section 2 a full DPIA isn't required and there is no need to complete the additional sections of this assessment (see Approval).

If you answer **yes** to any of the screening questions in section 2 you **must** complete a full DPIA. You should complete all sections of this form except for 6.3 and 6.4 (see Approval).

Approval:

If a full DPIA isn't required. Inform your IAO and retain a copy of the partially completed form (sections 1 and 2) within your department.

If a full DPIA is required, the completed form **must** be submitted to the DPSIA Forum for their consideration and recommendations.

Once complete you should send this to informationmanagement@ico.org.uk

DRAFT

1. Process/system overview

1.1 Summary

Guidance: For projects please provide the following key details. Non-projects should provide a key contact who is responsible for delivering the system or process.

Project ID:	BDG0139
Project Title:	Intune Mobile Device Management
Project Manager:	Raymond Wong

1.2 Synopsis

Guidance: Provide a summary of the process or system including any relevant background information and the key aims/objectives that the system or process must achieve. There is no need for a detailed discussion of data or data flows – these are covered later in the assessment.

The ICO uses Microsoft Office 365 enterprise services including **Intune** Mobile device management services (MDM).

Intune MDM allows us to manage access to ICO information on portable devices such as mobiles and laptops; ensuring this is secure and reliable. Intune will be used to replace the Airwatch application that is currently used for this purpose.

Intune allows us to specify access requirements for ICO portable devices and allows IT support staff to remotely manage the device and the apps accessible from the device.

Intune offers security features to automatically configure corporate devices so they meet ICO security requirements. Access to ICO services will only be permitted once the security of the device is confirmed.

Access control is also performed to ensure users are authenticated using security device pin and application pin.

Intune remote management services offer the capability to wipe the device data in the event the device is lost.

The ICO will be using Intune in 2 scenarios for deployment.

Scenario 1 - Corporate enrolled devices:

Intune will allow selected staff access to the Microsoft suite of services on their ICO mobile phones, laptop or tablet. This includes access to applications such as Email, Word, Excel and OneDrive services for storage.

Scenario 2:

Bring your own device (BYOD)

For BYOD deployment **Intune** allows for access to the ICO **email and calendar services only** from a personal mobile device.

No corporate applications (i.e. ICON, ICE, CMEH etc) or other Microsoft cloud services like one drive will be accessible from personal devices.

Intune offers security features to create a data boundary on the personal device that prevents loss of corporate data. A data boundary prevents information to be copied and pasted from Outlook.

It is not possible for Intune to access an information such as texts, social media accounts or photos on a personal device. Only the device name will be stored.

As with ICO corporate devices Intune lets us wipe ICO email data on personal devices.

Access to ICO emails on personal mobile devices is optional and is not mandatory for staff.

Microsoft may occasionally need to access Intune for the purposes of providing technical support.

1.3 Definition of processing

Guidance: As a data controller we are required to maintain a "record of processing activities" for which we are responsible (Article 30 refers). The following table is designed to help us define the planned processing operation.

Data controller(s)	ICO
Data processor(s)	
Joint data controllers	N/A
Purpose of processing	To enable ICO employees to securely access Microsoft apps on mobile devices
Categories of data	ICO devices – User's name, device name, work phone number, device serial number, last activity date/time Personal devices – Name, work email address, device name (IOS only), last activity date/time (last time work emails were accessed on the device)
Categories of subjects	ICO employees
Categories of recipients	Microsoft
Overseas transfers	N/A

1.4 Purpose for processing

Guidance: State the context and business need being pursued in the processing, including the purposes, aims and the intended benefits for you, data subjects, society or others.

The personal data is being processed to enable Intune to security check devices before allowing them access to ICO systems. On corporately owned MMD devices the data is also being processed to enable administrators to push out apps or updates, or wipe corporate data from the device in the event that it is lost or stolen. It is necessary for Intune to store some information about each device in order to keep track of each device.

1.5 Lawful basis

Guidance: State the basis on which the processing is lawful under GDPR Article 6 (consent, performance of contractual obligations to a data subject, compliance with legal obligations, protecting the vital interests of a natural person, public task or legitimate interests). If you are processing based on legitimate interests you must also complete a legitimate interests assessment.

If you are processing data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, data concerning a person's sex life or sexual orientation or data relating to criminal convictions or offences, you will also need to state a further basis for that processing –see GDPR Article 9 and 10.

The lawful basis for this processing is article 6(1)(e) – necessary for the performance of a task carried out in the public interest.

1.6 Mandatory requirements

Guidance: Add the following requirements to your project backlog unless they do not apply (e.g. data need not be kept up to date in a system for storing old records). Section 4 can be used to check that these have been completed, particularly if delivery is not being managed as a project.

Data Accuracy

a) Data must be kept up to date
b) There must be means to validate the accuracy of any personal data collected
c) Inaccurate or incomplete personal data must be updated on receipt of a lawful request from the data subject

Retention & Deletion

d) All data collected will have a retention period
e) Data must be deleted at the end of its retention period unless required by the National Archives for permanent preservation
f) Data kept beyond the retention period will be pseudonymised
g) Personal data must be erased upon receipt of a lawful request from the data subject

Information & Transparency

h) The data subjects shall be provided with:
(i) The identity and contact details of the data controller;
(ii) The purposes of the processing, including the legal basis and legitimate interests pursued
(iii) Details of the categories of personal data collected

(iv) Details of the recipients of personal data

<u>Objection & Restriction</u>

i) There must be means to restrict the processing of data on receipt of a lawful request from the data subject

j) There must be means to stop the processing of data on receipt of a lawful request from the data subject

<u>Security</u>

k) Appropriate training and instructions will be put in place to enable staff to operate the new system / process securely

l) Identify an Information Asset Owner

m) Update the Information Asset Register

n) Access controls must be in place for both physical and digital records

<u>Is the data being transferred outside the UK and EEA? If so:</u>

o) The data subjects must be provided with information on where to obtain details of any safeguards over data transferred to non-GDPR compliant countries

p) Consult the DPO for additional requirements to ensure the processing is GDPR compliant.

<u>Is the data being transferred to or through another organisation? If so:</u>

q) There must be controls to ensure or monitor compliance by external organisations.

<u>Is consent or pursuit of a contract the lawful basis for an automated processing operation? If so:</u>

r) There must be a means to extract and transmit the data in a structured, commonly used and machine-readable format on receipt of a lawful request from the data subject

s) The consent must be recorded in some manner to serve as evidence

<u>Does our Privacy Notice need to be updated? If so:</u>

t) *Update the Privacy Notice*

u) Update the records of processing activities

v) There must be appropriate contracts in place with data processors / sub-contractors

2. Data protection assessment screening

Guidance: The purpose of the screening questions is to determine if a DPIA is required. As a data controller we are required to perform DPIAs where the processing is likely to result in a high risk to the rights and freedoms of individuals (Article 35 refers).

2.1 Screening questions

ID	Criteria	Y/N
1	Will the processing involve evaluation or scoring, including profiling or predicting, especially in relation to an individual's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements?	N
2	Will the processing involve automated decision making that will have a legal or similar detrimental effect on individuals? For example, decisions that lead to exclusion or discrimination.	N
3	Will the processing involve the systematic monitoring of individuals in a publicly accessible area? For example, surveillance cameras in a shopping centre or train station.	N
4	Will the processing involve sensitive personal data or data of a highly personal nature? For example, special categories of data (Article 9 refers), personal data relating to criminal convictions or offences (Article 10 refers), and personal data linked to household and private activities.	N
5	Does the processing involve large scale processing of data at a regional, national or supranational level, and which could affect a large number of data subjects?	N
6	Does the processing involve matching and combining two or more datasets that have been collected for different purposes and/or by different data controllers?	N
7	Does the processing concern vulnerable individuals who may be unable to easily give consent or object to the processing? For example, children, employees, and others who require special protection (mentally ill persons, asylum seekers, patients, the elderly).	N
8	Does the processing involve the innovative use or application of new technological or organisational solutions? For example, "Internet of Things" applications can have significant impacts on subjects' daily lives and privacy.	N

DRAFT

9	Does the processing prevent individuals from exercising a rights or using a service or contract? For example, where a bank screens its customers again credit reference database in order to decide whether to offer them a loan.	N

*Guidance: If you answer "Yes" to one or more questions you should complete a DPIA. If you answer "No" to all questions a full DPIA is **not** required but you must still keep a record of this document as evidence that you have considered the data processing operation against the screening questions. You can save this locally in your department and it does not need to be submitted for consideration by the DPSIA forum.*

2.2 DPIA approach and consultation

Guidance: Record which parts of the DPIA you will be completing and your rationale (especially if your choices differ from the guidance above).

Explain what practical steps you will take to ensure that you identify and address the data protection risks. Include details of:

- *Who should be consulted, internally and externally? This must include the DPO's team and Cyber Security. You should also consult data subjects or their representatives unless this is not possible or appropriate – e.g. it would be disproportionate, impractical, undermine security or compromise commercial confidentiality.*
- *If data subjects (or their representatives) will not be consulted you must document the reasons for this.*
- *Consider whether consultation with processors or sub-processors is needed.*
- *How you will carry out the consultation. You should link this to the relevant stages of your project management process or delivery plan.*

3. Data inventory

3.1 Information flows

Guidance: Provide a systematic description of the processing, including:

- *What personal data is collected*
- *The specific purpose of your processing*
- *The source of the data (including whether the data subjects are vulnerable, the relationship with the data subjects, the manner of collection and the level of control the data subjects have over the data once collected)*
- *The nature and context of the processing (including whether there are new technological developments or any relevant current issues of public concern)*
- *The scope of the processing (including the nature and volume of data, frequency and duration of processing, sensitivity of the data and the extent of the processing)*
- *The storage and transfer of the data (including details of hardware, software, networks, key people and details of any paper records or transmission channels)*
- *Responsibilities for the data (including the information asset owners, how responsibilities for information change through the data flow and the boundaries of responsibilities in any handover)*

You may find it useful to refer to a flow diagram or other way of explaining information flows. You should also say how many individuals are likely to be affected by the processing of personal data.

3.2 Data inventory

Guidance: Identify the personal data to be held, the recipients (those with access to the data), the retention period and the necessity of the data collection, processing and retention.

Data Type	**Recipients**	**Retention Period**	**Necessity**
[Description of the data held (e.g. dates of birth, addresses etc.)]	[Who will have access to the data?]	[How long will the data be held for?]	[Is the collection, processing and retention of this data necessary for the purpose pursued? You should always aim to minimise your data collection.]

DRAFT

4. Compliance measures

Guidance: Use this section to record your compliance with the requirements in section 1.6. Fill in the details of how the requirements have been met. The requirement source is a reference to GDPR unless otherwise stated.

Requirement	**Implementation Details**
Data Accuracy	
a) Data must be kept up to date	
b) There must be means to validate the accuracy of any personal data collected	
c) Inaccurate or incomplete personal data must be updated on receipt of a lawful request from the data subject	
Retention & Deletion	
d) All data collected will have a retention period	
e) Data must be deleted at the end of its retention period unless required by the National Archives for permanent preservation	
f) Data kept beyond the retention period will be pseudonymised	
g) Personal data must be erased upon receipt of a lawful request from the data subject	
Information & Transparency	
h) The data subjects shall be provided with: ● the identity and contact details of the data controller; ● the contact details of the Data Protection Officer; ● the purposes of the processing, including the legal basis and legitimate interests pursued ● details of the categories of personal data collected ● details of the recipients of personal data	
Objection & Restriction	
i) There must be means to restrict the processing of data on receipt of a lawful request from the data subject	
j) There must be means to stop the processing of data on receipt of a lawful request from the data subject	
Security	
k) Appropriate training and instructions will be put in place to enable staff to operate the new system / process securely	
l) Identify an Information Asset Owner	
m) Update the Information Asset Register	
n) Access controls must be in place for both physical and digital records	
Conditional Requirements	
o) The data subjects must be provided with information on where to obtain details of any safeguards over data transferred to non-GDPR compliant countries	
p) Consult the DPO for additional requirements to ensure the processing is GDPR compliant.	

DRAFT

q) There must be controls to ensure or monitor compliance by external organisations.	
r) There must be a means to extract and transmit the data in a structured, commonly used and machine-readable format on receipt of a lawful request from the data subject	
s) Any consent must be recorded in some manner to serve as evidence	
t) Update the Privacy Notice	
u) Update the Article 30 Records of Processing Activities	
v) There must be appropriate contracts in place with data processors / sub-contractors	

DRAFT

5. Data protection summary risk assessment

Guidance: Record a summary of identified and assessed risks to data subjects' rights, the actions you have taken (existing) and could take (expected) to reduce the risks. Detail any future steps that will be necessary (eg the production of new guidance or security testing for new systems). Some example risk sources have been listed to aid you below and in Appendix 2. The examples are not exhaustive. Equally not all will be relevant to your specific processing activities. See Appendix 1 for guidance on assessing impact and probability.

Risks should be considered from the data subject's perspective not the ICO's (eg a reputational risk to the ICO should not be recorded here). Some example threats to consider include:

- *Discrimination*
- *Identity theft and fraud*
- *Financial loss*
- *Damage to data subjects' reputation*
- *Loss of confidentiality of professional secrets*
- *Unauthorised reversal of pseudonymisation*
- *Social or economic disadvantage*
- *Deprivation of legal rights or freedoms*
- *Data subjects losing control over their data*
- *Loss of privacy or intrusion into private life*
- *Prevention from accessing services*

DRAFT

Risk Description	Response to Risk	Risk Mitigation	Expected Risk Score		
			I	P	Total
[Guidance: Describe the cause and likelihood of; and the threat to the data subjects rights, and the impact on the data subject should the risk be realised- 3 elements]	*[Guidance: Describe risk treatment (e.g. reduce, avoid, accept or transfer)]*	*[Guidance: Describe existing activity and controls to reduce risk and any further activity or controls to be taken that are expected to reduce the risk- 2 elements]*	*[Guidance: I is impact score and P is probability score and IxP is the Total Score. Probability is the likelihood of the risk being realised after Risk Mitigations have been achieved.*		
Example: *(cause)There are no access restrictions to the IT network presenting a risk that (threat) sensitive financial data is stolen or modified in our premises resulting in (impact) potential significant consequences and difficulties to data subjects such as loss of funds.*	*Reduce*	*Existing mitigation: Physical security restrictions preventing access to building and therefore network.* *Expected mitigation: New network firewall and password security with encryption to be added before data is input onto system.*	*4*	*2*	*8*

DRAFT

6. Expected residual risk and sign off

6.1 High and medium level expected residual risk

Guidance: Record details of the remaining risk. It is never possible to remove all risk so this section should not be omitted or blank. If the residual risk remains high (e.g. red on the traffic light scoring in the Appendix) then you will need to consult the ICO by following the process used by external organisations.

6.2 Necessity and proportionality

Guidance: If you answered "Yes" to one or more of the screening questions in Section 2.1 you should discuss the necessity and proportionality of the collection, processing and retention of this data here, weighing the impact on data subjects rights and freedoms against the benefits of the processing activity. You should also consider whether there are other reasonable ways to achieve the same result with less impact on data subjects.

6.3 DPO recommendations

Guidance: Record any recommendations from the DPO or their delegates and responses here. This serves as useful tool when reconsidering a rejected DPIA or in recording the justification if the organisation rejects the DPO's advice.

No	Recommendation	Project Team Response
1	[Record any changes recommended by the DPO here]	[Record the actions taken as a result of the recommendation]

6.4 Sign Off

Guidance: Send this to the DPSIA forum to consider the privacy and security risks involved in the processing, the solutions to be implemented and the residual risk.

Considered by	Role	Date	Project Stage
	DPO		
	Head of Cyber Security		
	[Add others as necessary]		

7. Integrate the outcomes back into the plan

Guidance: Identify who is responsible for integrating the DPIA outcomes back into any project plan and updating any project management paperwork. Who is responsible for implementing the solutions that have been approved? Who is the contact for any data protection concerns which may arise in the future?

Action to be taken	Date for completion	Responsibility for Action	Completed Date

Contact point(s) for future data protection concerns	

8. Change history

Guidance: To be completed by the person responsible for delivering the system, service or process (in a project this will be the project manager).

Version	Date	Author	Change description

9. Template Document control

Title	Data Protection Impact Assessment Template
Version	2.0
Status	Final release
Owner	DPSIA Forum
Release date	17/07/19
Review date	17/07/20

DRAFT

Appendix 1: Risk Assessment Criteria
The following criteria are aligned with our corporate risk assessment criteria.

Impact
Impact is the consequence of a risk to the rights and freedoms of individuals being realised. Factors to consider include the financial harm or emotional distress that can be expected to occur.

Impact	Scoring criteria
Very low (1)	No discernible impact on individuals.
Low (2)	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc).
Medium (3)	Individuals may encounter significant inconveniences, which they will overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc)
High (4)	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc).
Very high (5)	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Probability
Probability is the likelihood of a risk to the rights and freedoms of individuals being realised. Factors to consider include the expected frequency of occurrence, and the motivation and capability of threat sources (eg does the threat require insider knowledge and/or significant technical resources to exploit any vulnerability?).

Probability	Scoring criteria
Very low (1)	0-5% - extremely unlikely or improbable For example, the risk has not occurred before or is not expected to occur within the next three years.
Low (2)	6-20% - low but not improbable For example, the risk is expected to occur once a year.
Medium (3)	21-50% - fairly likely to occur For example, the risk is expected to occur several times a year.

DRAFT

High (4)	51-80% - more likely to occur than not For example, the risk is expected to occur once a month.
Very high (5)	81-100% - almost certainly will occur For example, the risk is expected to occur once a week.

Risk level

Risk level is a function of impact and probability, and is represented by a RAG rating.

Probability / Impact	Very low (1)	Low (2)	Medium (3)	High (4)	Very high (5)
Very high (5)	Amber (5)	Amber (10)	Red (15)	Red (20)	Red (25)
High (4)	Green (4)	Amber (8)	Amber (12)	Red (16)	Red (20)
Medium (3)	Green (3)	Amber (6)	Amber (9)	Amber (12)	Red (15)
Low (2)	Green (2)	Green (4)	Amber (6)	Amber (8)	Amber (10)
Very low (1)	Green (1)	Green (2)	Green (3)	Green (4)	Amber (5)

Risk acceptance criteria

These criteria are guidelines only, and any risk treatment decisions should be made on a case-by-case basis. For example, it may be prudent to reduce a low risk because of legal and regulatory requirements.

Risk level	Acceptance criteria
Low (Green)	Within this range risks can be routinely accepted.
Medium (Amber)	Within this range risks can occasionally be accepted but shall be kept under regular review.
High (Red)	Within this range risks shall not be accepted and immediate action is required to reduce, avoid or transfer the risk.

Appendix 2: Common risks to data subjects

The following are examples of common risks associated with the processing of personal data to assist with your risk assessment. Not all of them will apply to your processing and the list is not exhaustive – you should consider any other specific risks that may apply in relation to your intended processing.

- Data is processed for unspecified / unlawful purposes/ not within expectations of data subjects
- Excessive data is processed
- Data is not kept up to date
- Data is kept for longer than is necessary by us
- Data is kept for longer than is necessary by data processor
- Data processed in contravention of data subject rights
- Data subjects unable to exercise their rights
- Data stolen or modified in transit
- Data stolen or modified at rest in our premises
- Data stolen or modified at rest in data processor premises
- Data transferred overseas to a jurisdiction that does not adequately protect data subject rights
- Re-identification of pseudonymised data by data processor or third party
- Unauthorised destruction or loss of data
- Data processor network / system / online portal not secure
- Data processor fails to process data in accordance with our instructions
- Personal data of children processed without appropriate safeguards / parental authority
- Consent of data subject not freely given (for example employer / employee processing)
- The data subject is particularly vulnerable (elderly or disabled) or is there a potential imbalance of power between the individual and the data controller (employee/employer)
- Source of data poses risks re accuracy (obtained from a unverified or old list)
- Risk to accuracy of data due to matching / combining data from different sources
- Use of new technology, e.g. fingerprinting, face recognition
- Monitoring or recording individuals
- Using profiling according to characteristics or behavior
- Non-compliance with DP principles

DRAFT

Case reference

IC-203321-W1K8

Machine Learning – Text Classification - DPIA

ico.
Information Commissioner's Office

Data Protection Impact Assessment - template

Document Name	Machine Learning – Text classification- Data Protection Impact Assessment
Author/Owner (name and job title)	Raymond Wong, Project Manager
Department/Team	Business Development Group
Document Status (draft, published or superseded)	
Version Number	1.0
Release Date	19/05/2021
Approver (if applicable)	
Review Date	
Distribution (internal or external)	Internal

Guidance for completing this template

Complete this Data Protection Impact Assessment (DPIA) template if your 'Screening Assessment - do I need to carry out a DPIA?' indicates a high risk to individuals. If you are unsure whether you need to complete a DPIA use the **screening assessment** first to help you decide.

Aim to complete your DPIA as early as possible as the outcome of the assessment could affect the viability of your plans. In extreme cases, you will not be able to continue with your plans without changing them, or at all.

Guidance notes are included within the template to help you with its completion- just hover your mouse over any blue text for further information.

The Information Management Service is also available for further advice and support. Please keep in mind our service standards if you require advice.

1. Process/system overview

1.1 Ownership

Project Title:	BDG 184b – Machine Learning – Text classification
Project Manager:	Raymond wong
Information Asset Owner:	Mike Fitzgerald, Director of Digital, IT and Business Services
Data controller(s)	ICO
Data processor(s)	Microsoft *ICS.AI is the contracted developer of the text classification solution. They will be creating the solution within ICO managed environment.*

1.2 Describe your new service or process

In this document with reference to Customers it is defined as anyone who has sent an email into the dataprotectionfee@ico.org.uk mailbox which is made up of a majority of organisations although not exclusive. ICO will introduce a new service that will send an automated email to customers if they are making a change of address. Emails sent to the dataprotectionfee@ico.org.uk inbox will be classified using a machine learning service which will then automatically send an email.

Training Phase:
To develop the model ICS.AI will have to train the model to define the classification the emails will be measured against. This will require emails from ICO inbox dataprotectionfee@ico.org.uk.

During the training phase all data will remain within ICO managed services inside of UK region. Our privacy has been updated to ensure to include the use of machine learning. Once training has been completed no data will be left in the model and data will be deleted from the inbox dataprotectionfee@ico.org.uk as standard ICO email policy.

During the model training phase, no automated emails will be sent to customers.

Production:
When this service goes live all emails sent to dataprotectionfee@ico.org.uk will be classified and based on the model calculation they will receive a predefined automated response.

All emails should receive an automated response.

For a change of address classification, an email is sent to the customer containing information about how they can complete the change using the new change of address service online.
Other emails classified as a generic query will receive an automated email acknowledging receiving the request and an expected SLA of when the request will be completed.

Emails sent to dataprotectionfee@ico.org.uk typically contain information relating to a registration query i.e., name change or change of address. This information is publicly available on the data registration online.

However, there is no restriction on what information can be entered in the email, there is a risk of unintentional or intentional personal data being included by a customer and being processed.

The machine learning services will be within the ICO managed Azure subscription services and within the UK region. Data will not leave the UK during the processing or training.

A privacy notice will be updated to discourage users from entering personal data not related to registration queries and inform them of the email processing involved.

The dataprotectionfee@ico.org.uk retention is set as the standard ICO email policy.

Emails sent to the inbox will not be lost or altered by the machine learning process. The current design means that all emails sent to the inbox will be unaltered and will be processed as per normal by CRM.

All ICO registration agents with required permissions will be able to access and look at the inbox as normal.

Development for the machine learning text classification model has been contracted to a company called ICS.AI. They will be completing work within our managed ICO environment and will not hold or process any data outside of our enviroment. Contract is under the Gcloud framework.

1.3 Personal data inventory - explain what personal data is involved

Categories of data	Data subjects	Recipients	Overseas transfers	Retention period
Emails sent to the dataprotectionfee@ico.org.uk mailbox will have its contents classified. This will include the email address, subject title and the contents of the email which may contain information relating to registrations queries around address of trader/trading name/contacts for the registrations/payment categories or any other information they input in the email body. Email header information will be removed and is not processed by machine learning text classification service. No Cookies are used for this service.	Members of the public submitting email queries to dataprotectionfee@ico.org.uk	ICO Microsoft	None.	ICO standard email policy

This inbox is reserved for registration related queries and there are no restrictions preventing customers sending in personal information. A privacy notice will be updated on the website to inform users that any information sent to the above inbox will be processed using a text classification service provided by Microsoft Azure services which are managed within the ICO enviroment.				
Azure Database Raw text strings of email will be uploaded and through the text classification process data will be put into a format where statistics calculated from our training data is used to calculate probabilities for new data. Probabilities are calculated separately for each class. This means that we first calculate the probability that a new piece of data belongs to the first class, then calculate probabilities that it belongs to	Members of the public submitting email queries to dataprotectionfee@ico.org.uk	ICO Microsoft	None.	Data will be deleted after the training of the text classification model. This deletion of data will be done once the model has been created. The creation of the model and deletion of the data will be done by ICS.AI which is a contracted company for developing the text classification model. ICS.AI will be creating the model and deleting the data from the Azure database server within our managed ICO environment and will not hold or process any data outside of our enviroment.

the second class, and so on for all the classes				

1.4 Identify a lawful basis for your processing

ICO

The lawful basis for processing under GDPR article 6 is 6(1)(e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

1.5 Explain why it is necessary to process this personal data

The Machine learning project will provide a text classification service, that will allow ICO to response to customers based on the content of their email query.

Customers sending emails which are classed of type" change of address" will receive an automated email advising them of the new online service and further information required to process a change request in the form of a security pin.

This will efficiently direct customers to a new service and provide instructions on how to request a security pin. Reducing registration queries directed to the inbox.

Other customer queries will receive a generic response that acknowledges the receipt of the request and further information on expected response times. This will enhance our customer experience by reassuring their query has been received and reducing the number of follow up queries.

The text classification service will provide a quick and efficient way for customers to get the further information when requesting a change without contacting the helpline.

The project is necessary to reduce the number of staff to manually process incoming email. The current backlog is circa 4000 and the volume of emails is increasing daily. The backlog will increase further with expected growth of the registration. This back log and cannot be managed without hiring additional staff and working additional hours.

1.6 Outline your approach to completing this DPIA

We consulted our internal cyber security team to complete a security opinion reports.

Our internal information management team will be consulted to provide advise and guidance on data privacy.

Externally, ICS.AI have provided a proof of concept of the text classification service which was assessed before project was approved. ICS.AI have provided a number of similar services for the public sector and expert in their field.

ICS.AI are part of the UK government digital marketplace and approved for providing IT services.

Public consultation is not appropriate as internal processes are being updated to make ICO business processes more efficient. The original intent of the email is not being used for other purposes.

2.0 Data flows

2.1 Provide a systematic description of your processing, from the point that the data is first collected through to its destruction.

If your plans involve the use of new technology, you should explain how this technology works and outline any 'privacy friendly' features that are available.

High level Data Flow
Training process

The first phase to develop a Text classification model for production. In the model training phase, all training data will be deleted from the SQL server and NO automated response will be set to customers. This will be done by our contract supplier ICS.AI.

- Customer email data is copied and uploaded onto SQL server. (original Data remains within inbox)
- Azure ML services uses computation power from the virtual machine to process data stored on the database to generate model.
  Example process **Naive Bayes Classifier** includes.
  Step 1: Separate by Class

  Separating our training data by class.
  Create a dictionary object where each key is the class value and then add a list of all the records as the value in the dictionary
  This will be the class dataset.

  Step 2: Summarize Dataset.
  Calculate mean and the standard deviation for each dataset (split by class)

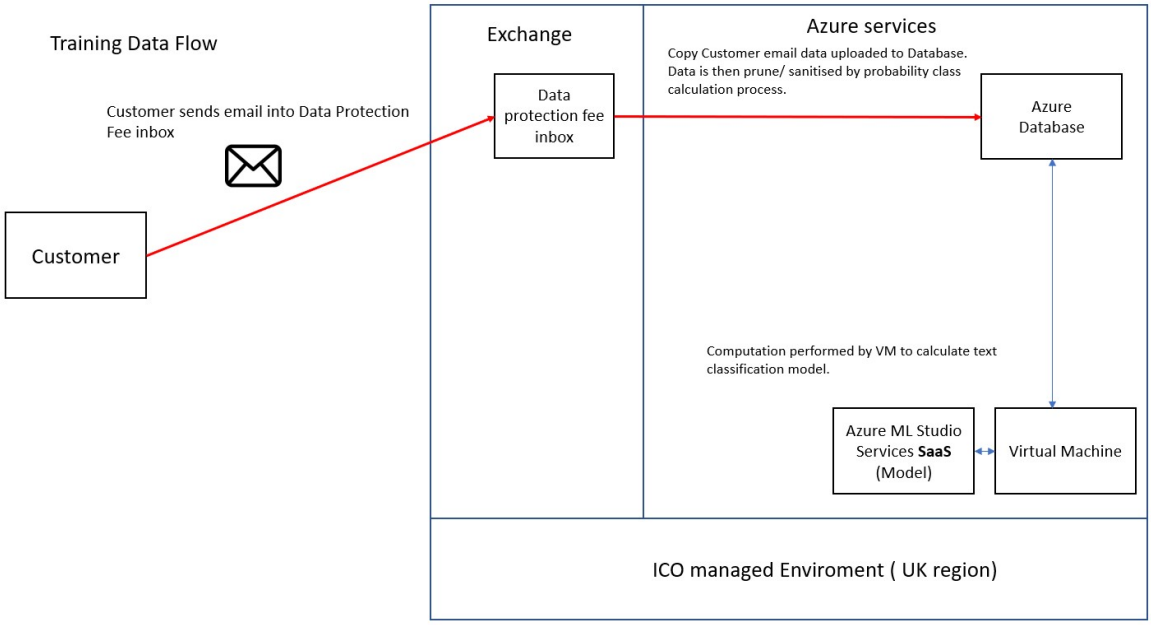
  Step 3: Summarize Data by Class.
  The dataset is first split by class, then statistics are calculated on each subset. The results in the form of a list of tuples of statistics are then stored in a dictionary by their class value.

  Step 4: Probability Density Function.
  estimate the probability of a given value to class
  Probability density function (PDF) is a statistical expression that defines a probability distribution (the likelihood of an outcome) for a discrete random variable

  Step 5: Class Probabilities.
  Now it is time to use the statistics calculated from our training data to calculate probabilities for new data.
  Probabilities are calculated separately for each class. This means that we first calculate the probability that a new piece of data belongs to

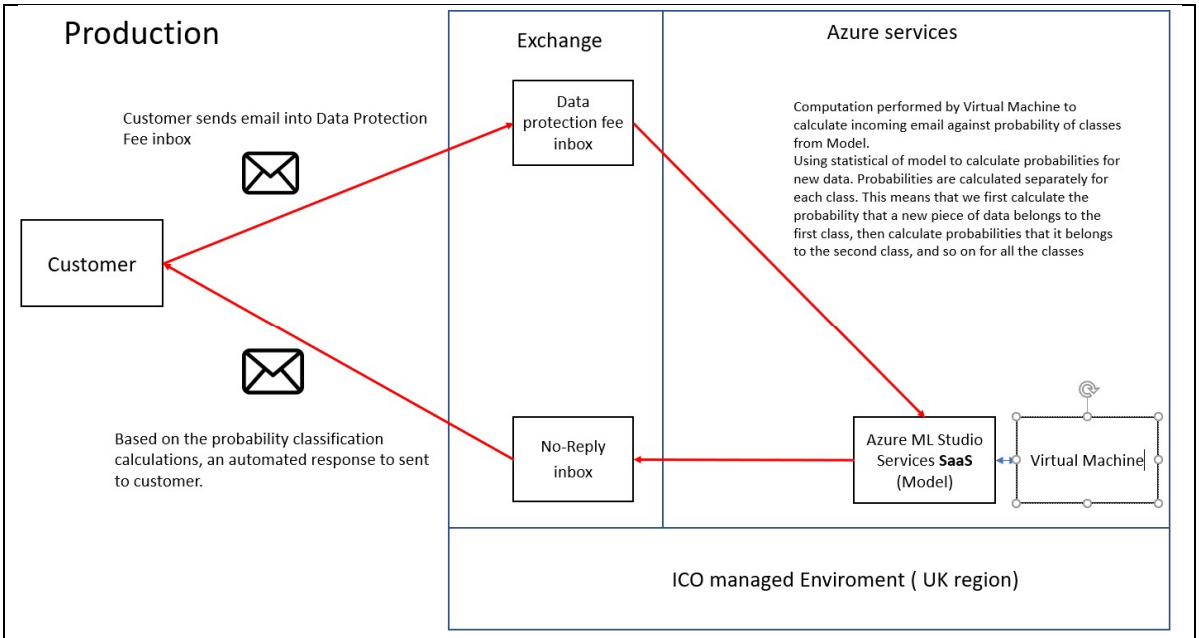
the first class, then calculate probabilities that it belongs to the second class, and so on for all the classes

- Classification Model is generated.
- Delete training Data from database.



Production Dataflow.
High level Data Flow

- Azure ML services uses computation power from the virtual machine to process incoming mail.
  This process includes.
  - Data pruning/sanitising by getting data into a format usage for the text classification model.
  - Calculation of probability of new data being of classification based on Model classification values.
  - Data is classified if it meets the probability threshold.
- Classification of emails is generated.
- Customers are emailed based on the classification.



The accuracy of the model will depend on the dataset and the quality of the model. Our estimated accuracy rate is 88% on the proof-of-concept demo.

3.0 Key principles and requirements

Purpose & Transparency

1. Will you need to update our privacy notices?

Yes ☒ No ☐

2. If you are not updating our privacy notices how do you intend to communicate information about your processing to the data subjects?

ICO AI guidance advises that the transparency information on training data is to be given prior of starting.

A privacy notice has been updated before the training phase to inform customers of the additional processing using machine learning services.

Although the service uses Machine learning technology for text classification no decision or judgement is made that impacts on the individual. All business processes remain unaltered and their request are not biased or altered in any way.

A privacy notice will be updated prior to the service going live.

3. If consent is your lawful basis for processing personal data are you maintaining appropriate records of the data subjects consent?

Yes ☐ No ☐ N/a ☒

4. If legitimate interests is your lawful basis for processing have you completed a legitimate interest assessment?

Yes ☐ No ☐ N/a ☒

If applicable, please provide a link to your completed assessment.

Accuracy

5. Are you satisfied the personal data you are processing is accurate?

Yes ☒ No ☐

6. How will you ensure the personal data remains accurate for the duration of your processing?

The data will not be altered, and original email will remain in the inbox.

7. If the personal data isn't being obtained directly from the data subject what steps will you take to verify accuracy?

N/A

Minimisation, Retention & Deletion

8. Have you done everything you can to minimise the personal data you are processing?

Emails headers will be removed and by the model as part of the text classification process.

Yes ☒ No ☐

9. How will you ensure the personal data are deleted at the end of the retention period?

A Retention policy of 12 months is applied on the mailbox. All training data will be deleted after the model has been created from the Azure Database while the original email will remain in the inbox for 12 months.

10. Will you need to update the retention and disposal schedule?

Yes ☐ No ☒

Integrity and confidentiality

11. Where will the personal data be stored?

Data will be stored in the ICO managed Azure subscription.

12. Are there appropriate access controls to keep the personal data secure?

Access to the training model will be restricted by role base access to the azure subscription. Access control is managed by ICO global admins who have access to the azure subscription which will be 2 users (Digital platform Architect and infrastructure Architect). The permitted users will be ICO IT admins and ICS.AI staff while creating the solution. Post training when the service is live access will be restricted to ICO IT admins and ICS.AI for support and maintenance of the service when required. ICS. AI may access ICO enviroment if the service is not working, they will not access the service as pat of Business-as-usual practices.

Yes ☒ No ☐

13. Have you contacted the cyber security team for a security assessment of your plans?

Yes ☒ No ☐ N/a ☐

If applicable, please provide a link to any assessment.

Open SOR - Ref 000057 - SOR - Identify emails for auto reply in dataprotectfee mailbox using machine learning.docx

14. Please explain the policies, training or other instructions you intend to put in place to enable staff to operate the new system or process securely.

N/A service will only be accessible to specific users with elevated administration permissions.

Accountability

15. Who will be the Information Asset Owner for this personal data?

Director of Digital, IT and business services

16. Will you need to update our Article 30 record of processing activities?

Yes ☒ No ☐

17. If you are using a data processor have you agreed, or will you be agreeing, a written contract with them?

Yes ☒ No ☐ N/a ☐

Individual Rights

18. Is there a means of providing the data subjects with access to the personal data being processed?

Yes ☒ No ☐

19. Can inaccurate or incomplete personal data be updated on receipt of a request from a data subject?

Yes ☒ No ☐

20. Can we restrict our processing of the personal data on receipt of a request from a data subject?

Yes ☒ No ☐

21. Can we stop our processing of the personal data on receipt of a request from a data subject?

Yes ☒ No ☐ N/a ☐

22. Can we extract and transmit the personal data in a structured, commonly used and machine readable format if requested by the data subject?

Yes ☒ No ☐ N/a ☐

23. Can we erase the personal data on receipt of a request from the data subject?

Yes ☒ No ☐

Risk Description	Response to Risk	Risk Mitigation	Expected Risk Score		
			I	P	Total
			See Appendix 1 – Risk Assessment Criteria		
A customer receives an incorrect response as a result of the automated email response.	Accept	*Expected mitigation: The classification scope is limited to change of address and a generic response stating we have received the customers request and that which will be processed within an estimated timeframe. Customers incorrectly classified would receive the default response which is an acknowledgement. This will not have an impact on personal data. Only emails with an 80% certainty of a change of address request will be sent an email containing the link to change of address form.*	*1*	*1*	*1-Low*
Failure to provide transparency information prior to starting the Model training process	Avoid	*Expected mitigation:* *A privacy notice has been updated to inform customers the additional use for training purposes including machine learning.*	*1*	*1*	*1-Low*

User bias and discrimination.	Accept	*Expected mitigation:* *Users will NOT be categorized/labelled, and their requests will NOT be prioritised for preference.* *There is no decision made on the text classification that will alter the content and affect the processing of their email.* *By default, all current business processes remain, and the customer email will arrive in the inbox and be processed by the ICO registration department as current process. The Text classification will only send an acknowledgement email OR an email informing them of a change of address service.*	*1*	*1*	*1 - Low*

4.0 Risk assessment

5.0 Consult the DPO

Guidance: Submit your DPIA for consideration by the DPIA Forum. The process to follow is here.
Any recommendations from the DPOs team will be documented below and your DPIA will be returned to you. You should then record your response to each recommendation.

	Recommendation	Date and project stage	Project Team Response
1.	**See emails dated 11/03/2021 & 23/03/2021**	Planning 23.03.21	All recommendations accepted including Privacy notice updated on contact us page to include use of machine learning tools for training phase.
2	**Privacy notice before go live**	Planning 19.06.21	Privacy notice updated on contact us page to include statement we may send an automatic reply from insights from machine learning tools.

6.0 Integrate the outcomes back into your plans

Guidance: Identify who is responsible for integrating the DPIA outcomes. The outcomes include any expected mitigation you need to take as identified in your risk assessment and any further actions resulting from the DPOs recommendations.

Action	Date for completion	Responsibility for Action	Completed Date
Update Privacy Notice for training	03.03.21	Raymond Wong	03.03.2021

Delete Training Data	28.04.2021	ICS.AI	28.04.2021
Update Article 30 record of processing activities (3.0 Q18)	Before Go-Live	Raymond Wong	19.05.2021
Update Privacy Notice before Go-Live	28.05.21	Raymond Wong	19.05.2021

7.0 Expected residual risk and sign off

Guidance: Summarise the expected residual risk below. This is any remaining risk *after* you implement all of your mitigation measures and complete all actions.

It is never possible to remove all risk so this section shouldn't be omitted or blank. If the expected residual risk remains high (e.g. red on the traffic light scoring in the Appendix) then you will need to consult the ICO as the regulator by following the process used by external organisations.

The text classification and automated reply service is reliant on the Microsoft services being available and secure.

It is not possible to guarantee the service will always be available and that there is will be no security related incidents in future. The residual risk is low for Microsoft to be affected by either service interruption or security incident.

The overall residual risk is low , customers are not subject to bias/discrimination and the impact on users in an event of a false positive would be they receive an email with reference to a new change of address link.

7.1 IAO sign off

IAO (name and role)	Date	Project Stage
Mike Fitzgerald	19.05.21	Planning

8.0 Change history

Guidance: To be completed by the person responsible for completing the DPIA and delivering the system, service or process)

Version	Date	Author	Change description
V0.1		Ray Wong	First Draft
V0.2		Steven Johnston	Completed section 5.0 DPIA forum recommendations

Appendix 1: Risk Assessment Criteria

The following criteria are aligned with our corporate risk assessment criteria.

Impact

Impact is the consequence of a risk to the rights and freedoms of individuals being realised. Factors to consider include the financial harm or emotional distress that can be expected to occur.

Impact	Scoring criteria
Very low (1)	No discernible impact on individuals.
Low (2)	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc).
Medium (3)	Individuals may encounter significant inconveniences, which they will overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc)
High (4)	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc).
Very high (5)	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Probability

Probability is the likelihood of a risk to the rights and freedoms of individuals being realised. Factors to consider include the expected frequency of occurrence, and the motivation and capability of threat sources (eg does the threat require insider knowledge and/or significant technical resources to exploit any vulnerability?).

Probability	Scoring criteria
Very low (1)	0-5% - extremely unlikely or improbable For example, the risk has not occurred before or is not expected to occur within the next three years.
Low (2)	6-20% - low but not improbable

	For example, the risk is expected to occur once a year.
Medium (3)	21-50% - fairly likely to occur For example, the risk is expected to occur several times a year.
High (4)	51-80% - more likely to occur than not For example, the risk is expected to occur once a month.
Very high (5)	81-100% - almost certainly will occur For example, the risk is expected to occur once a week.

Risk level

Risk level is a function of impact and probability, and is represented by a RAG rating.

Probability / Impact	Very low (1)	Low (2)	Medium (3)	High (4)	Very high (5)
Very high (5)	Amber (5)	Amber (10)	Red (15)	Red (20)	Red (25)
High (4)	Green (4)	Amber (8)	Amber (12)	Red (16)	Red (20)
Medium (3)	Green (3)	Amber (6)	Amber (9)	Amber (12)	Red (15)
Low (2)	Green (2)	Green (4)	Amber (6)	Amber (8)	Amber (10)
Very low (1)	Green (1)	Green (2)	Green (3)	Green (4)	Amber (5)

Risk acceptance criteria

These criteria are guidelines only, and any risk treatment decisions should be made on a case-by-case basis. For example, it may be prudent to reduce a low risk because of legal and regulatory requirements.

Risk level	Acceptance criteria
Low (Green)	Within this range risks can be routinely accepted.
Medium (Amber)	Within this range risks can occasionally be accepted but shall be kept under regular review.
High (Red)	Within this range risks shall not be accepted and immediate action is required to reduce, avoid or transfer the risk.

Appendix 2: example risks to data subjects

Guidance: The following are examples of common risks associated with the processing of personal data to assist with your risk assessment. Not all of them will apply to your processing and the list is not exhaustive – you should consider specific risks that are relevant to your plans.

- Data is processed for unspecified / unlawful purposes/ not within expectations of data subjects
- Excessive data is processed
- Data is not kept up to date
- Data is kept for longer than is necessary by us
- Data is kept for longer than is necessary by data processor
- Data processed in contravention of data subject rights
- Data subjects unable to exercise their rights
- Data stolen or modified in transit
- Data stolen or modified at rest in our premises
- Data stolen or modified at rest in data processor premises
- Data transferred overseas to a jurisdiction that does not adequately protect data subject rights
- Re-identification of pseudonymised data by data processor or third party
- Unauthorised destruction or loss of data
- Data processor network / system / online portal not secure
- Data processor fails to process data in accordance with our instructions
- Personal data of children processed without appropriate safeguards / parental authority
- Consent of data subject not freely given (for example employer / employee processing)
- The data subject is particularly vulnerable (elderly or disabled) or is there a potential imbalance of power between the individual and the data controller (employee/employer)
- Source of data poses risks re accuracy (obtained from a unverified or old list)
- Risk to accuracy of data due to matching / combining data from different sources
- Use of new technology, e.g. fingerprinting, face recognition
- Monitoring or recording individuals
- Using profiling according to characteristics or behavior
- Non-compliance with DP principles

9.0 Template Change History (for Information Management Service only)

Version	Date	Author	Change description
v0.1	01/06/2020	Steven Johnston	First draft
v1.0	07/10/2020	Steven Johnston	First release
v1.1	07/01/2021	Iman Elmehdawy	Amendment to guidance note page 2.

Case reference

IC-203321-W1K8

Microsoft AI Builder for Processing Paper Direct Debit Mandates - DPIA

ico.
Information Commissioner's Office

Data Protection Impact Assessment – Microsoft AI Builder

Document Name	Data Protection Impact Assessment – Microsoft AI Builder for Processing Paper Direct Debits mandates
Author/Owner (name and job title)	Sue Shepherd
Department/Team	Business Development Group
Document Status (draft, published or superseded)	Published
Version Number	1.0
Release Date	12/01/2021
Approver (if applicable)	
Review Date	
Distribution (internal or external)	Internal

Guidance for completing this template

Complete this Data Protection Impact Assessment (DPIA) template if your DPIA screening assessment indicates a high risk to individuals. If you are unsure whether you need to complete a DPIA use the **DPIA Screening Assessment** to help you decide.

Aim to complete your DPIA as early as possible as the outcome of the assessment could affect the viability of your plans. In extreme cases, you will not be able to continue with your plans without changing them, or at all.

Guidance notes are included within the template to help you with its completion- just hover your mouse over any blue text for further information.

The Information Management Service is also available for further advice and support. Please keep in mind our service standards if you require advice.

1. Process/system overview

1.1 Ownership

Project Title:	Microsoft AI builder for processing paper direct debit mandates
Project Manager:	Sue Shepherd
Information Asset Owner:	Mike Fitzgerald
Data controller(s)	ICO
Data processor(s)	Microsoft, BACS

1.2 Describe your new service or process

This is a new process for AI assisted processing of direct debit paper mandates.

Traditionally direct debit paper mandates have been sent out to customers for the payment of their data protection fees. These paper mandates have been completed by the customer and posted or emailed into the office, then manually keyed in by staff.

We are moving to an online approach for digital direct debit sign-up but will still be offering this paper method, plus due to the pandemic we have a backlog of mandates waiting to be processed.

Microsoft AI builder and Flow have been designed to automate time consuming manual processes and this is an ideal small project to transition to this new technology.

We will be implementing Microsoft's AI builder to scan and read the data and Microsoft's Flow module to push this data into a csv file which can then be processed into ICE registration.

During AI scanning a confidence level will be applied based on rules such as 6 numeric characters for sort code. Any documents not obtaining the required confidence level will have a manual intervention or import rules applied, which will mean that if a field doesn't meet the confidence level, we will revert to another field which is text rather than handwritten – such as DD mandate date to scanned date.

The scanned data will be collated into a csv file which will be scheduled to run once a day, with a maximum number processed of 500 DD's in a file. The file is then passed into our ICO estate for processing into the ICE registration system.

This will be our first use of Microsoft's AI builder and the processing method will be subject to an internal security opinion report (SOR) review. The data transfer method will be using our Data Gateway, the same process that is used for passing csv file of our digital direct debits data collected via our website. The AI builder will be trained using 300 paper direct debit mandates.

1.3 Personal data inventory - explain what personal data is involved

Categories of data	Data subjects	Recipients	Overseas transfers	Retention period
The data pulled from the DD mandate form is limited to – Account name Bank account number Bank sort code Registration reference (pre-populated on mandate form) DD date signed Scanned date (added by restore scanning service)	Data Protection fee payers who wish to pay the annual registration fee by completing a paper direct debit mandate.	ICO, Registration and collection of DP fees BACS for processing payments Microsoft, when investigation and support is required for issues	Data can be hosted in Microsoft's UK and/or EEA data centres. We have chosen to set our data flow to use UK region, so data stays within UK and within our 365 tenancy	Scanned copy of paper mandate retained for six years, as a requirement for financial data, stored within our corporate store. Scanned mandates would be stored in EDRM and deleted in line with our EDRM retention processes – this will be Finance site and Finance will have responsibility for deletion. Mailbox retention will be in line with ICO schedule – automated deletion after 12 months.

a. Identify a lawful basis for your processing

The lawful basis for processing is Article 6(1)(e) - Public Task.

b. Explain why it is necessary to process this personal data

A DP fee payer may choose to set up a Direct Debit mandate by completing a paper form with their bank details and posting or emailing this to the ICO. Our current process, during the pandemic, is for Restore to scan any postal mandates into an ICO mailbox. Staff would then open the emails, both those from Restore and those received direct from customers and key in the information from the mandate into our ICE registration system. We are proposing to use Microsoft's AI builder to scan the direct debit mandates and Microsoft's Flow module to push this data into a csv file which can then be processed into ICE registration. This will provide a more efficient, accurate and faster method to process the backlog and ensure we stay on top of these paper mandates. It will also free up staff in the DP Fees department. To do this we have identified the minimum amount of personal data required as explained in section 1.3.

c. Outline your approach to completing this DPIA

DPIA questionnaire and screening assessment have been completed, which indicated a full DPIA assessment, due to this being the first use of Microsoft AI builder

We have been following advice from our third party supplier Kainos in conjunction with Microsoft's best practise for the PowerApps environment, including data loss protection policies, creating a default policy for all environments. Access to the PowerApps environment will be limited to specified admin accounts.

SOR is in progress with cyber security team.

We will not be consulting with data subjects as the categories of data are already processed by the ICO and we are only utilising the AI software as an OCR reader. The processing will not include any automated decision making that will have a legal or similar detrimental effect on individuals.

2.0 Data flows

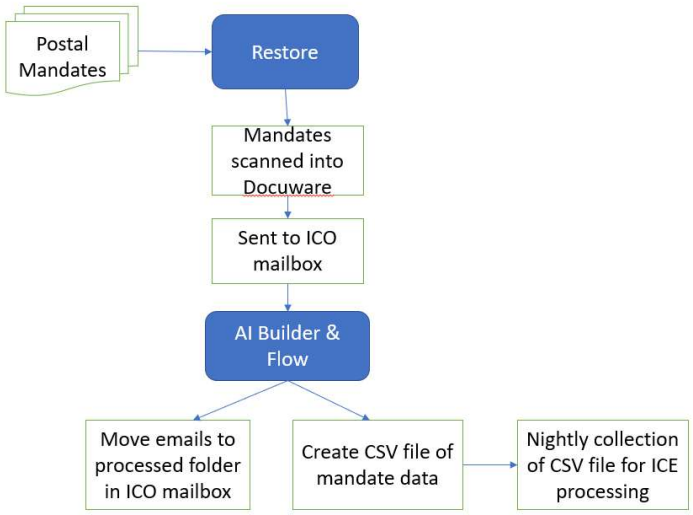
2.1 Provide a systematic description of your processing, from the point that the data is first collected through to its destruction.

If your plans involve the use of new technology you should explain how this technology works and outline any 'privacy friendly' features that are available.

Paper direct debit mandates coming through the Royal Mail postal system are currently being collected and scanned by Restore and emailed to the ICO, they are then manually entered into the ICE registration system.

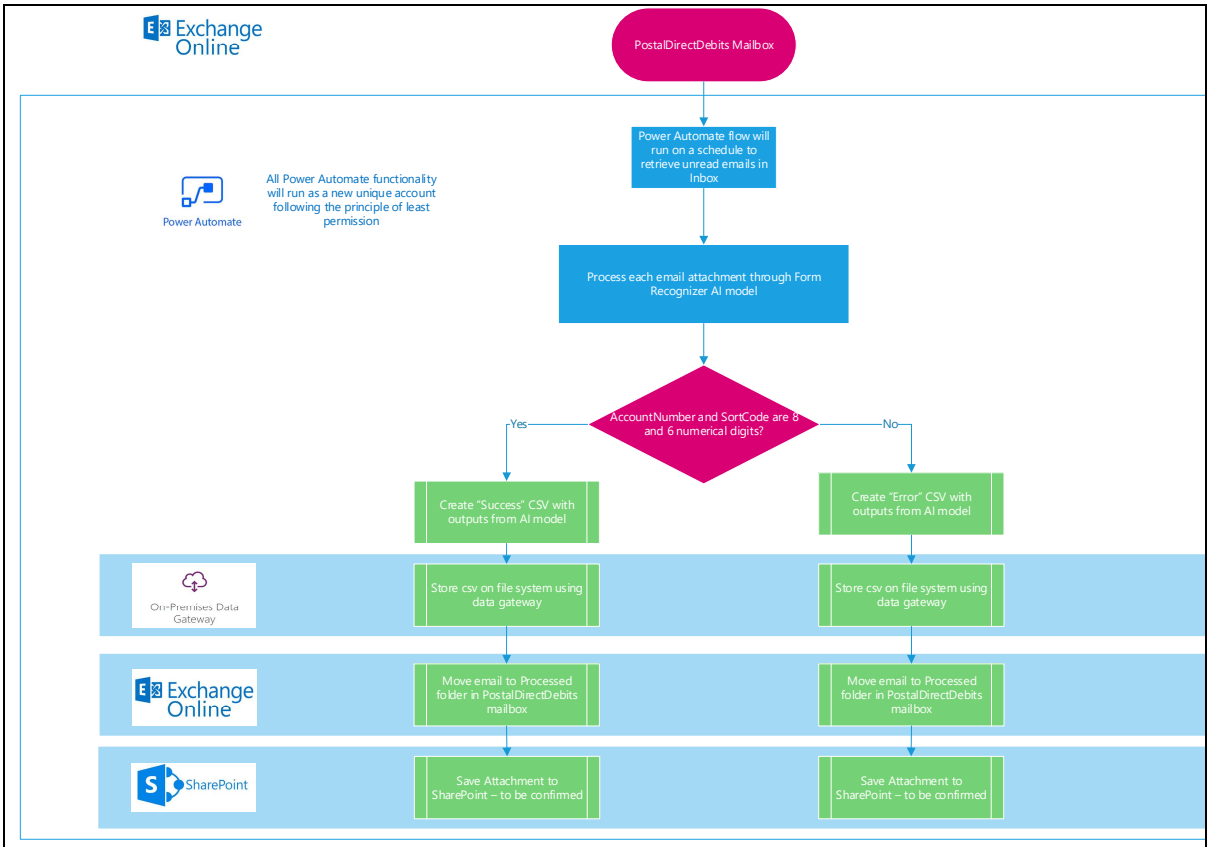
The proposed processing solution for increasing efficiency, avoiding data backlogs and improving data entry uses Microsoft's AI builder to scan the direct debit mandate data from the emails and push this data into to a csv file for processing into our ICE system.

The full process flow will be:



1. Post scanned by Restore into Docuware digital mail room
2. Received into ICO mailbox 'Postaldirectdebits@ico.org.uk'
3. Microsoft AI Builder will be used to scan and extract the ICO registration number, bank account name, sort code, account number and date signed from the direct debit mandate form. Microsoft Flow will take this extracted data and format it into a csv file
4. As emails are processed by AI Builder they will be moved from the inbox into a processed folder in ICO mailbox 'Postaldirectdebits@ico.org.uk'. At a later date copies of mandate will be stored in our corporate data store in a Sharepoint Finance folder.
5. csv file transferred via Data Gateway to CRM server nightly
6. csv processed into ICE registration

Below is the data flow for step3 using the Microsoft AI builder.



Our Microsoft AI builder model will be trained using the first 300 paper direct debit mandates processed from customers. The model will be taught, using point and click functionality, to look for and identify the ICO registration number, bank account name, sort code, account number and date signed from the direct debit mandate form. Having identified the fields it will then use text recognition(OCR) to extract the data, Microsoft's Flow will then take this data and push it into a formatted csv file.

The direct debit mandates used during the AI Builder training cycle will be stored in Microsoft's common data store in the UK and will be deleted once the training cycle has been completed. This process will happen once on the first 300 paper mandates, after that the training model will be turned off and the AI builder will not be continually learning.

As part of the training cycle a confidence level will be applied to scanned data. any documents not obtaining the required confidence level will be processed manually.

3.0 Key principles and requirements

Purpose & Transparency

1. Will you need to update our privacy notices?

Yes ☐ No ☒

2. If you are not updating our privacy notices how do you intend to communicate information about your processing to the data subjects?

3. If consent is your lawful basis for processing personal data are you maintaining appropriate records of the data subjects consent?

Yes ☐ No ☐ N/a ☒

4. If legitimate interests is your lawful basis for processing have you completed a legitimate interest assessment?

Yes ☐ No ☐ N/a ☒

If applicable please provide a link to your completed assessment.

Accuracy

5. Are you satisfied the personal data you are processing is accurate?

Yes ☒ No ☐

6. How will you ensure the personal data remains accurate for the duration of your processing?

During AI scanning a confidence level will be applied based on rules such as 6 numeric characters for sort code. Any mandates not obtaining the required confidence level will not be automatically processed, but will be recorded in a 'Failed' file and will be manually processed. Registration number will be validated against ICE registration system. During the BACS processing validation checks are performed, known as 'Mod check', any account sort code/ account number discrepancies are highlighted in an error file.

There are existing processes in place for customers to amend and update their direct debit mandate details and processes within Finance to handle incorrect and invalid paper DD mandates.

7. If the personal data isn't being obtained directly from the data subject what steps will you take to verify accuracy?

N/A

Minimisation, Retention & Deletion

8. Have you done everything you can to minimise the personal data you are processing?

Yes ☒ No ☐

9. How will you ensure the personal data are deleted at the end of the retention period?

Scanned copy of paper mandate retained for six years, as a requirement for financial data, stored within our corporate store.

Scanned mandates would be stored in EDRM and deleted in line with our EDRM retention processes – this will be Finance site and Finance will have responsibility for deletion.

Mailbox retention will be in line with ICO schedule – automated deletion after 12 months.

csv file for transfer/import will be kept for 14 days on CRM server, automated deletion process.

10. Will you need to update the retention and disposal schedule?

Yes ☒ No ☐

Integrity and confidentiality

11. Where will the personal data be stored?

ICO systems:

1. Docuware digital mail room
2. ICO mailbox 'Postaldirectdebits@ico.org.uk'
3. Microsoft Common Data Store held in the UK region
4. Csv file transferred via Data Gateway to CRM server
5. csv processed into ICE registration system
6. at a later date the mandates will be transferred from the mailbox into a Sharepoint Finance folder

csv file for transfer/import to CRM (ICE) will be held for 14 days

12. Are there appropriate access controls to keep the personal data secure?

Yes ☒ No ☐

13. Have you contacted the cyber security team for a security assessment of your plans?

Yes ☒ No ☐ N/a ☐

If applicable please provide a link to any assessment.

A separate Security Opinion Report (SOR) for Microsoft AI Builder is being prepared

14. Please explain the policies, training or other instructions you intend to put in place to enable staff to operate the new system or process securely.

Update to Business processes for DP fees, to include new process and processing of those 'failed' from the mailbox that need manual intervention.

Service Definition Document (SDD) being prepared for ITHelp for the file transfer process via Data Gateway to CRM server.

Accountability

15. Who will be the Information Asset Owner for this personal data?

Director of Digital, IT and Customer Services

16. Will you need to update our Article 30 record of processing activities?

Yes ☒ No ☐

17. If you are using a data processor have you agreed, or will you be agreeing, a written contract with them?

Yes ☒ No ☐ N/a ☐

Individual Rights

18. Is there a means of providing the data subjects with access to the personal data being processed?

Yes ☒ No ☐

19. Can inaccurate or incomplete personal data be updated on receipt of a request from a data subject?

Yes ☒ No ☐

20. Can we restrict our processing of the personal data on receipt of a request from a data subject?

Yes ☒ No ☐

21. Can we stop our processing of the personal data on receipt of a request from a data subject?

Yes ☒ No ☐ N/a ☐

22. Can we extract and transmit the personal data in a structured, commonly used and machine readable format if requested by the data subject?

Yes ☒ No ☐ N/a ☐

23. Can we erase the personal data on receipt of a request from the data subject?

Yes ☒ No ☐

4.0 Risk assessment

Risk Description	Response to Risk	Risk Mitigation	Expected Risk Score		
			I	P	Total
			See Appendix 1 – Risk Assessment Criteria		
A valid bank sort code and account number is entered that does not belong to the DP Fee payer. Example: the digit 7 is mistaken for digit 1 in the account number.	Reduced	During AI scanning a confidence level will be applied, 300 DD mandates will be used to train the AI builder Mod Check in the BACS processing will eliminate any invalid sort code and bank account number combinations.	2	1	2- Low
Access to ICO mailbox where paper direct debit mandates are stored	Reduced	Only certain groups of ICO colleagues will have access to the mailbox	1	1	1 – very low
Data being transferred outside UK	Avoid	Microsoft AI builder project, during implementation set Region = UK so all data held is placed in UK Common Data Store in our Microsoft O365 tenancy	1	1	1 – very low
Access controls and restrictions to the data held in the Microsoft Common Data Store	Reduced	During Microsoft AI builder implementation, system administrator and admin roles will be assigned	2	1	2 - Low
Not conforming to best practice in AI processing	Reduced	Liaised with our Technology and Innovation team and reviewed Guidance on AI and data protection | ICO	1	1	1 - very low
Data loss during the processing	Reduced	Regular checks on numbers received from Restore and number processed	2	1	2 - Low

5.0 Consult the DPO

Guidance: Submit your DPIA for consideration by the DPIA Forum. The process to follow is here.
Any recommendations from the DPOs team will be documented below and your DPIA will be returned to you. You should then record your response to each recommendation.

	Recommendation	**Date and project stage**	**Project Team Response**
1.	Clarify wording regarding overseas transfers in section 1.3	12/01/2021 - planning	Accept – 1.3 amended.
2.	Amend recipients in section 1.3 to clarify Microsoft only when support required.	12/01/2021 - planning	Accept – 1.3 amended.
3.	Include further detail about the process of training the AI module in section 2.1.	12/01/2021 - planning	Accept – 2.1 amended.
4.	Reference existing processes for customers to amend / update DD mandate.	12/01/2021 - planning	Accept – addition made to response to section 3.0 Q6.
5.	Specify if deletion of csv file after 14 days is manual or automated process.	12/01/2021 - planning	Accept – addition made to response to section 3.0 Q9.

6.	Update retention schedule for new information asset – digital scans of DD mandates.	12/01/2021 - planning	Accept – schedule to be updated.
7.	Add additional risks to section 4.0 • Not following AI best practice • Data leakage during processing operation	12/01/2021 - planning	Accept – addition made to 4.0.

6.0 Integrate the outcomes back into your plans

Guidance: Identify who is responsible for integrating the DPIA outcomes. The outcomes include any expected mitigation you need to take as identified in your risk assessment and any further actions resulting from the DPOs recommendations.

Action	Date for completion	Responsibility for Action	Completed Date
Update Retention Schedule	ASAP	IM Service	13/01/2020

7.0 Expected residual risk and sign off

Guidance: Summarise the expected residual risk below. This is any remaining risk *after* you implement all of your mitigation measures and complete all actions.

It is never possible to remove all risk so this section shouldn't be omitted or blank. If the expected residual risk remains high (e.g. red on the traffic light scoring in the Appendix) then you will need to consult the ICO as the regulator by following the process used by external organisations.

The residual risk is low as a result of the minimal data being collected and the mitigation controls put in place.

7.1 IAO sign off

IAO (name and role)	Date	Project Stage
Mike Fitzgerald, Director of Digital, IT and Business Services	13/1/21	IAO Sign Off

8.0 Change history

Guidance: To be completed by the person responsible for delivering the system, service or process (in a project this will be the project manager).

Version	Date	Author	Change description
V0.1	7/12/2020	Sue Shepherd	First Draft
V0.2	6/1/2021	Sue Shepherd	Updated for consideration by DPIA forum
V0.3	12/1/2021	Steven Johnston	Section 5.0 DPIA forum recommendations.
V1.0	12/1/2021	Sue Shepherd	Updated following recommendations from DPIA forum
V.1.1	13/1/2021	Mike Fitzgerald	Section 7.1 IAO sign off

Appendix 1: Risk Assessment Criteria

The following criteria are aligned with our corporate risk assessment criteria.

Impact

Impact is the consequence of a risk to the rights and freedoms of individuals being realised. Factors to consider include the financial harm or emotional distress that can be expected to occur.

Impact	Scoring criteria
Very low (1)	No discernible impact on individuals.

Low (2)	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc).
Medium (3)	Individuals may encounter significant inconveniences, which they will overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc)
High (4)	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc).
Very high (5)	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Probability
Probability is the likelihood of a risk to the rights and freedoms of individuals being realised. Factors to consider include the expected frequency of occurrence, and the motivation and capability of threat sources (eg does the threat require insider knowledge and/or significant technical resources to exploit any vulnerability?).

Probability	Scoring criteria
Very low (1)	0-5% - extremely unlikely or improbable For example, the risk has not occurred before or is not expected to occur within the next three years.
Low (2)	6-20% - low but not improbable For example, the risk is expected to occur once a year.
Medium (3)	21-50% - fairly likely to occur For example, the risk is expected to occur several times a year.
High (4)	51-80% - more likely to occur than not For example, the risk is expected to occur once a month.
Very high (5)	81-100% - almost certainly will occur For example, the risk is expected to occur once a week.

Risk level
Risk level is a function of impact and probability, and is represented by a RAG rating.

Probability / Impact	Very low (1)	Low (2)	Medium (3)	High (4)	Very high (5)
Very high (5)	Amber (5)	Amber (10)	Red (15)	Red (20)	Red (25)
High (4)	Green (4)	Amber (8)	Amber (12)	Red (16)	Red (20)
Medium (3)	Green (3)	Amber (6)	Amber (9)	Amber (12)	Red (15)
Low (2)	Green (2)	Green (4)	Amber (6)	Amber (8)	Amber (10)
Very low (1)	Green (1)	Green (2)	Green (3)	Green (4)	Amber (5)

Risk acceptance criteria
These criteria are guidelines only, and any risk treatment decisions should be made on a case-by-case basis. For example, it may be prudent to reduce a low risk because of legal and regulatory requirements.

Risk level	Acceptance criteria
Low (Green)	Within this range risks can be routinely accepted.
Medium (Amber)	Within this range risks can occasionally be accepted but shall be kept under regular review.
High (Red)	Within this range risks shall not be accepted and immediate action is required to reduce, avoid or transfer the risk.

Appendix 2: Common risks to data subjects

Guidance: The following are examples of common risks associated with the processing of personal data to assist with your risk assessment. Not all of them will apply to your processing and the list is not exhaustive – you should consider specific risks that are relevant to your plans.

- Data is processed for unspecified / unlawful purposes/ not within expectations of data subjects

- Excessive data is processed
- Data is not kept up to date
- Data is kept for longer than is necessary by us
- Data is kept for longer than is necessary by data processor
- Data processed in contravention of data subject rights
- Data subjects unable to exercise their rights
- Data stolen or modified in transit
- Data stolen or modified at rest in our premises
- Data stolen or modified at rest in data processor premises
- Data transferred overseas to a jurisdiction that does not adequately protect data subject rights
- Re-identification of pseudonymised data by data processor or third party
- Unauthorised destruction or loss of data
- Data processor network / system / online portal not secure
- Data processor fails to process data in accordance with our instructions
- Personal data of children processed without appropriate safeguards / parental authority
- Consent of data subject not freely given (for example employer / employee processing)
- The data subject is particularly vulnerable (elderly or disabled) or is there a potential imbalance of power between the individual and the data controller (employee/employer)
- Source of data poses risks re accuracy (obtained from a unverified or old list)
- Risk to accuracy of data due to matching / combining data from different sources
- Use of new technology, e.g. fingerprinting, face recognition
- Monitoring or recording individuals
- Using profiling according to characteristics or behavior
- Non-compliance with DP principles

9.0 Template Document control

Title	Data Protection Impact Assessment Template
Version	3.0
Status	Final release

Owner	DPSIA Forum
Release date	XX/06/20
Review date	XX/06/21

Case reference

IC-203321-W1K8

Microsoft Cortana Voice Recognition – Draft DPIA

ico.
Information Commissioner's Office

Data Protection Impact Assessment (DPIA) template

You should complete this template where there is a new (or significant change to an existing) service or process that involves the storage/processing of personal data (whether digital or hardcopy). When dealing with an existing process, service or system **only the change should be impact assessed.**

The DPO's team is available to assist and advise on completing this template.

The template should be submitted to the DPSIA Committee for their recommendations and approval.

For assistance or to submit a DPIA for approval email IGhelp@ico.org.uk.

You should start to complete the template as soon as you decide to implement a new system or process. How frequently the DPIA is reviewed and the governance required will vary with the risk of the system or process. At a **minimum**:

Projects: you should produce an initial DPIA prior to finalising your requirements, complete it before finalising your design and review & update the DPIA at least once more prior to go-live. In an Agile project, you should update the DPIA at the start and end of each Epic, or where there is a significant change to the data being processed or the technology or platform. Each update should be submitted to the DPSIA Committee.

Non-projects: you should complete the DPIA prior to designing the service or seeking suppliers and update it whenever there are material changes to the planned system or process.

Screening: Determine what to complete:

1. **GDPR DPIA**: Complete all sections if you meet 2+ questions in section 2.1
2. **Full DPIA**: Complete everything but section 6.2 if you meet 2+ screening questions in any section
3. **Compliance Checklist**: Complete sections 1, 2 and 4, plus signoff, if you don't meet the screening questions

Approval: Consult the DPO's team and select an option for the approvers based on your risk:

1. **DPSIA Committee**: including Senior Information Risk Officer, Head of Cyber Security, DPO
2. **DPSIA Committee**: including DPO and Head of Cyber Security
3. Representatives of DPO and Cyber Security, who will also send it to the DPSIA Committee for their information

Regardless of the option chosen, **the DPIA should be submitted together with your SIA**.

1. Process/system overview

1.1 Summary

Guidance: For projects please provide the following key details. Non-projects should provide a key contact who is responsible for delivering the system or process.

Project ID:	N/A
Project Title:	Microsoft Cortana Voice Recognition.
Project Manager:	Neil Smithies / Deborah Holt

1.2 Synopsis

Guidance: Provide a summary of the process or system including any relevant background information and the key aims/objectives that the system or process must achieve. There is no need for a detailed discussion of data or data flows – these are covered later in the assessment.

The Microsoft Managed Desktop programme is currently an invite only programme where Microsoft takes responsibility for the configuration, imaging, application deployment, software updates, security and end user support of a device. The service is made up of a combination of existing Microsoft services with an additional monitoring, management and support wrapper.

The components can be summarised as follows;

- Microsoft 365 E5
  - Office 365 E5
  - Windows 10 Enterprise E5
  - Enterprise Mobility + Security E5
- Microsoft Managed Desktop IT as a Service
  - Microsoft Support ("Get Help")
  - Microsoft Operations & Monitoring
- A Microsoft Surface Device

DPSIA's have already been completed for the following areas;

- Office 365 including Enterprise Mobility + Security
- Microsoft Get Help 24x7 Support ("Get Help")
- Microsoft Windows Diagnostics and Telemetry (Advanced Threat Protection)
- Windows Hello Biometric Framework

Scope of this DPSIA

- Microsoft Cortana Voice Recognition

Microsoft provides both a device-based speech recognition feature and a cloud-based (online) speech recognition service.

Turning on the Online speech recognition setting lets you use Microsoft cloud-based speech recognition in Cortana, ~~the Mixed Reality Portal,~~ dictation in

Windows from the software keyboard, supported Microsoft Store apps, and over time, in other parts of Windows.

When you use the Microsoft cloud-based speech recognition service, Microsoft collects and uses your voice recordings to create a text transcription of the spoken words in the voice data. The voice data is used in the aggregate to help improve Microsoft's ability to correctly recognize all users' speech, so the data Microsoft collects from these online services helps to improve them.

You can use device-based speech recognition without sending your voice data to Microsoft. However, the Microsoft cloud-based speech recognition service provides more accurate recognition than the device-based speech recognition. When the Online speech recognition setting is turned off, speech services that don't rely on the cloud and only use device-based recognition—like the Narrator app or the Windows Speech Recognition app—will still work, and Microsoft won't collect any voice data.

If you've given permission in Cortana, we also collect additional information, like your name and nickname, your recent calendar events and the names of the people in your appointments, information about your contacts including names and nicknames, names of your favourite places, apps you use and information about your music preferences. This additional data enables us to better recognise people, events, places and music when you dictate commands, messages or documents.

Online speech recognition is a accessibility feature that allows users to speak to their computer and their speech be represented on screen. This allows speech to text, real time subtitling and real time language translation.

Online speech recognition is turned off by default on an MMD device, however there are not restrictions in place to prevent a user from opting in to this service. At the time of writing, there are no standard management policies available to disable this service completely.

Commented [IEM1]: Can we switch off all of them?

Commented [SJ2]: Which of these things are we actually using / intending to use?

Commented [SJ3]: Most of this is lifted from the Microsoft privacy support documentation but we've omitted the section below. Is there a reason for this? I think it's important that we consider this in the DPIA even if the resulting decision is that we opt to disable this functionality.

If you've allowed Cortana to do so, Microsoft also collects information about your Calendar and People (also known as contacts) to help personalize your speech experience, and to help Windows and Cortana better recognize people, events, places, and music when you dictate messages or documents. The information Cortana collects will help personalize your speech experience on all your Windows devices and Cortana apps when you sign in with the same Microsoft account.

Commented [NS4R3]: I don't think it was on the support document when I stole it.

Commented [SJ5]: So do we want staff to be able to use this functionality or are we happy with it being disabled?

Commented [SJ6]: Most of this is lifted from the Microsoft privacy support documentation but we've omitted the section below. Is there a reason for this? I think it's important that we consider this in the DPIA even if the resulting decision is that we opt to disable this functionality.

If you've allowed Cortana to do so, Microsoft also collects information about your Calendar and People (also known as contacts) to help personalize your speech experience, and to help Windows and Cortana better recognize people, events, places, and music when you dictate messages or documents. The information Cortana collects will help personalize your speech experience on all your Windows devices and Cortana apps when you sign in with the same Microsoft account.

1.3 Definition of processing

Guidance: As a data controller we are required to maintain a "record of processing activities" for which we are responsible (Article 30 refers). The following table is designed to help us define the planned processing operation.

Data controller(s)	ICO & Microsoft ~~Michael Fitzgerald~~
Data processor(s)	Microsoft
Purpose of processing	Voice control and dictation
Categories of data	Speech
Categories of subjects	ICO Staff, ICO staff contacts and event organisers, invitees. Subjects of ICO communications depending

Commented [SJ7]: Potentially calendar and contact information too.

Also if Microsoft collects voice recordings to create a transcript of the spoken words then potentially the personal data shared could be broader. For example if I dictate a letter to a customer about a complaint it will contain that customers personal data – this DPIA needs to consider if we are comfortable with that

Commented [SJ8]: Potentially others depending on what is dictated

	on what is actually dictated
Categories of recipients	Microsoft Speech Recognition Servers and occasionally staff
Overseas transfers	Microsoft staff and speech reconigtion servers are located globally.

1.4 Purpose for processing

Guidance: State the business need being pursued in the processing, including the purposes, aims and the intended benefits for you, data subjects, society or others.

~~When you use the Microsoft cloud-based speech recognition service, Microsoft collects and uses your voice recordings to create a text transcription of the spoken words in the voice data. The voice data is used in the aggregate to help improve Microsoft's ability to correctly recognize all users' speech, so the data Microsoft collects from these online services helps to improve them.~~This data is processed if an ICO user wishes to dicate directly to their Windows 10 device, this may be an accessibility requirement, reducing the need for keyboard input or may be a requirement for real time subtliting or translation of streaming video content (such as a staff presentation or briefing)

Commented [SJ9]: This has all already been stated above. This section needs to focus on why we at the ICO want to use these features. What aim is being pursued? Some examples of what we think staff will use this for would be useful.

1.5 Lawful basis

Guidance: State the basis on which the processing is lawful under GDPR Article 6 (consent, performance of contractual obligations to a data subject, compliance with legal obligations, protecting the vital interests of a natural person, public task or legitimate interests). If you are processing based on legitimate interests you must also complete a legitimate interests assessment.

If you are processing data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, data concerning a person's sex life or sexual orientation or data relating to criminal convictions or offences, you will also need to state a further basis for that processing – you can find a list of these in GDPR Article 9 and 10.

~~User is briefed on speech recognition as part of on-boarding process. Online speech recognition is disabled by default on an MMD device.~~

The lawful basis for processing is Article 6(1)(f) – legitimate interests. For the processing of any special categories of personal data the the lawful basis is Article 9(2) XXXX

Commented [SJ10]: A legitimate interest assessment will be needed

Commented [SJ11]: Need to confirm appropriate lawful basis once we know more about why we want to use this functionality.

1.6 Mandatory requirements

Guidance: Add the following requirements to your project backlog unless they do not apply (e.g. data need not be kept up to date in a system for storing old records). Section 4 can be used to check that these have been completed, particularly if delivery is not being managed as a project.

Data Accuracy

a) Data must be kept up to date
b) There must be means to validate the accuracy of any personal data collected
c) Inaccurate or incomplete personal data must be updated on receipt of a lawful request from the data subject

Retention & Deletion

d) All data collected will have a retention period
e) Data must be deleted at the end of its retention period
f) Personal data must be erased upon receipt of a lawful request from the data subject

Information & Transparency

g) The data subjects shall be provided with:
(i) The identity and contact details of the data controller;
(ii) The purposes of the processing, including the legal basis and legitimate interests pursued
(iii) Details of the categories of personal data collected
(iv) Details of the recipients of personal data

Objection & Restriction

h) There must be means to restrict the processing of data on receipt of a lawful request from the data subject
i) There must be means to stop the processing of data on receipt of a lawful request from the data subject

Security

j) Appropriate training and instructions will be put in place to enable staff to operate the new system / process securely
k) Identify an Information Asset Owner
l) Update the Information Asset Register

Is the data being transferred outside the UK and EEA? If so:

m) The data subjects must be provided with information on where to obtain details of any safeguards over data transferred to non-GDPR compliant countries
n) Consult the DPO for additional requirements to ensure the processing is GDPR compliant.

Is the data being transferred to or through another organisation? If so:

o) There must be controls to ensure or monitor compliance by external organisations.

Is consent or pursuit of a contract the lawful basis for an automated processing operation? If so:

p) There must be a means to extract and transmit the data in a structured, commonly used and machine-readable format on receipt of a lawful request from the data subject
q) The consent must be recorded in some manner to serve as evidence

Does our Privacy Notice need to be updated? If so:

r) *Update the Privacy Notice*

DRAFT

2. Data protection assessment screening

Guidance: The purpose of the screening questions is to determine if a DPIA is required. As a data controller we are required to perform DPIAs where the processing is likely to result in a high risk to the rights and freedoms of individuals (Article 35 refers).

2.1 Screening questions

ID	Criteria	Y/N
1	Will the processing involve evaluation or scoring, including profiling or predicting, especially in relation to an individual's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements?	N
2	Will the processing involve automated decision making that will have a legal or similar detrimental effect on individuals? For example, decisions that lead to exclusion or discrimination.	N
3	Will the processing involve the systematic monitoring of individuals in a publicly accessible area? For example, surveillance cameras in a shopping centre or train station.	N
4	Will the processing involve sensitive personal data or data of a highly personal nature? For example, special categories of data (Article 9 refers), personal data relating to criminal convictions or offences (Article 10 refers), and personal data linked to household and private activities.	~~N~~Y
5	Does the processing involve large scale processing of data at a regional, national or supranational level, and which could affect a large number of data subjects?	N
6	Does the processing involve matching and combining two or more datasets that have been collected for different purposes and/or by different data controllers?	N
7	Does the processing concern vulnerable individuals who may be unable to easily give consent or object to the processing? For example, children, employees, and others who require special protection (mentally ill persons, asylum seekers, patients, the elderly).	N
8	Does the processing involve the innovative use or application of new technological or organisational solutions? For example, "Internet of Things" applications can have significant impacts on subjects' daily lives and privacy.	N
9	Does the processing prevent individuals from exercising a	N

Commented [SJ12]: Potentially Yes depending on PD involved

DRAFT

	rights or using a service or contract? For example, where a bank screens its customers again credit reference database in order to decide whether to offer them a loan.	

Guidance: If you answer "Yes" to one or more questions you should complete a DPIA. If you answer "No" to all questions please proceed to section 6.

2.2 DPIA approach and consultation

Commented [SJ13]: Needs completion

Guidance: Record which parts of the DPIA you will be completing and your rationale (especially if your choices differ from the guidance above).

Explain what practical steps you will take to ensure that you identify and address the data protection risks. Include details of:

- *Who should be consulted, internally and externally? This must include the DPO's team and Cyber Security. You should also consult data subjects or their representatives unless this is not possible or appropriate – e.g. it would be disproportionate, impractical, undermine security or compromise commercial confidentiality.*
- *If data subjects (or their representatives) will not be consulted you must document the reasons for this.*
- *How you will carry out the consultation. You should link this to the relevant stages of your project management process or delivery plan.*

Microsoft documentation and privacy policy reviewed, alternate software offerings and costs identified.

Formatted: Font: Not Bold

Review of administrative controls for Speech Recognition in MMD and Intune Portals completed – currently immature. Enhancement request to allow centralised management of Speech Recongition controls in progress with Microsoft.

DRAFT

3. Data inventory

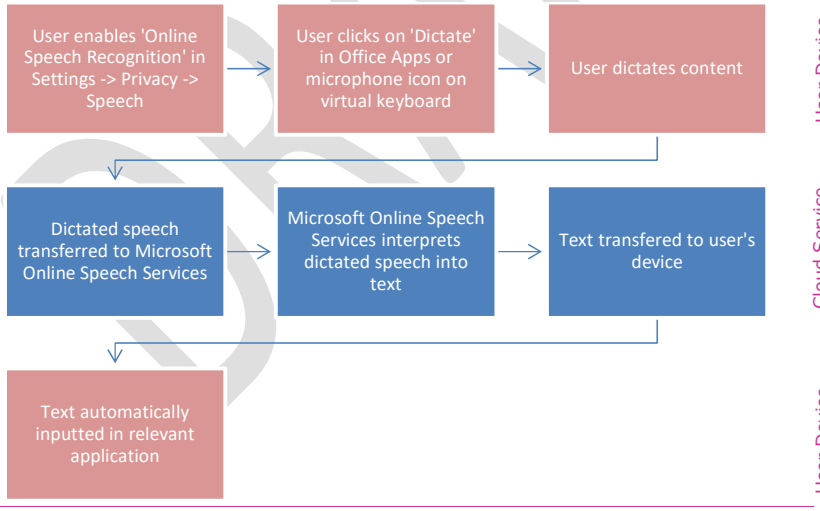
3.1 Information flows

Commented [SJ14]: Needs completing

Guidance: Provide a systematic description of the processing, including:

- *Whether data collected is personal data*
- *The source of the data (including whether the data subjects are vulnerable, the relationship with the data subjects, the manner of collection and the level of control the data subjects have over the data once collected)*
- *The nature and context of the processing (including whether there are new technological developments or any relevant current issues of public concern)*
- *The scope of the processing (including the nature and volume of data, frequency and duration of processing, sensitivity of the data and the extent of the processing)*
- *The storage and transfer of the data (including details of hardware, software, networks, key people and details of any paper records or transmission channels)*
- *Responsibilities for the data (including the information asset owners, how responsibilities for information change through the data flow and the boundaries of responsibilities in any handover)*

You may find it useful to refer to a flow diagram or other way of explaining information flows. You should also say how many individuals are likely to be affected by the processing of personal data.



Formatted: Font: 9 pt
Formatted: Centered
Formatted: Centered
Formatted: Font: 9 pt
Formatted: Font: 9 pt
Formatted: Centered

3.2 Data inventory

Guidance: Identify the personal data to be held, the recipients (those with access to the data), the retention period and the necessity of the data collection, processing and retention.

Data Type	Recipients	Retention Period	Necessity
Speech data (audio recordings) when user opts into to Online speech recognition.	Microsoft speech recognition servers.	Aggregated, anonymised voice data is stored indefinitely unless a user opts to delete records via the Microsoft Privacy Portal.	This is used when a user opts into online speech recognition in order to improve the efficiency of the speech recognition.
Calendar and contact information	Microsoft speech recognition servers.	Aggregated, anonymised voice data is stored indefinitely unless a user opts to delete records via the Microsoft Privacy Portal.	This is used when a user opts into online speech recognition in order to improve the efficiency of the speech recognition.
Personal data / special category data recorded when dictated	Microsoft speech recognition servers.	Aggregated, anonymised voice data is stored indefinitely unless a user opts to delete records via the Microsoft Privacy Portal.	This is used when a user opts into online speech recognition in order to improve the efficiency of the speech recognition.

Commented [IEM15]: Are staff suitably informed about those choices?

Commented [NS16R15]: The information is clear when a user opts to activate the service

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

DRAFT

4. Compliance measures

Use this section to record your compliance with the requirements in section 1.5. Fill in the details of how the requirements have been met or list the requirement as N/A. The requirement source is a reference to GDPR unless otherwise stated.

Requirement	Implementation Details
Data Accuracy	
a) Data must be kept up to date	n/a
b) There must be means to validate the accuracy of any personal data collected	n/a – personal data is not collected as part of this process Personal calendar appointments may be converted to speech by this service. This data is a literal speech conversion of the data that the user has entered into their calender.
c) Inaccurate or incomplete personal data must be updated on receipt of a lawful request from the data subject	n/a
Retention & Deletion	
d) All data collected will have a retention period	
e) Data must be deleted at the end of its retention period	
f) Personal data must be erased upon receipt of a lawful request from the data subject	Data can be deleted by a user through the Microsoft Privacy Portal.
Information & Transparency	
g) The data subjects shall be provided with: • the identity and contact details of the data controller; • the contact details of the Data Protection Officer; • the purposes of the processing, including the legal basis and legitimate interests pursued • details of the categories of personal data collected • details of the recipients of personal data	Information is provided to users during the device onboarding process
Objection & Restriction	
h) There must be means to restrict the processing of data on receipt of a lawful request from the data subject	User must 'activate' speech recognition and opt in to online speech recognition.
i) There must be means to stop the processing of data on receipt of a lawful request from the data subject	User must 'activate' speech recognition and opt in to online speech recognition, this can be turned off at any time.
Security	
j) Appropriate training and instructions will be put in place to enable staff to operate the new	~~Information is provided to users during the device onboarding process, ICO staff are available during on-boarding to support the process. Microsoft~~

Commented [SJ17]: Need to clarify personal data involved before we can consider comoliance measures and risk assessment

Commented [IEM18]: Not sure this is accurate, voice identification is PD! Also all information on calendar for example hospital appointment etc

Commented [NS19R18]: It's not voice identification as it isn't fingerprinting your voice and using it's unique characteristics to assign an identity to it. It's transcribing your speech which is a different thing.

Commented [IEM20]: Any clear written guifdance about privacy controls, for example switching off cloud recognition or deleting voice data?

DRAFT

system / process securely	~~Windows has detailed instructions to support the user during the process.~~User guidance to be issued on the privacy implications of this service, once a determination has been made over it's appropriateness for the ICO.
k) Identify an Information Asset Owner	IAO is Michael Fitzgerald.
l) Update the Information Asset Register	
Conditional Requirements	
m) The data subjects must be provided with information on where to obtain details of any safeguards over data transferred to non-GDPR compliant countries	Data is covered by Privacy Shield.
n) Consult the DPO for additional requirements to ensure the processing is GDPR compliant.	
o) There must be controls to ensure or monitor compliance by external organisations.	
p) There must be a means to extract and transmit the data in a structured, commonly used and machine-readable format on receipt of a lawful request from the data subject	Data can be accessed, downloaded or deleted via the Microsoft Privacy Portal.
q) The consent must be recorded in some manner to serve as evidence	
r) Update the Privacy Notice	

Commented [IEM21]: Is this all covered by privacy shield ?

DRAFT

5. Data protection risk assessment

Guidance: Identify and assess the risks to subjects' rights, the actions you could take to reduce the risks and any future steps that will be necessary (eg the production of new guidance or security testing for new systems). Some example risk sources have been listed to aid you. This list is not comprehensive and will not necessarily apply to your system or process. See Appendix for guidance on assessing impact and probability.

Risks should be considered from the data subject's perspective not the ICO's (eg a reputational risk to the ICO should not be recorded here). Some example threats to consider include:

- *Discrimination*
- *Identity theft and fraud*
- *Financial loss*
- *Damage to data subjects' reputation*
- *Loss of confidentiality of professional secrets*
- *Unauthorised reversal of pseudonymisation*
- *Social or economic disadvantage*
- *Deprivation of legal rights or freedoms*
- *Data subjects losing control over their data*
- *Loss of privacy or intrusion into private life*
- *Prevention from accessing services*

Risk Details	**Impact**	**Probability**	**Response**
[Guidance: Describe risks to data subjects]	*[Guidance: Describe consequences to data subjects if risk realised]*	*[Guidance: Describe likelihood that risk will be realised]*	*[Guidance: Describe risk treatment (eg reduce, avoid, accept or transfer)]*
Processing – A user opts into online speech recognition and dictates confidential information, which cannot be processed by the server and is consequently heard by a Microsoft employee.	Microsoft employee becomes aware of potentially confidential information.	Medium	Accept - Issue guidance that 'online speech recognition' is not suitable for confidential material. Microsoft employees bound by non-disclosure agreements so unlikely that they will act on the information that they receive.
Illegitimate Access to Data – A user opts into online speech recognition	Potentially confidential information is overheard by	Low – Microsoft have access controls in place to prevent this	Accept - Issue guidance that 'online speech recognition' is not

Commented [IEM22]: Has this already been issued?

Commented [IEM23]: What are they?

and a rogue Microsoft employee accesses stored voice recordings.	Microsoft employee	from happening. Microsoft Employees are only given 10 seconds of audio to analyse, audio is analysed in a secure Microsoft facility and association between audio file and a specific user is obfuscated.	suitable for confidential material. Microsoft employees bound by non-disclosure agreements so unlikely that they will act on the information that they receive.

DRAFT

6. Residual risk and sign off

6.1 Residual risk

Guidance: Record details of the remaining risk. It is never possible to remove all risk so this section should not be omitted or blank. If the residual risk remains high (e.g. red on the traffic light scoring in the Appendix) then you will need to consult the ICO by following the process used by external organisations.

6.2 Necessity and proportionality

Guidance: If you answered "Yes" to one or more of the screening questions in Section 2.1 you should discuss the necessity and proportionality of the collection, processing and retention of this data here, weighing the impact on data subjects rights and freedoms against the benefits of the processing activity. You should also consider whether there are other reasonable ways to achieve the same result with less impact on data subjects. If you have not answered "Yes" to any of the screening questions in Section 2.1 you can leave this section blank.

6.3 DPO recommendations

Guidance: Record any recommendations from the DPO or their delegates and responses here. This serves as useful tool when reconsidering a rejected DPIA or in recording the justification if the organisation rejects the DPO's advice.

No	Recommendation	Project Team Response
1	[Record any changes recommended by the DPO here]	[Record the actions taken as a result of the recommendation]

6.4 Sign Off

Guidance: Send this to the DPSIA Committee to approve the privacy and security risks involved in the project, the solutions to be implemented and the residual risk.

Approved by	Role	Date	Project Stage
	DPO		
	Head of Cyber Security		
	[Add others as necessary]		

7. Integrate the outcomes back into the plan

Guidance: Who is responsible for integrating the DPIA outcomes back into any project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any data protection concerns which may arise in the future?

Action to be taken	Date for completion	Responsibility for Action	Completed Date

Contact point(s) for future data protection concerns	

8. Change history

Guidance: To be completed by the person responsible for delivering the system, service or process (in a project this will be the project manager).

Version	Date	Author	Change description

9. Template Document control

Title	Data Protection Impact Assessment Template
Version	1.1
Status	Final release
Owner	DPSIA Committee
Release date	02/04/19
Review date	10/12/20

DRAFT

Appendix: Risk Assessment Criteria
The following criteria are aligned with our corporate risk assessment criteria.

Impact
Impact is the consequence of a risk to the rights and freedoms of individuals being realised. Factors to consider include the financial harm or emotional distress that can be expected to occur.

Impact	Scoring criteria
Very low (1)	No discernible impact on individuals.
Low (2)	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc).
Medium (3)	Individuals may encounter significant inconveniences, which they will overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc)
High (4)	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc).
Very high (5)	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Probability
Probability is the likelihood of a risk to the rights and freedoms of individuals being realised. Factors to consider include the expected frequency of occurrence, and the motivation and capability of threat sources (eg does the threat require insider knowledge and/or significant technical resources to exploit any vulnerability?).

Probability	Scoring criteria
Very low (1)	0-5% - extremely unlikely or improbable For example, the risk has not occurred before or is not expected to occur within the next three years.
Low (2)	6-20% - low but not improbable For example, the risk is expected to occur once a year.
Medium (3)	21-50% - fairly likely to occur For example, the risk is expected to occur several times a year.

High (4)	51-80% - more likely to occur than not For example, the risk is expected to occur once a month.
Very high (5)	81-100% - almost certainly will occur For example, the risk is expected to occur once a week.

Risk level
Risk level is a function of impact and probability, and is represented by a RAG rating.

Probability / Impact	Very low (1)	Low (2)	Medium (3)	High (4)	Very high (5)
Very high (5)	Amber (5)	Amber (10)	Red (15)	Red (20)	Red (25)
High (4)	Green (4)	Amber (8)	Amber (12)	Red (16)	Red (20)
Medium (3)	Green (3)	Amber (6)	Amber (9)	Amber (12)	Red (15)
Low (2)	Green (2)	Green (4)	Amber (6)	Amber (8)	Amber (10)
Very low (1)	Green (1)	Green (2)	Green (3)	Green (4)	Amber (5)

Risk acceptance criteria
These criteria are guidelines only, and any risk treatment decisions should be made on a case-by-case basis. For example, it may be prudent to reduce a low risk because of legal and regulatory requirements.

Risk level	Acceptance criteria
Low (Green)	Within this range risks can be routinely accepted.
Medium (Amber)	Within this range risks can occasionally be accepted but shall be kept under regular review.
High (Red)	Within this range risks shall not be accepted and immediate action is required to reduce, avoid or transfer the risk.

Case reference

IC-203321-W1K8

Microsoft Managed Desktop - DPIA

ico.
Information Commissioner's Office

Data Protection Impact Assessment (DPIA) template

You should complete this template where there is a new (or significant change to an existing) service or process that involves the storage/processing of personal data (whether digital or hardcopy). When dealing with an existing process, service or system **only the change should be impact assessed.**

The DPO's team is available to assist and advise on completing this template.

The template should be submitted to the DPSIA Committee for their recommendations and approval.

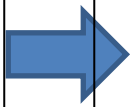
You should start to complete the template as soon as you decide to implement a new system or process. How frequently the DPIA is reviewed and the governance required will vary with the risk of the system or process. At a **minimum**:

Projects: you should produce an initial DPIA prior to finalising your requirements, complete it before finalising your design and review & update the DPIA at least once more prior to go-live. In an Agile project, you should update the DPIA at the start and end of each Epic, or where there is a significant change to the data being processed or the technology or platform. Each update should be submitted to the DPSIA Committee.

Non-projects: you should complete the DPIA prior to designing the service or seeking suppliers and update it whenever there are material changes to the planned system or process.

Screening: Determine what to complete:

1. **GDPR DPIA**: Complete all sections if you meet 2+ questions in section 2.1
2. **Full DPIA**: Complete everything but section 6.2 if you meet 2+ screening questions in any section
3. **Compliance Checklist**: Complete sections 1, 2 and 4, plus signoff, if you don't meet the screening questions



Approval: Consult the DPO's team and select an option for the approvers based on your risk:

1. **DPSIA Committee**: including Senior Information Risk Officer, Head of Cyber Security, DPO
2. **DPSIA Committee**: including DPO and Head of Cyber Security
3. Representatives of DPO and Cyber Security, who will also send it to the DPSIA Committee for their information

Regardless of the option chosen, **the DPIA should be submitted together with your SIA**.

1. Process/system overview

1.1 Summary

Guidance: For projects please provide the following key details. Non-projects should provide a key contact who is responsible for delivering the system or process.

Project ID:	N/A
Project Title:	Microsoft Managed Desktop
Project Manager:	Debra Holt

1.2 Synopsis

Guidance: Provide a summary of the process or system including any relevant background information and the key aims/objectives that the system or process must achieve. There is no need for a detailed discussion of data or data flows – these are covered later in the assessment.

The Microsoft Managed Desktop programme is currently an invite only programme where Microsoft takes responsibility for the configuration, imaging, application deployment, software updates, security and end user support of a device. The service is made up of a combination of existing Microsoft services with an additional monitoring, management and support wrapper.

The components can be summarised as follows;

- Microsoft 365 E5
    - Office 365 E5
    - Windows 10 Enterprise E5
    - Enterprise Mobility + Security E5
- Microsoft Managed Desktop IT as a Service
    - Microsoft Support
    - Microsoft Operations & Monitoring
- A Microsoft Surface Device

DPSIA's have already been completed for the following areas;

- Office 365 including Enterprise Mobility + Security

Additional DPSIA's will be completed for;

- Microsoft Get Help 24x7 Support
- Microsoft Cortana Voice Recognition
- Windows Hello

Scope of DPSIA

- Microsoft Diagnostic Data to support Advanced Threat Protection, Advanced Threat Hunting.
- Microsoft Advanced Identity Protection

Device Management, Security & Monitoring

The Microsoft Defender application installed on the Microsoft Managed Desktop Device monitors the device for activity on the device that may cause a threat to the device or the organisation.
Defender uses four levels of response to protect the ICO's devices, users and reputation;

1. Automatic quarantining of known events, processes or software based on local processing – If the software installed on the device recognises an event, process or attempt to install software that is indicative of an attempt to compromise the device, then the locally installed software takes action to quarantine the event, process or software. This level of detection is typically associated with common malware and viruses.
2. Automatic quarantining of events, processes or software based on cloud processing – If detected events match known patterns on new and emerging threats, then the Defender Cloud will automatically quarantine the associated event, process or software. This level of detection is associated with new and emerging threats being detected globally across all Microsoft Defender users.
3. Security Operations Centre initiated quarantining of device – If events or processes detected on the device match a pattern that would suggest there is an active attempt to compromise a device, then an alert is triggered at the Microsoft 24x7 Security Operations Centre, currently based in Seattle. A SOC agent then makes an interpretation of that data and responds appropriately. Either contacting a security representative of the ICO to alert them of the unusual behaviour or initiating a quarantine of the device and user, to prevent them from harming other devices / users within the ICO.
4. Microsoft Threat Experts – Artificial intelligence based analysis of device and user activity to detect advanced, targeted attacks and cyber espionage. This analysis can lead to advice and guidance from Microsoft Cyber Security Experts in the event of an incident. These Cyber Security Experts will speak to both the ICO and the Microsoft SOC to help determine the best course of action if such an event occurs.

These aspects of Microsoft Advanced Threat Protection all leverage the 'Enhanced' diagnostic data provided by an MMD device.

Advanced Identity Protection

The Microsoft Advanced Identity Service monitors and analyses user activities and information across the network, such as permissions and group membership, creating a behavioural baseline for each user. This data is used by the AIP service only and cannot be extracted or reported upon, however the component information gathered is non-invasive and could be viewed at the component level by IT Administrators as part of standard administration tasks.

Anomalies are identified with adaptive built-in intelligence, giving insights into suspicious activities and events, revealing the advanced threats, compromised users, and insider threats we face facing your organization.

The Microsoft service can take pro-active action such as automatically locking accounts, prompting for credential changes or additional authentication factors

when it believes that an account is compromised, being actively misused or under threat of compromise.

Diagnostic data

Devices will be set to provide enhanced diagnostic data to Microsoft under a known commercial identifier. As part of Microsoft Managed Desktop, IT admins cannot change these settings.

Enhanced Diagnostic Data

The Enhanced level gathers data about how Windows and apps are used and how they perform. This level also includes data from both the **Basic** and **Security** levels. This level helps to improve the user experience with the operating system and apps. Data from this level can be abstracted into patterns and trends that can help Microsoft determine future improvements.

This level is needed to quickly identify and address Windows quality issues.

The normal upload range for the Enhanced diagnostic data level is between 239 KB - 348 KB per day, per device.

The data gathered at this level includes:

- **Operating system events**. Helps to gain insights into different areas of the operating system, including networking, Hyper-V, Cortana, storage, file system, and other components.

- **Operating system app events**. A set of events resulting from Microsoft applications and management tools that were downloaded from the Store or pre-installed with Windows including Photos, Mail, and Microsoft Edge.

- **Some crash dump types**. All crash dump types, except for heap dumps and full dumps.

If the Connected User Experiences and Telemetry component detects a problem on Windows 10 that requires gathering more detailed instrumentation, the Connected User Experiences and Telemetry component at the **Enhanced** diagnostic data level will only gather data about the events associated with the specific issue.

This level of data collected is similar to that which can be collected through the use of a Security Incident and Event Monitoring tool that received logs from end user devices and other security monitoring tools such as 'FireEye'.

This data is used to enhance the security of the ICO's Microsoft Managed Desktop estate and the security and reliability of all Microsoft Windows devices.

A full catalogue of data provided to Microsoft under the 'Enhanced' diagnostic data level is provided in the data inventory.

1.3 Definition of processing

Guidance: As a data controller we are required to maintain a "record of processing activities" for which we are responsible (Article 30 refers). The following table is designed to help us define the planned processing operation.

Data controller(s)	ICO
Data processor(s)	Microsoft
Purpose of processing	Security Information and Event Management
Categories of data	Internal IP Address (ICO) External IP Address (ICO Proxy) Username (ICO Staff) Device Name (Randomly Assigned) User Login Activity (username, time of login, success / failure) Applications Downloaded Applications Launched Blocked Security Events (Applications or files that have been blocked / quarantined and the reason)
Categories of subjects	ICO Staff / Device Usage
Categories of recipients	Microsoft acting on behalf of the ICO to manage the security and stability of the ICO devices
Overseas transfers	Microsoft Security Operations Centre is based in Redmond, Seattle, USA. Microsoft has a current certification to privacy shield.

1.4 Purpose for processing

Guidance: State the legitimate interest being pursued in the processing, including the purposes, aims and the intended benefits for you, data subjects, society or others.

The data is processed in order to enhance the security posture of all devices within the Microsoft Managed Desktop programme and all other devices utilising Microsoft Advanced Threat and Identity Protection services. Processing is to enhance the security of MMD devices and will not be used routinely to track user workplace performance. This information could be made available to aid a workplace investigation upon instruction and approval of Human Resources.

1.5 Lawful basis

Guidance: State the basis on which the processing is lawful under GDPR Article 6 (consent, performance of contractual obligations to a data subject, compliance with legal obligations, public interest, exercise of official authority, or protecting the vital interests of a natural person).

If you are processing data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, data concerning a person's sex life or sexual orientation or data relating to criminal convictions or offences, you will

also need to state a further basis for that processing – you can find a list of these in GDPR Article 9 and 10.

Processing of this data is required to allow Microsoft to perform their contractual obligations regarding security monitoring and end user support of Microsoft Managed Desktop Devices.

The lawful basis for processing is Article 6(1)(e) – public task.

1.6 Mandatory requirements

Guidance: Add the following requirements to your project backlog unless they do not apply (e.g. data need not be kept up to date in a system for storing old records). Section 4 can be used to check that these have been completed, particularly if delivery is not being managed as a project.

<u>Data Accuracy</u>
a) Data must be kept up to date
b) There must be means to validate the accuracy of any personal data collected
c) Inaccurate or incomplete personal data must be updated on receipt of a lawful request from the data subject

<u>Retention & Deletion</u>
d) All data collected will have a retention period
e) Data must be deleted at the end of its retention period
f) Personal data must be erased upon receipt of a lawful request from the data subject

<u>Information & Transparency</u>
g) The data subjects shall be provided with:
(i) The identity and contact details of the data controller;
(ii) The purposes of the processing, including the legal basis and legitimate interests pursued
(iii) Details of the categories of personal data collected
(iv) Details of the recipients of personal data

<u>Objection & Restriction</u>
h) There must be means to restrict the processing of data on receipt of a lawful request from the data subject
i) There must be means to stop the processing of data on receipt of a lawful request from the data subject

<u>Security</u>
j) Appropriate training and instructions will be put in place to enable staff to operate the new system / process securely
k) Identify an Information Asset Owner
l) Update the Information Asset Register

<u>Is the data being transferred outside the UK and EEA? If so:</u>
m) The data subjects must be provided with information on where to obtain details of any safeguards over data transferred to non-GDPR compliant countries

n) Consult the DPO for additional requirements to ensure the processing is GDPR compliant.

<u>Is the data being transferred to or through another organisation? If so:</u>
o) There must be controls to ensure or monitor compliance by external organisations.

<u>Is consent or pursuit of a contract the lawful basis for an automated processing operation? If so:</u>
p) There must be a means to extract and transmit the data in a structured, commonly used and machine-readable format on receipt of a lawful request from the data subject
q) The consent must be recorded in some manner to serve as evidence

<u>Does our Privacy Notice need to be updated? If so:</u>
r) *Update the Privacy Notice*

2. Data protection assessment screening

Guidance: The purpose of the screening questions is to determine if a DPIA is required. As a data controller we are required to perform DPIAs where the processing is likely to result in a high risk to the rights and freedoms of individuals (Article 35 refers).

2.1 Screening questions

ID	Criteria	Y/N
1	Will the processing involve evaluation or scoring, including profiling or predicting, especially in relation to an individual's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements?	Y
2	Will the processing involve automated decision making that will have a legal or similar detrimental effect on individuals? For example, decisions that lead to exclusion or discrimination.	N
3	Will the processing involve the systematic monitoring of individuals in a publicly accessible area? For example, surveillance cameras in a shopping centre or train station.	N
4	Will the processing involve sensitive personal data or data of a highly personal nature? For example, special categories of data (Article 9 refers), personal data relating to criminal convictions or offences (Article 10 refers), and personal data linked to household and private activities.	N
5	Does the processing involve large scale processing of data at a regional, national or supranational level, and which could affect a large number of data subjects?	N

6	Does the processing involve matching and combining two or more datasets that have been collected for different purposes and/or by different data controllers?	N
7	Does the processing concern vulnerable individuals who may be unable to easily give consent or object to the processing? For example, children, employees, and others who require special protection (mentally ill persons, asylum seekers, patients, the elderly).	N
8	Does the processing involve the innovative use or application of new technological or organisational solutions? For example, "Internet of Things" applications can have significant impacts on subjects' daily lives and privacy.	N
9	Does the processing prevent individuals from exercising a rights or using a service or contract? For example, where a bank screens its customers again credit reference database in order to decide whether to offer them a loan.	N

Guidance: If you answer "Yes" to one or more questions you should complete a DPIA. If you answer "No" to all questions please proceed to section 6.

2.2 DPIA approach and consultation

Guidance: Record which parts of the DPIA you will be completing and your rationale (especially if your choices differ from the guidance above).

Explain what practical steps you will take to ensure that you identify and address the data protection risks. Include details of:

- *Who should be consulted, internally and externally? This must include the DPO's team and Cyber Security. You should also consult data subjects or their representatives unless this is not possible or appropriate – e.g. it would be disproportionate, impractical, undermine security or compromise commercial confidentiality.*
- *If data subjects (or their representatives) will not be consulted you must document the reasons for this.*
- *How you will carry out the consultation. You should link this to the relevant stages of your project management process or delivery plan.*

Work has been carried out with Microsoft to understand the levels of diagnostic data consumed by the Microsoft Security Operations Centre, why the data is collected and the reasons behind it's use. A full list of the diagnostic data is available below. Consultation will also take place internally with the DPO and their team and cyber security.

3. Data inventory

3.1 Information flows

Guidance: Provide a systematic description of the processing, including:
- *Whether data collected is personal data*
- *The source of the data (including whether the data subjects are vulnerable, the relationship with the data subjects, the manner of collection and the level of control the data subjects have over the data once collected)*
- *The nature and context of the processing (including whether there are new technological developments or any relevant current issues of public concern)*
- *The scope of the processing (including the nature and volume of data, frequency and duration of processing, sensitivity of the data and the extent of the processing)*
- *The storage and transfer of the data (including details of hardware, software, networks, key people and details of any paper records or transmission channels)*
- *Responsibilities for the data (including the information asset owners, how responsibilities for information change through the data flow and the boundaries of responsibilities in any handover)*

You may find it useful to refer to a flow diagram or other way of explaining information flows. You should also say how many individuals are likely to be affected by the processing of personal data.

- Microsoft's Intelligent Security Graph analyses user activity (date, times, IP address, location, number of successful / failed logons, data accessed, emailed or deleted) to produce a baseline of 'normal' behaviour for an individual user. Microsoft can proactively alert, lock out, block or request additional authentication factors if 'unusual' activity is detected.
- Microsoft's Intelligent Security Graph compares accounts credentials against published lists of compromised credentials. If user credentials appear on compromised lists then Microsoft can proactively force a password change on an account where it believes the credentials have been compromised.
- Microsoft's Intelligent Security Graph can prevent a user from changing their password to common passwords as determined by lists of compromised passwords gathered at global level.
- If a device under Microsoft's protection is compromised then Microsoft's Intelligent Security Graph quarantine the device and will ensure that all devices covered under its 'Advanced Threat Detection' are pro-actively immunised against to prevent spread.

Data is transferred directly from the device to the Microsoft Security Operations Centre and is an accurate representation of the security and event activities of the end user device. The level of data transferred is similar to that of other Security Information and Event Management (SIEM) solutions focussed on end user devices.

The information transferred to Microsoft is stored for 90 days as standard and can be extended at the ICOs request if the data is required to assist in the investigation of security incidents.

3.2 Data inventory

Guidance: Identify the personal data to be held, the recipients (those with access to the data), the retention period and the necessity of the data collection, processing and retention.

Data Type	Recipients	Retention Period	Necessity
User name	Microsoft Security Information and Event Management within the Microsoft Security Operations Centre	Username is attached to each recorded event. Each event is retained for 90 days as standard before automatic deletion and can be extended to support security investigations if required.	Required to provide security information and event management on behalf of the ICO
IP Address	Microsoft Security Information and Event Management within the Microsoft Security Operations Centre	IP Address is attached to each recorded event. Each event is retained for 90 days as standard before automatic deletion and can be extended to support security investigations if required.	Required to provide security information and event management on behalf of the ICO
Application Activity – Application name executed, whether the application was allowed or blocked by the ICO Application Whitelisting policy	Microsoft Security Information and Event Management within the Microsoft Security Operations Centre	Application activity is a specific event type. Each event is retained for 90 days as standard before automatic deletion and can be extended to support security investigations if required.	Required to provide security information and event management on behalf of the ICO
Configuration Changes – changes to	Microsoft Security Information and Event	Configuration changes is a specific event	Required to provide security information and

settings on the device. Including network, domain join and logging levels.	Management within the Microsoft Security Operations Centre	type. Each event is retained for 90 days as standard before automatic deletion and can be extended to support security investigations if required.	event management on behalf of the ICO

Microsoft Enhanced Diagnostic Data

A full list of the diagnostic data available to Microsoft is available here:

https://docs.microsoft.com/en-us/windows/privacy/enhanced-diagnostic-data-windows-analytics-events-and-fields

4. Compliance measures

Guidance: Use this section to record your compliance with the requirements in section 1.5. Fill in the details of how the requirements have been met or list the requirement as N/A. The requirement source is a reference to GDPR unless otherwise stated.

Requirement	**Implementation Details**
Data Accuracy	
a) Data must be kept up to date	User data is updated as part of ICO driven Joiner, Mover, Leaver processes. Device use and security data is gathered by Windows Defender Advanced Threat Protection and associated services.
b) There must be means to validate the accuracy of any personal data collected	Personal data is driven from ICO Active Directory which is kept updated in line with ICO JML processes.
c) Inaccurate or incomplete personal data must be updated on receipt of a lawful request from the data subject	This process is handled through the ICO JML process & the active directory can be updated in the event of a lawful request being received.
Retention & Deletion	
d) All data collected will have a retention period	Provided above
e) Data must be deleted at the end of its retention period	Automatically deleted by Microsoft.
f) Personal data must be erased upon receipt of a lawful request from the data subject	Processed by Microsoft through the compliance portal. Microsoft to act on our instructions to erase data if a lawful request is received by us.
Information & Transparency	
g) The data subjects shall be provided with:	ICO will issue statement to users about Microsoft Managed Desktop service data

● the identity and contact details of the data controller; ● the contact details of the Data Protection Officer; ● the purposes of the processing, including the legal basis and legitimate interests pursued ● details of the categories of personal data collected ● details of the recipients of personal data	processing as part of the end user training. The ICO Privacy Policy will be updated as part of the project.
Objection & Restriction	
h) There must be means to restrict the processing of data on receipt of a lawful request from the data subject	Processed by Microsoft through the compliance portal. Microsoft to act on our instructions to restrict data if a lawful request is received by us.
i) There must be means to stop the processing of data on receipt of a lawful request from the data subject	Processed by Microsoft through the compliance portal. Microsoft to act on our instructions to cease processing of data if a lawful request is received by us.
Security	
j) Appropriate training and instructions will be put in place to enable staff to operate the new system / process securely	Full training is provided on the use of the Microsoft Managed Desktop Solution
k) Identify an Information Asset Owner	The Information Asset Owner is the Director of Digital, IT & Customer Contact.
l) Update the Information Asset Register	The Information Asset Register will be updated to reflect this.
Conditional Requirements	
m) The data subjects must be provided with information on where to obtain details of any safeguards over data transferred to non-GDPR compliant countries	ICO will issue statement to users about Microsoft Managed Desktop service data processing as part of the end user training.
n) Consult the DPO for additional requirements to ensure the processing is GDPR compliant.	Added to project backlog
o) There must be controls to ensure or monitor compliance by external organisations.	This forms part of the signed agreements with Microsoft.
p) There must be a means to extract and transmit the data in a structured, commonly used and machine-readable format on receipt of a lawful request from the data subject	
q) The consent must be recorded in some manner to serve as evidence	N/A
r) Update the Privacy Notice	

5. Data protection risk assessment

Guidance: Identify and assess the risks to subjects' rights, the actions you could take to reduce the risks and any future steps that will be necessary (eg the production of new guidance or security testing for new systems). Some example risk sources have been listed to aid you. This list is not comprehensive and will not necessarily apply to your system or process. See Appendix for guidance on assessing impact and probability.

Risks should be considered from the data subject's perspective not the ICO's (eg a reputational risk to the ICO should not be recorded here). Some example threats to consider include:

- *Discrimination*
- *Identity theft and fraud*
- *Financial loss*
- *Damage to data subjects' reputation*
- *Loss of confidentiality of professional secrets*
- *Unauthorised reversal of pseudonymisation*
- *Social or economic disadvantage*
- *Deprivation of legal rights or freedoms*
- *Data subjects losing control over their data*
- *Loss of privacy or intrusion into private life*
- *Prevention from accessing services*

Risk Details	**Impact**	**Probability**	**Response**
[Guidance: Describe risks to data subjects]	*[Guidance: Describe consequences to data subjects if risk realised]*	*[Guidance: Describe likelihood that risk will be realised]*	*[Guidance: Describe risk treatment (eg reduce, avoid, accept or transfer)]*
Risk of Microsoft Security Staff accessing ICO information inappropriately	High – Reputational Damage	Low	Microsoft vetting process provide assurances on staff.
Risk of SOC accidently quarantining or locking a non-malicious account	Low	Medium	Accepted risk, ICO can initiate reinstatement of device and account near instantly.

6. Residual risk and sign off

6.1 Residual risk

Guidance: Record details of the remaining risk. It is never possible to remove all risk so this section should not be omitted or blank. If the residual risk remains high (e.g. red on the traffic light scoring in the Appendix) then you will need to consult the ICO by following the process used by external organisations.

6.2 Necessity and proportionality

Guidance: If you answered "Yes" to one or more of the screening questions in Section 2.1 you should discuss the necessity and proportionality of the collection, processing and retention of this data here, weighing the impact on data subjects rights and freedoms against the benefits of the processing activity. You should also consider whether there are other reasonable ways to achieve the same result with less impact on data subjects. If you have not answered "Yes" to any of the screening questions in Section 2.1 you can leave this section blank.

6.3 DPO recommendations

Guidance: Record any recommendations from the DPO or their delegates and responses here. This serves as useful tool when reconsidering a rejected DPIA or in recording the justification if the organisation rejects the DPO's advice.

No	Recommendation	Project Team Response
1	[Record any changes recommended by the DPO here]	[Record the actions taken as a result of the recommendation]

6.4 Sign Off

Guidance: Send this to the DPSIA Committee to approve the privacy and security risks involved in the project, the solutions to be implemented and the residual risk.

Considered by	Date	Project Stage
DPIA Forum	20/02/2020	

7. Integrate the outcomes back into the plan

Guidance: Who is responsible for integrating the DPIA outcomes back into any project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any data protection concerns which may arise in the future?

Action to be taken	Date for completion	Responsibility for Action	Completed Date

Contact point(s) for future data protection concerns	

8. Change history

Guidance: To be completed by the person responsible for delivering the system, service or process (in a project this will be the project manager).

Version	Date	Author	Change description
V0.1		Neil Smithies	First draft

9. Template Document control

Title	Data Protection Impact Assessment Template
Version	1.0
Status	Final release
Owner	DPSIA Committee
Release date	10/12/18
Review date	10/12/20

Appendix: Risk Assessment Criteria
The following criteria are aligned with our corporate risk assessment criteria.

Impact
Impact is the consequence of a risk to the rights and freedoms of individuals being realised. Factors to consider include the financial harm or emotional distress that can be expected to occur.

Impact	Scoring criteria
Very low (1)	No discernible impact on individuals.
Low (2)	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc).
Medium (3)	Individuals may encounter significant inconveniences, which they will overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc)
High (4)	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc).
Very high (5)	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Probability
Probability is the likelihood of a risk to the rights and freedoms of individuals being realised. Factors to consider include the expected frequency of occurrence, and the motivation and capability of threat sources (eg does the threat require insider knowledge and/or significant technical resources to exploit any vulnerability?).

Probability	Scoring criteria
Very low (1)	0-5% - extremely unlikely or improbable For example, the risk has not occurred before or is not expected to occur within the next three years.
Low (2)	6-20% - low but not improbable For example, the risk is expected to occur once a year.
Medium (3)	21-50% - fairly likely to occur For example, the risk is expected to occur several times a year.

High (4)	51-80% - more likely to occur than not For example, the risk is expected to occur once a month.
Very high (5)	81-100% - almost certainly will occur For example, the risk is expected to occur once a week.

Risk level

Risk level is a function of impact and probability, and is represented by a RAG rating.

Probability / Impact	Very low (1)	Low (2)	Medium (3)	High (4)	Very high (5)
Very high (5)	Amber (5)	Amber (10)	Red (15)	Red (20)	Red (25)
High (4)	Green (4)	Amber (8)	Amber (12)	Red (16)	Red (20)
Medium (3)	Green (3)	Amber (6)	Amber (9)	Amber (12)	Red (15)
Low (2)	Green (2)	Green (4)	Amber (6)	Amber (8)	Amber (10)
Very low (1)	Green (1)	Green (2)	Green (3)	Green (4)	Amber (5)

Risk acceptance criteria

These criteria are guidelines only, and any risk treatment decisions should be made on a case-by-case basis. For example, it may be prudent to reduce a low risk because of legal and regulatory requirements.

Risk level	Acceptance criteria
Low (Green)	Within this range risks can be routinely accepted.
Medium (Amber)	Within this range risks can occasionally be accepted but shall be kept under regular review.
High (Red)	Within this range risks shall not be accepted and immediate action is required to reduce, avoid or transfer the risk.

Case reference

IC-203321-W1K8

Microsoft Teams – Draft DPIA

ico.
Information Commissioner's Office

Data Protection Impact Assessment – Microsoft Teams

Document Name	Data Protection Impact Assessment – Microsoft Teams
Author/Owner (name and job title)	Raymond Wong / Debra Holt
Department/Team	Business development Group
Document Status (draft, published or superseded)	Draft
Version Number	1.0
Release Date	
Approver (if applicable)	
Review Date	
Distribution (internal or external)	Internal

Guidance for completing this template

Complete this Data Protection Impact Assessment (DPIA) template if your DPIA screening assessment indicates a high risk to individuals. If you are unsure whether you need to complete a DPIA use the **DPIA Screening Assessment** to help you decide.

Aim to complete your DPIA as early as possible as the outcome of the assessment could affect the viability of your plans. In extreme cases, you will not be able to continue with your plans without changing them, or at all.

Guidance notes are included within the template to help you with its completion- just hover your mouse over any blue text for further information.

The Information Management Service is also available for further advice and support. Please keep in mind our service standards if you require advice.

1. Process/system overview

1.1 Ownership

Project Title:	Ways of Working – Microsoft Teams
Project Manager:	Raymond Wong
Information Asset Owner:	Mike Fitzgerald
Data controller(s)	ICO Microsoft - to the extent Microsoft processes personal data in connection with its own legitimate business operations, as described in the Online Services Terms, Microsoft will be an independent controller for such processing.
Data processor(s)	Microsoft

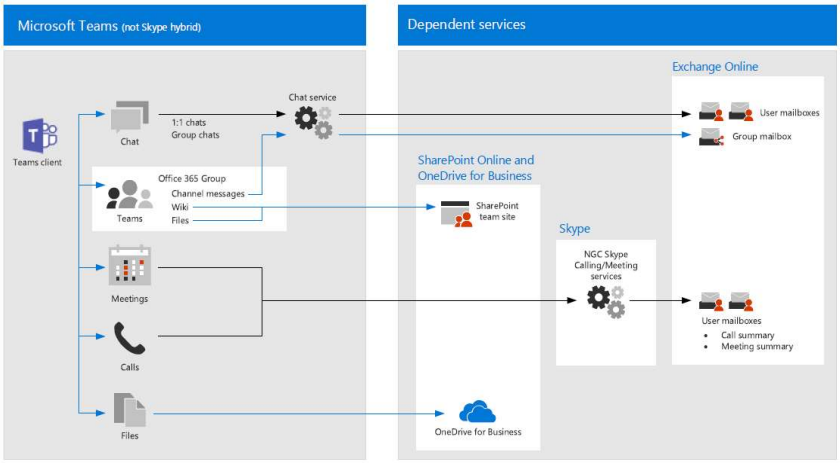
1.2 Describe your new service or process

Microsoft Teams is built on Microsoft 365 groups, Microsoft Graph, and has the same enterprise-level security, compliance, and manageability as the rest of Microsoft 365 and Office 365. Teams leverages identities stored in Azure Active Directory (Azure AD).
Teams utilizes existing services as part of O365 to offer telephony (including video conferencing and meeting services), instant messaging and email services with cloud storage facilities.

Microsoft Teams is central to the logical architecture of productivity services in Microsoft 365 - including data governance, security, and compliance capabilities.
The following PDF provides a diagram of the logical architecture of productivity services for Microsoft Teams;

msft-m365-teams-logical-architecture.pdf

Microsoft Teams is a central access point where new services or features on existing services are introduced. Due to the nature of Teams as a software as a service, data access and processes are not static and evolve with time.



Separate DPIA of Team features
Following documents cover the updated data protection assessment for specific features in team meetings/Stream including the changes to privacy notice.

- DPIA Team meetings/Recordings/Stream
- DPIA Enabling Teams Live Broadcast and Stream
- DPIA for GPA for teams
- Guest Access - DPIA screening assessment template

1.3 Personal data inventory - explain what personal data is involved

Categories of data	Data subjects	Recipients	Overseas transfers	Retention period
Usage Data Usage data includes information such as number of calls made, number of IMs sent or received, number of meetings joined, frequency of features used, and stability issues. • **Content:** Your meetings and conversations chats, voicemail, shared files, recordings and transcriptions. • **Profile Data:** Data that is shared within your company about you. Examples include your E-mail address, profile picture, and phone number. • **Call History:** A detailed history of the phone calls you make, which allows you to go back and review your own call records. **Census Data** is acquired solely to provide, support, and improve Skype for Business. Microsoft Teams, and Skype for Business Online. It includes environmental information such as device and operating system versions, and regional and language settings. It also	**Usage Data** ICO Staff in relation to Chat/Channel posts/ meeting in MS Team service. Calling data will be collected from internal calls to ICO staff using teams calls. (External calls are routed via skype). **Census/Error Reporting data** Diagnostic Data is collected on managed laptop devices. Census data may also be captured from corporate mobile devices.	Microsoft	Data is hosted in Microsoft's UK and/or EEA data centres.	Usage data is available for the la 180 days before it is automatical removed from the O365 tenant.

Commented [SJ1]: This is much better than the first draft but it is still confusing in the way you have set it out. These two pages of the Microsoft guidance are key

https://docs.microsoft.com/en-us/microsoftteams/teams-privacy

https://docs.microsoft.com/en-us/microsoftteams/data-collection-practices

You can effectively cut and paste into the DPIA.

At the minute you seem to be mixing the two pages together talking about personal data that is collected but also census, usage and error reporting data all in one.

See my attachment to my email for how I suggest you set this section out and you can then fill in the blanks for each row.

includes counters for sign-in attempts and failures **Error Reporting Data** • **Call Quality data:** Details of meetings and call data are available to your system administrators. This allows your administrators to diagnose issues related to poor call quality and service usage. • **Support/Feedback data:** Information related to troubleshooting tickets or feedback submission to Microsoft. • **Diagnostic and service: data** Diagnostic data related to service usage. This personal data allows Microsoft to deliver the service (troubleshoot, secure and update the product and monitor performance) as well as perform some internal business operations, such as: o Determine revenue o Develop metrics o Determine service usage o Conduct product and capacity planning Reference link:	Support tickets are not usually logged by ICO staff. This is an activity normally carried out by ITHelp.			

https://docs.microsoft.com/en-us/microsoftteams/data-collection-practices				

a. Identify a lawful basis for your processing

ICO

The lawful basis for processing under GDPR article 6 is 6(1)(e) – public task. ~~(f) legitimate interests. The legitimate interest assessment is here.~~

Where the processing in Document Storage involves special category data the GDPR Article 9 conditions for processing are:

* Art. 9(2)(b) & the DPA 2018 Schedule 1 conditions is ~~for processing are~~ 1(a)~~., 2 (2)(a) and (b).~~

* Art 9(2)(g) & the DPA 2018 Schedule 1 condition for processing is 6(1).

Our safeguards policy provides further detail about our processing of special category and criminal conviction data. Additionally our safeguards policy - sensitive processing for law enforcement purposes will apply for the storage of any relevant data in Office 365 document storage.

Microsoft

To the extent Microsoft processes personal data in connection with its own legitimate business operations, as described in the Online Services Terms, Microsoft will be an independent controller for such processing, the legal basis of which is legitimate interests.

~~https://docs.microsoft.com/en-us/microsoftteams/teams-privacy#legal-basis-of-processing~~

"Microsoft's legitimate business operations" consist of the following, each as incident to delivery of Microsoft Teams to the customer:

(1) billing and account management;
(2) compensation (e.g., calculating employee commissions and partner incentives)
(3) internal reporting and modelling (e.g., forecasting, revenue, capacity planning, product strategy)
(4) combatting fraud, cybercrime, or cyber-attacks that may affect Microsoft or Microsoft Products;
(5) improving the core functionality of accessibility, privacy or energy-efficiency
(6) financial reporting and compliance with legal obligations.

Formatted: Font: Bold

Commented [SJ2]: We'll need to double check this when it gets to forum.

Formatted: Hyperlink, Font: Bold, Font color: Auto

Formatted: Font: Bold

Formatted: Font: Verdana

Formatted: Font: Verdana

Formatted: Space Before: 0 pt, After: 0 pt

b. Explain why it is necessary to process this personal data

Microsoft Teams apps, collect data to help Microsoft understand how these products are being used and what kinds of errors, such as sign-in errors, have occurred. This diagnostic data can be used to troubleshoot and fix problem areas.

For specific teams services refer to links in section 1.2

Commented [SJ3]: This needs more detail about why it is necessary for us to use Microsoft Teams and process this data. So, in the context of 'ways of working' why do we feel it is necessary for the ICO to use teams. Doesn't have to be much just a few sentences.

c. Outline your approach to completing this DPIA

In 2018 ICO carried out a PSIA which covered the entire hosted Office 365 environment and the secure connectivity which links to the ICO's Core network. This was reviewed by Auriga consulting who provided a detailed realistic assessment of the privacy and security implications of the implementation of Microsoft Office 365 Core Cloud Product.

Microsoft teams service is part of O365 core product and leverages existing services including Exchange online for messaging, SharePoint online for file storage and management, Skype online for telephony services, Azure & MS Stream services for media and content distribution.

MS Teams is a Software as a services with features and services being released through out its lifecycle. Following a review in September 2020, a separate MS Team DPIA was created and uplifted from the Core Cloud services DPIA to be a central reference point for individual Teams services. This allowed for better management of different privacy and data protection concerns as each service used a different set of technologies not included in the original Core Cloud DPIA.

Commented [SJ4]: This needs some more detail about who you will be consulting with internally and externally as part of your completion of this DPIA. Additionally where appropriate GDPR requires controllers to consult with data subjects (so our staff in this case). I don't imagine we will be doing this so it could do with a line or two to explain why.

2.0 Data flows

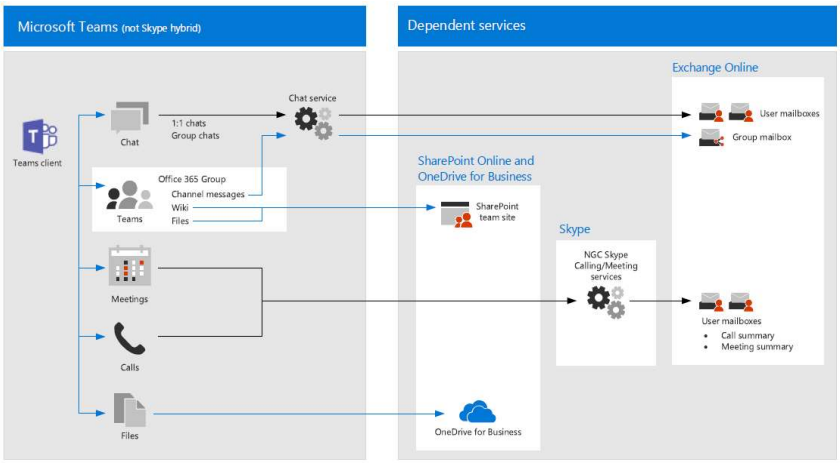
2.1 Provide a systematic description of your processing, from the point that the data is first collected through to its destruction.

If your plans involve the use of new technology you should explain how this technology works and outline any 'privacy friendly' features that are available.

The data in scope of this DPIA could be any documents currently created, received and stored within Teams.

The source of the documents could be any currently valid means of receiving or generating a document. For example, office applications (word, PowerPoint, OneNote, etc) created by employees.

Teams data storage will use different cloud services which are part of the office 365, these include OneDrive, Teams, SharePoint online, etc. See data flow diagram



Reference

msft-m365-teams-logical-architecture.pdf

Reference : https://docs.microsoft.com/en-gb/MicrosoftTeams/sharepoint-onedrive-interact

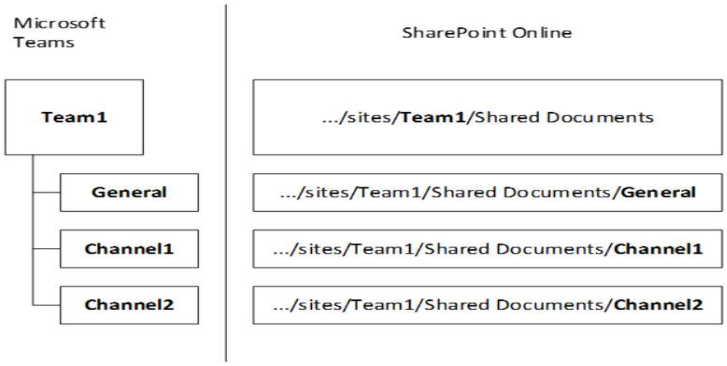
Commented [SJ5]: The personal data in scope is what you have set out in section 1.3.

Content but also profile data, call history, call quality data etc.

Some of this is relevant but you're not covering all of the personal data being processed.

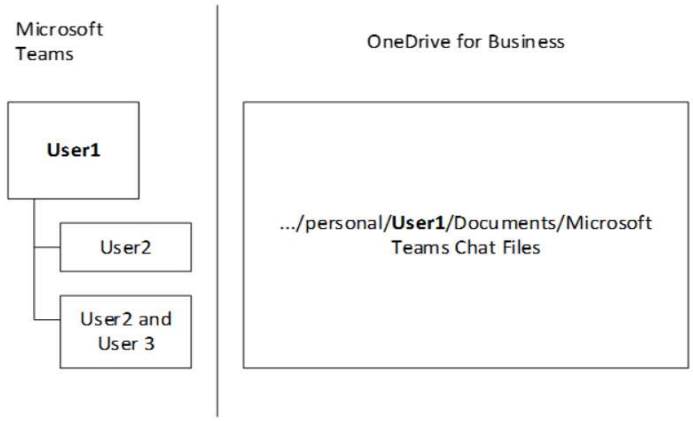
The following is the example of relationships between team, channel, and document library.

For every team, a SharePoint site is created, and the **Shared Documents** folder is the default folder creat the team. Each channel, including the **General** channel (the default channel for each team) has a folder ir **Documents**.



OneDrive: Retention will be 7 days for Team Chats

For every user, the OneDrive folder **Microsoft Teams Chat Files** is used to store all files shared within private chats with other users (1:1 or 1:many), with permissions configured automatically to restrict access to the intended user only.



No retention policy is applied to OneDrive.

EDRM will continue to be the central repository for electronic records. Teams is not the final storage location, and this is re-enforced through training and documented procedures.

- IM Risk & Recommendations MS Teams.docx

The transfer and storage of data utilises the same authentication and encrypted transfer and storage mechanisms as Office O365. The underlying

platform connectivity and security is common to all applications and all uses of Office 365.

High level responsibilities over the documents management in teams will fall on the team owner/creator. The overall security and retention/disposal policies applied to Teams will be managed by the Office 365 administrators.

At the lower level individual team users would have control over the adding, removing, editing and sharing of individual documents within their document stores in OneDrive and Teams. (Office 365 administrators will retain tenant wide management of external sharing features)

3.0 Key principles and requirements

Purpose & Transparency

1. Will you need to update our privacy notices?

Yes ☒ No ☐

2. If you are not updating our privacy notices how do you intend to communicate information about your processing to the data subjects?

3. If consent is your lawful basis for processing personal data are you maintaining appropriate records of the data subjects consent?

Yes ☐ No ☐ N/a ☒

4. If legitimate interests is your lawful basis for processing have you completed a legitimate interest assessment?

Yes ☐ No ☐☒ N/a ☒☐

If applicable please provide a link to your completed assessment.

Accuracy

5. Are you satisfied the personal data you are processing is accurate?

Yes ☒ No ☐

6. How will you ensure the personal data remains accurate for the duration of your processing?

In the context of personal data outlined in section 1.3 Diagnostic data will be collected at the time of usage, the data is not modified by any internal process and will remain unchanged and be accurate at the time it is collected.

Commented [SJ6]: This is good but what about all of the other data being processed?

7. If the personal data isn't being obtained directly from the data subject what steps will you take to verify accuracy?

N/A

Minimisation, Retention & Deletion

8. Have you done everything you can to minimise the personal data you are processing?

Yes ☒ No ☐

9. How will you ensure the personal data are deleted at the end of the retention period?

Usage data is automatically deleted after 180 days after usage in O365 tenant.

Commented [SJ7]: See comment above

10. Will you need to update the retention and disposal schedule?

Yes ☐ No ☒

Integrity and confidentiality

11. Where will the personal data be stored?

Usage data will be automatically collected and stored in the Office 365 tenant for the duration.

Commented [SJ8]: Don't' just limit this to usage data. As above you have other personal data being processed. I imagine this is the same for everything else too?

12. Are there appropriate access controls to keep the personal data secure?

Yes ☒ No ☐

13. Have you contacted the cyber security team for a security assessment of your plans?

Yes ☐ No ☒ N/a ☐

If applicable please provide a link to any assessment.

A separate Security opinions report for MS Teams will now be requested

14. Please explain the policies, training or other instructions you intend to put in place to enable staff to operate the new system or process securely.

Learning and development will delivery training, information management have provided guidance on how to use teams and the importance of moving documents to EDRM.

Commented [SJ9]: If you can link to the relevant materials here that would improve the DPIA

Accountability

15. Who will be the Information Asset Owner for this personal data?

16. Will you need to update our Article 30 record of processing activities?

Yes ☐ No ☐

17. If you are using a data processor have you agreed, or will you be agreeing, a written contract with them?

Yes ☒~~☐~~ No ☐ N/a ☒

Commented [SJ10]: This is applicable and I think you can tick yes – I assume we have a contract with Microsoft!

Individual Rights

Commented [SJ11]: You can't tick no to these!!

18. Is there a means of providing the data subjects with access to the personal data being processed?

Yes ☐ No ☒

19. Can inaccurate or incomplete personal data be updated on receipt of a request from a data subject?

Yes ☐ No ☒

20. Can we restrict our processing of the personal data on receipt of a request from a data subject?

Yes ☐ No ☒

21. Can we stop our processing of the personal data on receipt of a request from a data subject?

Yes ☐ No ☒ N/a ☐

22. Can we extract and transmit the personal data in a structured, commonly used and machine readable format if requested by the data subject?

Yes ☐ No ☒ N/a ☐

23. Can we erase the personal data on receipt of a request from the data subject?

Yes ☒ No ☐

4.0 Risk assessment

Risk Description	Response to Risk	Risk Mitigation	Expected Risk S		
			I	P	Tot
			See Appendix 1 – Assessment Crite		
Personal information is disclosed to unauthorized third-party organization during diagnostic/fault resolution activities.	*Reduce*	*Usage data is only accessible via o365 administrators, it is not shared with 3rd party organisations.* *O365 user feature lockbox is active. Microsoft support engineers requiring access to user data must first submit a lockbox data request. This can only be approved by O365 administrators.*	*2*	*1*	*2- L*
Personal information is disclosed to unauthorized third-party Teams applications.	*Reduce*	Teams apps policy restricts access to only approved Microsoft applications with known functionality. All new apps in Teams will be first assessed before becoming available to ICO staff.	2	1	*2- L*

5.0 Consult the DPO

Guidance: Submit your DPIA for consideration by the DPIA Forum. The process to follow is here.
Any recommendations from the DPOs team will be documented below and your DPIA will be returned to you. You should then record your response to each recommendation.

	Recommendation	**Date and project stage**	**Project Team Response**
1.			
2.			
2.			

6.0 Integrate the outcomes back into your plans

Guidance: Identify who is responsible for integrating the DPIA outcomes. The outcomes include any expected mitigation you need to take as identified in your risk assessment and any further actions resulting from the DPOs recommendations.

Action	**Date for completion**	**Responsibility for Action**	**Completed Date**

7.0 Expected residual risk and sign off

Guidance: Summarise the expected residual risk below. This is any remaining risk *after* you implement all of your mitigation measures and complete all actions. It is never possible to remove all risk so this section shouldn't be omitted or blank. If the expected residual risk remains high (e.g. red on the traffic light scoring in the Appendix) then you will need to consult the ICO as the regulator by following the process used by external organisations.

7.1 IAO sign off

IAO (name and role)	Date	Project Stage

8.0 Change history

Guidance: To be completed by the person responsible for delivering the system, service or process (in a project this will be the project manager).

Version	Date	Author	Change description
V0.1	26.10.2020	R.W	First Draft

Appendix 1: Risk Assessment Criteria

The following criteria are aligned with our corporate risk assessment criteria.

Impact

Impact is the consequence of a risk to the rights and freedoms of individuals being realised. Factors to consider include the financial harm or emotional distress that can be expected to occur.

Impact	Scoring criteria
Very low (1)	No discernible impact on individuals.
Low (2)	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc).
Medium (3)	Individuals may encounter significant inconveniences, which they will overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc)
High (4)	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc).
Very high (5)	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Probability

Probability is the likelihood of a risk to the rights and freedoms of individuals being realised. Factors to consider include the expected frequency of occurrence, and the motivation and capability of threat sources (eg does the threat require insider knowledge and/or significant technical resources to exploit any vulnerability?).

Probability	Scoring criteria
Very low (1)	0-5% - extremely unlikely or improbable For example, the risk has not occurred before or is not expected to occur within the next three years.
Low (2)	6-20% - low but not improbable For example, the risk is expected to occur once a year.
Medium (3)	21-50% - fairly likely to occur

	For example, the risk is expected to occur several times a year.
High (4)	51-80% - more likely to occur than not For example, the risk is expected to occur once a month.
Very high (5)	81-100% - almost certainly will occur For example, the risk is expected to occur once a week.

Risk level
Risk level is a function of impact and probability, and is represented by a RAG rating.

Probability / Impact	Very low (1)	Low (2)	Medium (3)	High (4)	Very high (5)
Very high (5)	Amber (5)	Amber (10)	Red (15)	Red (20)	Red (25)
High (4)	Green (4)	Amber (8)	Amber (12)	Red (16)	Red (20)
Medium (3)	Green (3)	Amber (6)	Amber (9)	Amber (12)	Red (15)
Low (2)	Green (2)	Green (4)	Amber (6)	Amber (8)	Amber (10)
Very low (1)	Green (1)	Green (2)	Green (3)	Green (4)	Amber (5)

Risk acceptance criteria
These criteria are guidelines only, and any risk treatment decisions should be made on a case-by-case basis. For example, it may be prudent to reduce a low risk because of legal and regulatory requirements.

Risk level	Acceptance criteria
Low (Green)	Within this range risks can be routinely accepted.
Medium (Amber)	Within this range risks can occasionally be accepted but shall be kept under regular review.
High (Red)	Within this range risks shall not be accepted and immediate action is required to reduce, avoid or transfer the risk.

Appendix 2: Common risks to data subjects

Guidance: The following are examples of common risks associated with the processing of personal data to assist with your risk assessment. Not all of them will apply to your processing and the list is not exhaustive – you should consider specific risks that are relevant to your plans.

- Data is processed for unspecified / unlawful purposes/ not within expectations of data subjects
- Excessive data is processed
- Data is not kept up to date
- Data is kept for longer than is necessary by us
- Data is kept for longer than is necessary by data processor
- Data processed in contravention of data subject rights
- Data subjects unable to exercise their rights
- Data stolen or modified in transit
- Data stolen or modified at rest in our premises
- Data stolen or modified at rest in data processor premises
- Data transferred overseas to a jurisdiction that does not adequately protect data subject rights
- Re-identification of pseudonymised data by data processor or third party
- Unauthorised destruction or loss of data
- Data processor network / system / online portal not secure
- Data processor fails to process data in accordance with our instructions
- Personal data of children processed without appropriate safeguards / parental authority
- Consent of data subject not freely given (for example employer / employee processing)
- The data subject is particularly vulnerable (elderly or disabled) or is there a potential imbalance of power between the individual and the data controller (employee/employer)
- Source of data poses risks re accuracy (obtained from a unverified or old list)
- Risk to accuracy of data due to matching / combining data from different sources
- Use of new technology, e.g. fingerprinting, face recognition
- Monitoring or recording individuals
- Using profiling according to characteristics or behavior
- Non-compliance with DP principles

9.0 Template Document control

Title	Data Protection Impact Assessment Template
Version	3.0
Status	Final release
Owner	DPSIA Forum
Release date	XX/06/20
Review date	XX/06/21

Case reference

IC-203321-W1K8

Microsoft Managed Desktop – Get Help – DPIA

ico.
Information Commissioner's Office

Data Protection Impact Assessment (DPIA) template

You should complete this template where there is a new (or significant change to an existing) service or process that involves the storage/processing of personal data (whether digital or hardcopy). When dealing with an existing process, service or system **only the change should be impact assessed.**

The DPO's team is available to assist and advise on completing this template.

The template should be submitted to the DPSIA Committee for their recommendations and approval.

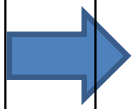
You should start to complete the template as soon as you decide to implement a new system or process. How frequently the DPIA is reviewed and the governance required will vary with the risk of the system or process. At a **minimum**:

Projects: you should produce an initial DPIA prior to finalising your requirements, complete it before finalising your design and review & update the DPIA at least once more prior to go-live. In an Agile project, you should update the DPIA at the start and end of each Epic, or where there is a significant change to the data being processed or the technology or platform. Each update should be submitted to the DPSIA Committee.

Non-projects: you should complete the DPIA prior to designing the service or seeking suppliers and update it whenever there are material changes to the planned system or process.

Screening: Determine what to complete:

1. **GDPR DPIA**: Complete all sections if you meet 2+ questions in section 2.1
2. **Full DPIA**: Complete everything but section 6.2 if you meet 2+ screening questions in any section
3. **Compliance Checklist**: Complete sections 1, 2 and 4, plus signoff, if you don't meet the screening questions



Approval: Consult the DPO's team and select an option for the approvers based on your risk:

1. **DPSIA Committee**: including Senior Information Risk Officer, Head of Cyber Security, DPO
2. **DPSIA Committee**: including DPO and Head of Cyber Security
3. Representatives of DPO and Cyber Security, who will also send it to the DPSIA Committee for their information

Regardless of the option chosen, **the DPIA should be submitted together with your SIA**.

1. Process/system overview

1.1 Summary

Guidance: For projects please provide the following key details. Non-projects should provide a key contact who is responsible for delivering the system or process.

Project ID:	N/A
Project Title:	Microsoft Managed Desktop – Get Help
Project Manager:	Debra Holt

1.2 Synopsis

Guidance: Provide a summary of the process or system including any relevant background information and the key aims/objectives that the system or process must achieve. There is no need for a detailed discussion of data or data flows – these are covered later in the assessment.

The Microsoft Managed Desktop programme where Microsoft takes responsibility for the configuration, imaging, application deployment, software updates, security and end user support of a device. The service is made up of a combination of existing Microsoft services with an additional monitoring, management and support wrapper.

The components can be summarised as follows;

- Microsoft Managed Desktop IT as a Service
    - Microsoft Support ("Get Help")
    - Microsoft Operations & Monitoring
- Microsoft 365 E5
    - Office 365 E5
    - Windows 10 Enterprise E5
    - Enterprise Mobility + Security E5
- A Microsoft Surface Device

DPSIA's have already been completed for the following areas;

- Office 366 365 including Enterprise Mobility + Security

Additional DPSIA's will be completed for;

- Microsoft Cortana Voice Recognition
- MMD Threat Protection
- Windows Hello

Scope of DPSIA

- Microsoft Support Offering ("Get Help")

Microsoft Support

Microsoft Support Services form part of the Microsoft Managed Desktop offering, where Microsoft provide end user support services for the Device, Operating System and Microsoft Office Applications.

This service is operated by Microsoft Professional Services and currently has offices in the United Kingdom, United States and Australia. This allows them to provide 24x7 'follow the sun' support.

This service is accessed through the telephone or through the Microsoft 'Get Help' application which is installed on all Microsoft Managed Desktop Devices and works like an instant messaging application.

Access to this service is user initiated and may result in the Microsoft Support Professional requesting a remote support session to view a user's desktop and MMD status and assist in the resolution of a fault. Again, the remote support session must be initiated and then confirmed by the user and cannot be instigated without the user accepting the remote support session.

ICO Process

As part of the deployment of Microsoft Managed Desktop, ICO users are instructed to contact the ICO support desk, IT Help as the first point of contact, if IT Help cannot resolve the issue, then the IT Help team member will advise the ICO user to contact Microsoft via the Get Help application and will shadow the call to aid the user.
A user may however choose to use MS Get help out of ICO IT help support hours when IT support shadowing will not be available.

1.3 Definition of processing

Guidance: As a data controller we are required to maintain a "record of processing activities" for which we are responsible (Article 30 refers). The following table is designed to help us define the planned processing operation.

Data controller(s)	Microsoft Professional Services & ICO
Data processor(s)	
Purpose of processing	End User Support
Categories of data	Username IP Address Device Name Fault Description Support steps Get Help call transcripts During a remote support session, the Microsoft Support Professional will have the ability to see a duplicate of the ICO user's screen (or screens) for the duration of the session, including any

	documents or emails that are currently visible to the user. However as part of the formal support process, the support engineers tell the user to shut down any documents or screens that could hold sensitive information so this is not expected to be a routine or frequent occurrence.
Categories of subjects	ICO Staff, Microsoft support staff, potentially other data subjects whose personal data is processed by the ICO and visible during screen share.
Categories of recipients	Microsoft acting on behalf of the ICO to support the user's device.
Overseas transfers	Microsoft Professional Services support teams located in the USA, UK and Australia. Microsoft has a current certification to Privacy Shield.

1.4 Purpose for processing

Guidance: State the legitimate interest being pursued in the processing, including the purposes, aims and the intended benefits for you, data subjects, society or others.

User and device data is processed in order to provide effective end user support.

1.5 Lawful basis

Guidance: State the basis on which the processing is lawful under GDPR Article 6 (consent, performance of contractual obligations to a data subject, compliance with legal obligations, public interest, exercise of official authority, or protecting the vital interests of a natural person).

If you are processing data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, data concerning a person's sex life or sexual orientation or data relating to criminal convictions or offences, you will also need to state a further basis for that processing – you can find a list of these in GDPR Article 9 and 10.

Processing of this data is required to allow Microsoft to perform their contractual obligations regarding security monitoring and end user support of Microsoft Managed Desktop Devices.

The lawful basis for processing is Article 6(1)(e) – public task.

1.6 Mandatory requirements

Guidance: Add the following requirements to your project backlog unless they do not apply (e.g. data need not be kept up to date in a system for storing old records). Section 4 can be used to check that these have been completed, particularly if delivery is not being managed as a project.

Data Accuracy

a) Data must be kept up to date
b) There must be means to validate the accuracy of any personal data collected
c) Inaccurate or incomplete personal data must be updated on receipt of a lawful request from the data subject

<u>Retention & Deletion</u>
d) All data collected will have a retention period
e) Data must be deleted at the end of its retention period
f) Personal data must be erased upon receipt of a lawful request from the data subject

<u>Information & Transparency</u>
g) The data subjects shall be provided with:
(i) The identity and contact details of the data controller;
(ii) The purposes of the processing, including the legal basis and legitimate interests pursued
(iii) Details of the categories of personal data collected
(iv) Details of the recipients of personal data

<u>Objection & Restriction</u>
h) There must be means to restrict the processing of data on receipt of a lawful request from the data subject
i) There must be means to stop the processing of data on receipt of a lawful request from the data subject

<u>Security</u>
j) Appropriate training and instructions will be put in place to enable staff to operate the new system / process securely
k) Identify an Information Asset Owner
l) Update the Information Asset Register

<u>Is the data being transferred outside the UK and EEA? If so:</u>
m) The data subjects must be provided with information on where to obtain details of any safeguards over data transferred to non-GDPR compliant countries
n) Consult the DPO for additional requirements to ensure the processing is GDPR compliant.

<u>Is the data being transferred to or through another organisation? If so:</u>
o) There must be controls to ensure or monitor compliance by external organisations.

<u>Is consent or pursuit of a contract the lawful basis for an automated processing operation? If so:</u>
p) There must be a means to extract and transmit the data in a structured, commonly used and machine-readable format on receipt of a lawful request from the data subject
q) The consent must be recorded in some manner to serve as evidence

<u>Does our Privacy Notice need to be updated? If so:</u>
r) *Update the Privacy Notice*

2. Data protection assessment screening

Guidance: The purpose of the screening questions is to determine if a DPIA is required. As a data controller we are required to perform DPIAs where the processing is likely to result in a high risk to the rights and freedoms of individuals (Article 35 refers).

2.1 Screening questions

ID	Criteria	Y/N
1	Will the processing involve evaluation or scoring, including profiling or predicting, especially in relation to an individual's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements?	N
2	Will the processing involve automated decision making that will have a legal or similar detrimental effect on individuals? For example, decisions that lead to exclusion or discrimination.	N
3	Will the processing involve the systematic monitoring of individuals in a publicly accessible area? For example, surveillance cameras in a shopping centre or train station.	N
4	Will the processing involve sensitive personal data or data of a highly personal nature? For example, special categories of data (Article 9 refers), personal data relating to criminal convictions or offences (Article 10 refers), and personal data linked to household and private activities.	Y
5	Does the processing involve large scale processing of data at a regional, national or supranational level, and which could affect a large number of data subjects?	N
6	Does the processing involve matching and combining two or more datasets that have been collected for different purposes and/or by different data controllers?	N
7	Does the processing concern vulnerable individuals who may be unable to easily give consent or object to the processing? For example, children, employees, and others who require special protection (mentally ill persons, asylum seekers, patients, the elderly).	N
8	Does the processing involve the innovative use or application of new technological or organisational solutions? For example, "Internet of Things" applications can have significant impacts on subjects' daily lives and privacy.	N

9	Does the processing prevent individuals from exercising a rights or using a service or contract? For example, where a bank screens its customers again credit reference database in order to decide whether to offer them a loan.	N

Guidance: If you answer "Yes" to one or more questions you should complete a DPIA. If you answer "No" to all questions please proceed to section 6.

2.2 DPIA approach and consultation

Guidance: Record which parts of the DPIA you will be completing and your rationale (especially if your choices differ from the guidance above).

Explain what practical steps you will take to ensure that you identify and address the data protection risks. Include details of:

- *Who should be consulted, internally and externally? This must include the DPO's team and Cyber Security. You should also consult data subjects or their representatives unless this is not possible or appropriate – e.g. it would be disproportionate, impractical, undermine security or compromise commercial confidentiality.*
- *If data subjects (or their representatives) will not be consulted you must document the reasons for this.*
- *How you will carry out the consultation. You should link this to the relevant stages of your project management process or delivery plan.*

Work has been carried out with Microsoft to understand the quality standards for Microsoft Professional Services and the Get Help Application. These are detailed in the - Microsoft professional services white paper in Appendix A

3. Data inventory

3.1 Information flows

Guidance: Provide a systematic description of the processing, including:

- *Whether data collected is personal data*
- *The source of the data (including whether the data subjects are vulnerable, the relationship with the data subjects, the manner of collection and the level of control the data subjects have over the data once collected)*
- *The nature and context of the processing (including whether there are new technological developments or any relevant current issues of public concern)*
- *The scope of the processing (including the nature and volume of data, frequency and duration of processing, sensitivity of the data and the extent of the processing)*
- *The storage and transfer of the data (including details of hardware, software, networks, key people and details of any paper records or transmission channels)*
- *Responsibilities for the data (including the information asset owners, how responsibilities for information change through the data flow and the boundaries of responsibilities in any handover)*

You may find it useful to refer to a flow diagram or other way of explaining information flows. You should also say how many individuals are likely to be affected by the processing of personal data.

IP Address, Device Name and User Name are made available to Microsoft when the device user is enrolled within the Microsoft Managed Desktop programme.

Support call data is recorded when a user contacts a Microsoft Support Professional via the telephone or through the Get Help Application.

A Microsoft Support Professional will be able to see a user's screen if a remote support session is initiated the ICO staff member accepts and approves the session by clicking 'allow'.

Username, IP Address and Device name is visible to Microsoft Professional Services for either the duration that the employee / device forms part of the ICO (plus 90 days) or for the life of the Microsoft Managed Desktop Contract, depending on which is shorter.

We have received assurance from Microsoft that no data is stored following a get help session.

3.2 Data inventory

Guidance: Identify the personal data to be held, the recipients (those with access to the data), the retention period and the necessity of the data collection, processing and retention.

Data Type	Recipients	Retention Period	Necessity
User name	Microsoft Professional Services	For the duration of the user's employ within the ICO plus 90 days.	Required to identify a user as an ICO employee and manage a support call.
IP Address	Microsoft Professional Services	For the duration of the IP lease to an ICO Device.	Required to identify a device within the ICO and manage a support call.
Device Name	Microsoft Professional Services	For the time that a device is assigned to a user and is not rebuilt	Required to identify a device within the ICO and manage a support call.
User Desktop	Microsoft Professional Services	User desktops (a view of the ICO user's screen or screens) is visible to the Microsoft Support Professional during a remote control session.	Required to provide remote support to an ICO user.

4. Compliance measures

Guidance: Use this section to record your compliance with the requirements in section 1.5. Fill in the details of how the requirements have been met or list the requirement as N/A. The requirement source is a reference to GDPR unless otherwise stated.

Requirement	Implementation Details
Data Accuracy	
a) Data must be kept up to date	Data is updated as part of ICO driven Joiner, Mover Leaver processes. For leaver users data is synchronised from Active Directory to directory to ensure that the data is deleted from after 90 days. We can override certain accounts with a legal hold by requesting this via the Microsoft compliance portal. Legal holds will be revoked by us when there is no longer a need to retain the data.
b) There must be means to validate the accuracy of any personal data collected	Personal data is driven from ICO Active Directory which is kept updated in line with ICO JML processes. We upload data to Microsoft multiple times per day.
c) Inaccurate or incomplete personal data must be updated on receipt of a lawful request from the data subject	This process is handled through the ICO JML process & the Active Directory can be updated in the event of a lawful request being received.
Retention & Deletion	
d) All data collected will have a retention period	Provided above
e) Data must be deleted at the end of its retention period	Automatically processed by Microsoft as detailed in service contract. Anything retained for longer due to a legal hold will be deleted by Microsoft upon instruction.
f) Personal data must be erased upon receipt of a lawful request from the data subject	Processed by Microsoft through the compliance portal. Microsoft to act on our instructions to erase data if a lawful request is received by us. The screen share is not recorded during the 'get help' event.
Information & Transparency	
g) The data subjects shall be provided with: ● the identity and contact details of the data controller; ● the contact details of the Data Protection Officer; ● the purposes of the processing, including the legal	ICO will issue statement to users about Microsoft Managed Desktop service data processing as part of the end user training.

basis and legitimate interests pursued • details of the categories of personal data collected • details of the recipients of personal data	
Objection & Restriction	
h) There must be means to restrict the processing of data on receipt of a lawful request from the data subject	Users have the option of not using the 'Get Help' application to obtain support and can submit a ticket to the ICO / Littlefish operating 'IT Help' team. Microsoft will remove stored information from the 'Get Help' system upon lawful request.
i) There must be means to stop the processing of data on receipt of a lawful request from the data subject	Users have the option of not using the 'Get Help' application to obtain support and can submit a ticket to the ICO / Littlefish operating 'IT Help' team. Microsoft will remove stored information from the 'Get Help' system upon lawful request.
Security	
j) Appropriate training and instructions will be put in place to enable staff to operate the new system / process securely	Full training is provided on the use of the Microsoft Managed Desktop Solution MMD onboarding sessions instruct users on appropriate use. IT help have a process for supporting MMD users. MS get help support have a process for engaging with a ICO user including minimising personal data shared via screen share.
k) Identify an Information Asset Owner	The Information Asset Owner is Mike Fitzgerald as Director of Digital, IT & Customer Contact.
l) Update the Information Asset Register	The Information Asset Register will be updated to reflect this.
Conditional Requirements	
m) The data subjects must be provided with information on where to obtain details of any safeguards over data transferred to non-GDPR compliant countries	N/A – overseas transfer covered by privacy shield framework so a finding of adequacy applies. In other countries (Australia) Microsoft has contractual clauses to assure the privacy of the data.
n) Consult the DPO for additional requirements to ensure the processing is GDPR compliant.	Added to project backlog
o) There must be controls to ensure or monitor compliance by external organisations.	This forms part of the signed agreements with Microsoft.

p) There must be a means to extract and transmit the data in a structured, commonly used and machine-readable format on receipt of a lawful request from the data subject	N/A
q) The consent must be recorded in some manner to serve as evidence	N/A
r) Update the Privacy Notice	

5. Data protection risk assessment

Guidance: Identify and assess the risks to subjects' rights, the actions you could take to reduce the risks and any future steps that will be necessary (eg the production of new guidance or security testing for new systems). Some example risk sources have been listed to aid you. This list is not comprehensive and will not necessarily apply to your system or process. See Appendix for guidance on assessing impact and probability.

Risks should be considered from the data subject's perspective not the ICO's (eg a reputational risk to the ICO should not be recorded here). Some example threats to consider include:

- *Discrimination*
- *Identity theft and fraud*
- *Financial loss*
- *Damage to data subjects' reputation*
- *Loss of confidentiality of professional secrets*
- *Unauthorised reversal of pseudonymisation*
- *Social or economic disadvantage*
- *Deprivation of legal rights or freedoms*
- *Data subjects losing control over their data*
- *Loss of privacy or intrusion into private life*
- *Prevention from accessing services*

Risk Details	**Impact**	**Probability**	**Response**
[Guidance: Describe risks to data subjects]	*[Guidance: Describe consequences to data subjects if risk realised]*	*[Guidance: Describe likelihood that risk will be realised]*	*[Guidance: Describe risk treatment (eg reduce, avoid, accept or transfer)]*
Risk of Microsoft Support Professional accessing ICO information inappropriately	Medium –	Very Low	Microsoft vetting process provides assurances on staff. Residual risk low and accepted
Risk of Microsoft Support Professional viewing 'private' information on a user's desktop during a remote support session.	Medium	Low	IT Help advise users to close 'private' documents when initiating a remote support call. We have received assurance from Microsoft that their support staff

			will also advise users to close documents prior to engaging in screen share support. Microsoft Support Professionals are covered under our Microsoft agreement and are covered under mutual privacy agreements. Residual risk medium and accepted.
Risk of end user accessing MS help without IT help shadowing.	Medium	Low	This removes the safeguard of our IT Help staff checking that no sensitive data is shared via screen share however we have received assurance from Microsoft that their support staff will also advise users to close documents prior to engaging in screen share support. Residual risk medium and accepted.

6. Residual risk and sign off

6.1 Residual risk

Guidance: Record details of the remaining risk. It is never possible to remove all risk so this section should not be omitted or blank. If the residual risk remains high (e.g. red on the traffic light scoring in the Appendix) then you will need to consult the ICO by following the process used by external organisations.

All residual risk is considered to be low and can be accepted.

6.2 Necessity and proportionality

Guidance: If you answered "Yes" to one or more of the screening questions in Section 2.1 you should discuss the necessity and proportionality of the collection, processing and retention of this data here, weighing the impact on data subjects rights and freedoms against the benefits of the processing activity. You should also consider whether there are other reasonable ways to achieve the same result with less impact on data subjects. If you have not answered "Yes" to any of the screening questions in Section 2.1 you can leave this section blank.

6.3 DPO recommendations

Guidance: Record any recommendations from the DPO or their delegates and responses here. This serves as useful tool when reconsidering a rejected DPIA or in recording the justification if the organisation rejects the DPO's advice.

No	Recommendation	Project Team Response
1	[Record any changes recommended by the DPO here]	[Record the actions taken as a result of the recommendation]

6.4 Sign Off

Guidance: Send this to the DPSIA Committee to approve the privacy and security risks involved in the project, the solutions to be implemented and the residual risk.

Considered by	Date	Project Stage
DPIA Forum	20/02/2020	

7. Integrate the outcomes back into the plan

Guidance: Who is responsible for integrating the DPIA outcomes back into any project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any data protection concerns which may arise in the future?

Action to be taken	Date for completion	Responsibility for Action	Completed Date

Contact point(s) for future data protection concerns	

8. Change history

Guidance: To be completed by the person responsible for delivering the system, service or process (in a project this will be the project manager).

Version	Date	Author	Change description
v.0.1	07.02.2020	Neil Smithies	First Draft

9. Template Document control

Title	Data Protection Impact Assessment Template
Version	1.0
Status	Final release
Owner	DPSIA Committee
Release date	10/12/18
Review date	10/12/20

Appendix: Risk Assessment Criteria
The following criteria are aligned with our corporate risk assessment criteria.

Impact
Impact is the consequence of a risk to the rights and freedoms of individuals being realised. Factors to consider include the financial harm or emotional distress that can be expected to occur.

Impact	Scoring criteria
Very low (1)	No discernible impact on individuals.
Low (2)	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc).
Medium (3)	Individuals may encounter significant inconveniences, which they will overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc)
High (4)	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc).
Very high (5)	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Probability
Probability is the likelihood of a risk to the rights and freedoms of individuals being realised. Factors to consider include the expected frequency of occurrence, and the motivation and capability of threat sources (eg does the threat require insider knowledge and/or significant technical resources to exploit any vulnerability?).

Probability	Scoring criteria
Very low (1)	0-5% - extremely unlikely or improbable For example, the risk has not occurred before or is not expected to occur within the next three years.
Low (2)	6-20% - low but not improbable For example, the risk is expected to occur once a year.
Medium (3)	21-50% - fairly likely to occur For example, the risk is expected to occur several times a year.

High (4)	51-80% - more likely to occur than not For example, the risk is expected to occur once a month.
Very high (5)	81-100% - almost certainly will occur For example, the risk is expected to occur once a week.

Risk level

Risk level is a function of impact and probability, and is represented by a RAG rating.

Probability / Impact	Very low (1)	Low (2)	Medium (3)	High (4)	Very high (5)
Very high (5)	Amber (5)	Amber (10)	Red (15)	Red (20)	Red (25)
High (4)	Green (4)	Amber (8)	Amber (12)	Red (16)	Red (20)
Medium (3)	Green (3)	Amber (6)	Amber (9)	Amber (12)	Red (15)
Low (2)	Green (2)	Green (4)	Amber (6)	Amber (8)	Amber (10)
Very low (1)	Green (1)	Green (2)	Green (3)	Green (4)	Amber (5)

Risk acceptance criteria

These criteria are guidelines only, and any risk treatment decisions should be made on a case-by-case basis. For example, it may be prudent to reduce a low risk because of legal and regulatory requirements.

Risk level	Acceptance criteria
Low (Green)	Within this range risks can be routinely accepted.
Medium (Amber)	Within this range risks can occasionally be accepted but shall be kept under regular review.
High (Red)	Within this range risks shall not be accepted and immediate action is required to reduce, avoid or transfer the risk.

Appendix A: Microsoft Professional Services White Paper

Microsoft
Professional Services

Case reference

IC-203321-W1K8

MMD Storage and Data Retention - DPIA

ico.
Information Commissioner's Office

Data Protection Impact Assessment – MMD Storage and date retention

Document Name	Data Protection Impact Assessment – MMD Storage and data retention
Author/Owner (name and job title)	Graham Rumens Project Manager
Department/Team	PMO – on behalf of Digital and IT
Document Status (draft, published or superseded)	Published
Version Number	v2.1
Release Date	13/09/22
Approver (if applicable)	Mike Fitzgerald
Review Date	12/09/23
Distribution (internal or external)	Internal

Privacy by design at the ICO

Welcome to our privacy by design process. You should use this every time you want to implement or change a product or process at the ICO. It is essential to managing your own project risks but also to managing the corporate risks of the ICO.

Responsibilities

It is your responsibility to ensure that data protection impact is taken into account during the design and build of your product or service. To do this successfully, you will need to be able to explain what your proposal is, and map out how data is used. This includes, amongst other things, where data might sit at any time geographically, but also the purpose of its use at different points in time.

Remember the basics. Key to a good assessment is knowing at all points in the process: what data you are collecting and why, where it will be stored, for how long will you keep it, who will access it and for what purpose, how it will be kept secure and whether it's being transferred to any other country.

Your Information Asset Owner (your Director) is ultimately responsible for managing any residual risk once you have completed any mitigations to the risks you identify.

The Information Management Service, working on behalf of our DPO, can help complete the paperwork, provide compliance advice and spot risks. It is not the Service's responsibility to own, manage or mitigate the risks identified during the process.

Getting advice

You might also need advice from subject matter experts in other teams to make sure that you understand how something works or risks resulting from what you're proposing to do. This is particularly likely if it involves new, or changing, technologies. Getting this advice will help to provide your IAO with assurance that you have understood and identified the risks.

You might well be working on a contract or agreement and a Security Opinion Report at the same time – these are also ways that you can mitigate risks and should be viewed as part of the overall assessment process.

The paperwork

You should think of this as a live document. You might change your plans or new information might come to light that changes the risk profile of your proposal. If that's the case, you should revisit the paperwork and update it to reflect any changes. You might also need to inform your IAO of new or changed risks.

The DPIA process

You should review our internal DPIA Process and allow time for this process in your project plans. Start early! How long it takes will depend on what you're proposing, and how well you can explain it and identify risks. It can take several weeks to get the right advice and risk assessment in place.

Guidance for completing this template – please read.

You only need to complete this Data Protection Impact Assessment (DPIA) template if you have completed a Screening assessment - do I need to do a DPIA? and this indicates a high risk to data subjects. If you are unsure whether you need to complete a DPIA use the screening assessment first to help you decide.

Aim to complete your DPIA as early as possible as the outcome of the assessment could affect the viability of your plans. In extreme cases, you won't be able to continue with your plans without changing them, or at all.

Guidance notes are included within this template to help you - just **hover your mouse over any blue text** for further information.

The Information Management Service is also available for further advice and support. Please keep in mind our service standards if you require advice.

1. Process/system overview

1.1 Ownership

Project Title:	MMD Storage and data retention
Project Manager:	Graham Rumens
Information Asset Owner:	Director of Digital and IT
Controller(s)	ICO
Data processor(s)	N/A

1.2 Describe your new service or process

It has been realised that we have a gap in DPIA coverage for the MMD devices currently in use across the ICO. Where DPIAs have been produced for the applications used on the devices (Windows Hello, OneDrive etc.), we now recognise that an assessment is required to consider the storage of data 'locally' on a staff members MMD device i.e. C Drive and Recycle bin.

There are two main storage areas on the MMDs:

- C Drive (local storage, downloads and profile storage)
- Recycle Bin. Any time a document from the above locations is deleted it will go to the Recycle Bin, where it will sit permanently until it is manually deleted.

We have consulted with Microsoft who have advised the following:

Block access to C drive:

In one of the previous such request, MMD recommendation was not to block C drive access.

Below are some implications of blocking C drive access but not limited to the list:

• Users will not be able to access the profile folders (documents, downloads, pictures etc.)
• Installation and upgrades for the software and applications that uses C drive to store files will get affected
• Scripts and Apps that are being deployed through Intune by user accounts will get affected
• Intune uses C drive to store the logs will get affected

Add downloads folder to OneDrive:

Yes, this will be an exception. We have implemented this previously to few customers so this can be done. However, the downloads will still be in local storage but be synced into OneDrive so this won't resolve the issue.

As it is not possible to employ organisational controls (i.e. automated deletion) in these locations, therefore documents stored there will be retained indefinitely until they deleted by the users. This has been identified as a potential risk to the data subject as Article 5(1)(e) of the UK GDPR states that personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. There is therefore a risk that personal data may end up being unintentionally retained for longer than it is required.

The intention behind this DPIA is to address and mitigate this risk for the new MMDs, which are being rollout out from September 2022.

Information stored in ICO systems such as EDRM and ICE, or M365 applications such as OneDrive and Teams, is out of scope for this DPIA. It is worth noting that OneDrive storage and local MMD storage are two separate locations.

1.3 Personal data inventory - explain what personal data is involved

Category of data	Data subjects	Recipients	Overseas transfers	Retention period
For the purposes of the DPIA we should assume that all categories of data are covered. In the pursuit of ICO activities staff may encounter and use all categories of personal data.	ICO Staff, Public,	ICO staff	N/A	Different classifications of data are subject to business policy retention periods, enforced elsewhere. Where data is stored locally on an MMD device, the same conventions apply.

1.4 Identify a lawful basis for your processing

The personal data on individual MMD devices can be processed under a variety of lawful bases. Any personal data downloaded to a user's MMD device is being processed under the same lawful basis as originally identified.

1.5 Explain why it is both necessary and proportionate to process the personal data you've listed in your data inventory

In the course of day to day ICO activities, staff members may see fit to access data and files which are then stored locally on their MMD device, as opposed to centrally in ICO systems and applications where it can be monitored, and the retention period applied automatically. Team members have advice on data storage but may still chose to store files (downloads etc.) on the C Drive during the course of their work. Even once these files have been moved locally to the Recycle Bin they may still be retrievable if this file is not emptied regularly. This local storage cannot be monitored centrally. There is therefore a risk that information that appears to have been deleted may actually be recoverable. There is no express business need for this practise of storage however, it is a feature/limitation of the Microsoft design and we are therefore recognising it as a possibility.

1.6 Outline your approach to completing this DPIA

This DPIA has been produced along with advice and input from Information management, PMO and Digital & IT. We have considered the current data retention policies that apply centrally and can be monitored (Application storage) and recognised the limitations of controls over individuals storing data locally. In this DPIA we plan to cover these potential risks and apply the necessary steps to mitigate them. Advice was obtained from the Knowledge Services team on this – details here. Relevant extracts from the advice are below:

'The upshot is that information sitting in recycle bins is unlikely to be considered as deleted, and we'd still expect organisations to – for example – keep this information secure in line with UK GDPR requirements. Failure to delete from recycle bins and put the data properly beyond use is also likely to mean a failure to comply with the storage limitation principle.'

'In terms of SAR responses, we might be able to argue for a pragmatic approach similar to our one under FOIA when handling UKGDPR information rights requests – that it's reasonable for us to interpret most requests as being about information contained in our 'live records' or those we hold in archives (so not really applicable to those items colleagues have intentionally sent to recycle bins – with that information therefore presumed to be outside the request's scope). This would be the case unless it's clear from the context that the information sitting in recycle bins falls within the request's scope (eg if someone specifically mentions an old or previous version of a document that could be sitting in a recycle bin or otherwise makes it clear that they expect us to provide any relevant information contained in recycle bins, in which case we'd need to appropriately consider that information too when handling their request).'

This advice has been used to inform the risks in the risk assessment of this DPIA.

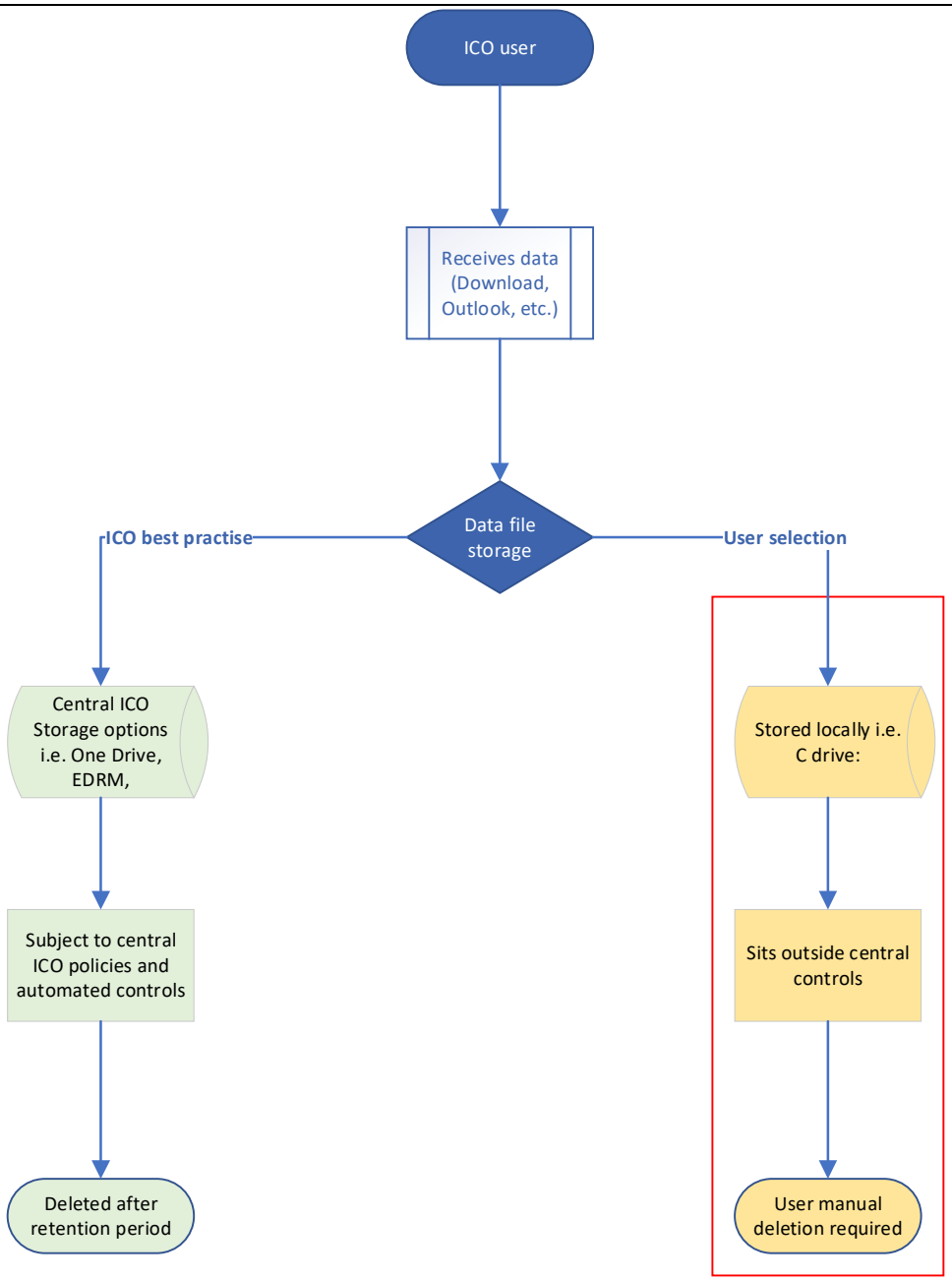
2.0 Personal Data Lifecycle

Guidance: You must provide a systematic description of your processing from the point that personal data is first collected through to its disposal.

You should explain the source of the data, how it is obtained, what technology is used to process it, who has access to it, where it is stored and how and when it is disposed of.

If your plans involve the use of any new technology you should explain how this technology works and outline any 'privacy friendly' features that are available.

You can use the headings provided below to help you construct your lifecycle. Also include a flow diagram if it helps your explanation.



Data source and collection:

External and internal file receipt and generation. Documents can be created on the MMD device, downloaded from an online system or application, or sent as an attachment via email.

Technology used for the processing:

Locally on MMD devices

Identified Storage locations:
Downloads Folder
MMD Recycle Bin
User Profile

Access controls and data sharing:
User only – the C drive can only be accessed by the user

Disposal:
It is not possible to set up organisational controls on the user's local MMD storage, therefore these will need to be deleted manually by the users. Once the documents are deleted they will be stored in the MMD Recycle Bin, where they will also be kept permanently.

The proposed method for addressing this risk from the rollout of the new devices is to send out regular reminders for users to delete files they no longer need, and to empty their Recycle Bins.

3.0 Key principles and requirements

Purpose & Transparency

1. Will you need to update our privacy notices?

Yes ☐ No ☒

2. If you are not updating our privacy notices how do you intend to communicate information about your processing to the data subjects?

3. If consent is your lawful basis for processing personal data are you maintaining appropriate records of the data subjects consent?

Yes ☐ No ☐ N/a ☒

4. If legitimate interests is your lawful basis for processing have you completed a legitimate interest assessment?

Yes ☐ No ☐ N/a ☒

If applicable please provide a link to your completed assessment.

Accuracy

5. Are you satisfied the personal data you are processing is accurate?

Yes ☒ No ☐

6. How will you ensure the personal data remains accurate for the duration of your processing?

Data stored on the C drive can be amended if required. Data stored in the Recycle Bin and downloads folder can be deleted when no longer required.

7. If the personal data isn't being obtained directly from the data subject what steps will you take to verify accuracy?

Minimisation, Retention & Deletion

8. Have you done everything you can to minimise the personal data you are processing?

Yes ☒ No ☐

9. How will you ensure the personal data are deleted at the end of the retention period?

Comms will be sent out twice a year to remind users to manually delete documents from their C drive, downloads folder and Recycle Bin.

10. Will you need to update the retention and disposal schedule?

Yes ☐ No ☒

Integrity and confidentiality

11. Where will the personal data be stored?

ICO systems: Local storage MMD devices.

12. Are there appropriate access controls to keep the personal data secure?

Yes ☒ No ☐

13. Have you contacted the cyber security team for a security assessment of your plans?

Yes ☐ No ☐ N/a ☒

14. Please explain the policies, training or other instructions you intend to put in place to enable staff to operate the new system or process securely.

Instructions on local device storage will be formally covered as part of the new staff on-boarding process by the IT Team, and information management will instigate regular comms to all team members to remind them of this obligation.

Accountability

15. Who will be the Information Asset Owner for this personal data?

Director of Digital and IT

16. Will you need to update our Article 30 record of processing activities?

Yes ☐ No ☒

17. If you are using a data processor have you agreed, or will you be agreeing, a written contract with them?

Yes ☐ No ☐ N/a ☒

Individual Rights

Guidance: UK GDPR provides a number of rights to data subjects where their personal data is being processed. As some rights are not absolute and only apply in limited circumstances we may have grounds to refuse a specific

request from an individual data subject. However you need to be sure your new service or process can facilitate the exercise of these rights by the data subject i.e. it should be technically feasible for us to action a request if required.

18. Is there a means of providing the data subjects with access to the personal data being processed?

Yes ☒ No ☐

19. Can inaccurate or incomplete personal data be updated on receipt of a request from a data subject?

Yes ☒ No ☐

20. Can we restrict our processing of the personal data on receipt of a request from a data subject?

Yes ☒ No ☐

21. Can we stop our processing of the personal data on receipt of a request from a data subject?

Yes ☒ No ☐ N/a ☐

22. Can we extract and transmit the personal data in a structured, commonly used and machine readable format if requested by the data subject?

Yes ☒ No ☐ N/a ☐

23. Can we erase the personal data on receipt of a request from the data subject?

Yes ☒ No ☐

Risk Description		Response to Risk	Risk Mitigation	Expected Risk Score		
				I	P	Total
				See Appendix 1 – Risk Assessment Criteria		
Example: *Access controls are not implemented correctly and personal data is accessible to an unauthorised third party.*		*Reduce*	*Existing mitigation: We have checked that the system we intend to procure allows us to set access permissions for different users.* *Expected mitigation: We will appoint and train a system administrator who will be responsible for implementing access controls and monitoring access. The system administrator will also audit the system periodically to review access permissions.*	*3*	*1*	*3 - low*
1.	Personal data being kept for longer than intended	Reduce	Expected mitigation: Communications sent out to all staff twice a year reminding them to delete files they don't need any more stored locally, and to empty their Recycle Bins.	2	3	6 - medium
2.	Information being stored outside of corporate systems and therefore overlooked in the event of an information request. Potential for non-compliance with data subject rights.	Reduce	Expected mitigation: Information Management policies and training advising staff to store information in corporate systems Expected mitigation: Communications sent out to all staff twice a year reminding them to delete files they don't need any	4	2	8 - medium

			more stored locally, and to empty their Recycle Bins.			
3.	Attachments and downloads will automatically store locally in the users profile. Sometimes these documents can remain in the profile but it is not possible for users or IT to manage the storage in these locations.	Accept	This is beyond our control and will need to be accepted as a low exposure to risk. Microsoft have recommended that we do not block access to C: for users. Cyber security and Applications have undertaken to investigate the possibility of scanning devices, centrally, as a future policing measure. This potential solution would enable remote observation of all devices and provide the IT team with an actionable list of devices which are using local storage.	4	3	12 - Medium

4.0 Risk assessment

5.0 Consult the DPO

Guidance: Once you have completed all of the sections above you should submit your DPIA for consideration by the DPIA Forum who will provide recommendations on behalf of our DPO. The process to follow is here.

Any recommendations from the DPOs team will be documented below and your DPIA will then be returned to you. You must then record your response to each recommendation and proceed with the rest of the template.

	Recommendation	Date and project stage	Project Team Response
1.	**Section 1.3. – data subjects needs clarifying, does staff refer to ICO staff? Organisations isn't a data subject so needs to be clearer – is this supposed to cover staff at stakeholder organisations that engage with us?**	18/10/22 Complete	Section 1.3 has been clarified to reflect ICO Staff
2.	**Section 1.5. – There isn't really any explanation of necessity here. Please could you add a brief paragraph about why ICO staff need to work in a way which sees them download files to C-drive – so typically when working on a draft or incomplete piece of work before a final version is placed into a central location. Something general about how this is essential for day to day operations would just help tick the necessity box.**	18/10/22 complete	Section 1.5 has been amended to reflect that there is no express business need but that the possibility remains that staff may still store locally if they see fit. After checking: Acceptable use policy, Mobile Device guidance, Retention & Disposal policy, and reviewing the new starter process, we cannot evidence that we provide "guidance" only "advice" therefore section has been updated this.

	This section mentions that team members have guidance. What guidance is this and what team? Can it be more specific or linked to? At the minute it's unclear what this is referring to. Are you talking generally here about IM policies and procedures?		
3.	**Section 3.9. – who will be responsible for sending out comms? This needs to be made clearer.**	18/10/22 Complete	Information management have accepted that they can this communication to remind people to empty recycle bins and review local C: storage.
4.	**Section 3.14. – What is the expected outcome? Question is what do you intend to put in place so you need to explain here what is happening. E.g. a twice yearly communication to staff etc.**	18/10/22 Complete	Communication to staff (see above) but there currently does not appear to be policy coverage. Information management could consider adding local storage to the appropriate policy and/or the Information Governance course which is required by all staff each year. As a minimum all c: storage is purged when MMD devices are replaced (currently every 3 years).
5.	**Risk 2 – The impact should be higher as anything that might deny data subjects fundamental rights is not a low impact.**	1/11/22 Complete	Impact increased to 4
6.	**Risk 3 – More explanation is needed about this risk. Response to risk is 'reduce' yet mitigation states risk is being accepted. Risk scoring should probably be higher if we're saying personal data is held in a space where we have no organisational control whatsoever**	1/11/22 Complete	The Risk has been adjusted to impact 4 and the response changed to accept. Added a paragraph to explain that there is an undertaking to investigate possible solutions to scan devices centrally in order to monitor c: storage.

	and even the end user can't manage the data. **Why isn't it possible to manage information in the user's profile? The issues and risks need to be mitigated if possible or the fact it can't be mitigated needs to be acknowledged in the risk score which should be scored highly in terms of probability.**		
7.	**There's a few references in this DPIA indicating data stored centrally in ICO systems can be monitored and retention period applied automatically (1.2 – not possible to automate retention, 1.5, 2.0 "subject to central ICO policies and automated controls").** **Not completely accurate to say all data stored in central systems allows for automated retention. Perhaps better adjusting to describe data held centrally as being subject to more technical and organisational controls like automated deletion whereas C-drive storage is not subject to any.**	18/10/22	Wording has been amended to reflect this.

6.0 Integrate the DPIA outcomes back into your plans

Guidance: Completing sections 1 to 5 of your DPIA should have helped you identify a number of key actions you now need to take to meet UK GDPR requirements and minimise risks to your data subjects. For example, you may now need to draft a suitable privacy notice for your data subjects; or you could have risk mitigations that you need to go and implement. You should also consider whether any additional actions are required as a result of any recommendations from the DPO.

Use the table below to list the actions you now need to take and to track your progress with implementation. Most actions will typically need to be completed *before* you can start your processing.

Action	**Date for completion**	**Responsibility for Action**	**Completed Date**
Roll out of communications plan to remind staff of the guidance to empty recycling bins and observe correct retention of C: storage	End Nov	Information management	
Formally introduce instruction on local storage and downloads as part of the IT help on-boarding process for new starters and when devices are exchanged at end of life	End Nov	IT Help aligned with IM comms	
Investigate central device scanning and	End Nov	Cyber security and Applications	

policing local storage and downloads in c: This will establish if remote monitoring can produce reliable reports of devices which have local storage not in line with he directives.			

7.0 Expected residual risk and sign off by IAO

Guidance: Summarise the expected residual risk below for the benefit of your IAO. This is any remaining risk ***after*** you implement all of your mitigation measures and complete all actions. It is never possible to remove all risk so this section shouldn't be omitted or blank.

Note: If the expected residual risk remains high (i.e. red on the traffic light scoring in the Appendix) then you will need to consult the ICO as the regulator by following the process used by external organisations.

The mitigations to risk in this document rely on the good conduct and 'housekeeping' of individual team members. Amending policies, sending communications and training may not, in entirety, lead to 100% compliance across the business.

The exception to this is with the remote centrally scanning of devices which could police local storage more effectively however, this is yet to be investigated and assessed.

7.1 IAO sign off

Guidance: Your IAO owns the risks associated with your processing and they have final sign off on your plans. You **must** get your IAO to review the expected residual risk and confirm their acceptance of this risk before you proceed.

IAO (name and role)	Date of sign off	Project Stage
Mike Fitzgerald Director of Digital & IT and Business services	2/11/22	N/A

8.0 DPIA Change history

Guidance: To be completed by the person responsible for completing the DPIA and delivering the system, service or process.

Version	Date	Author	Change description
V0.1	13/09/2022	Graham Rumens	First Draft
V0.2	03/10/2022	Ben Cudbertson	Recommendations added following DPIA Forum
V0.3	18/10/22	Graham Rumens	Further updates from forum feedback and review meeting. Added follow up actions.
V0.4	1/11/22	Graham Rumens	Final revision based on feedback from Ben C

Appendix 1: Risk Assessment Criteria

The following criteria are aligned with our corporate risk assessment criteria.

Impact

Impact is the consequence of a risk to the rights and freedoms of individuals being realised. Factors to consider include the financial harm or emotional distress that can be expected to occur.

Impact	Scoring criteria
Very low (1)	No discernible impact on individuals.
Low (2)	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc).
Medium (3)	Individuals may encounter significant inconveniences, which they will overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc)
High (4)	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc).
Very high (5)	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Probability
Probability is the likelihood of a risk to the rights and freedoms of individuals being realised. Factors to consider include the expected frequency of occurrence, and the motivation and capability of threat sources (eg does the threat require insider knowledge and/or significant technical resources to exploit any vulnerability?).

Probability	Scoring criteria
Very low (1)	0-5% - extremely unlikely or improbable For example, the risk has not occurred before or is not expected to occur within the next three years.
Low (2)	6-20% - low but not improbable For example, the risk is expected to occur once a year.
Medium (3)	21-50% - fairly likely to occur For example, the risk is expected to occur several times a year.
High (4)	51-80% - more likely to occur than not For example, the risk is expected to occur once a month.
Very high (5)	81-100% - almost certainly will occur For example, the risk is expected to occur once a week.

Risk level
Risk level is a function of impact and probability, and is represented by a RAG rating.

Probability / Impact	Very low (1)	Low (2)	Medium (3)	High (4)	Very high (5)
Very high (5)	Amber (5)	Amber (10)	Red (15)	Red (20)	Red (25)
High (4)	Green (4)	Amber (8)	Amber (12)	Red (16)	Red (20)
Medium (3)	Green (3)	Amber (6)	Amber (9)	Amber (12)	Red (15)
Low (2)	Green (2)	Green (4)	Amber (6)	Amber (8)	Amber (10)
Very low (1)	Green (1)	Green (2)	Green (3)	Green (4)	Amber (5)

Risk acceptance criteria

These criteria are guidelines only, and any risk treatment decisions should be made on a case-by-case basis. For example, it may be prudent to reduce a low risk because of legal and regulatory requirements.

Risk level	Acceptance criteria
Low (Green)	Within this range risks can be routinely accepted.
Medium (Amber)	Within this range risks can occasionally be accepted but shall be kept under regular review.
High (Red)	Within this range risks shall not be accepted and immediate action is required to reduce, avoid or transfer the risk.

Appendix 2: example risks to data subjects

Guidance: The following are examples of common risks associated with the processing of personal data to assist with your risk assessment. Not all of them will apply to your processing and the list is not exhaustive – you should consider specific risks that are relevant to your plans.

- Data is processed for unspecified / unlawful purposes/ not within expectations of data subjects
- Excessive data is processed
- Data is not kept up to date
- Data is kept for longer than is necessary by us
- Data is kept for longer than is necessary by data processor
- Data processed in contravention of data subject rights
- Data subjects unable to exercise their rights
- Data stolen or modified in transit
- Data stolen or modified at rest in our premises
- Data stolen or modified at rest in data processor premises
- Data transferred overseas to a jurisdiction that does not adequately protect data subject rights
- Re-identification of pseudonymised data by data processor or third party
- Unauthorised destruction or loss of data
- Data processor network / system / online portal not secure
- Data processor fails to process data in accordance with our instructions
- Personal data of children processed without appropriate safeguards / parental authority
- Consent of data subject not freely given (for example employer / employee processing)

- The data subject is particularly vulnerable (elderly or disabled) or is there a potential imbalance of power between the individual and the controller (employee/employer)
- Source of data poses risks re accuracy (obtained from a unverified or old list)
- Risk to accuracy of data due to matching / combining data from different sources
- Use of new technology, e.g. fingerprinting, face recognition
- Monitoring or recording individuals
- Using profiling according to characteristics or behavior
- Non-compliance with DP principles

9.0 Template Change History (for Information Management Service only)

Version	Date	Author	Change description
v0.1	01/06/2020	Steven Johnston	First draft
v1.0	07/10/2020	Steven Johnston	First release
v1.1	07/01/2021	Iman Elmehdawy	Amendment to guidance note page 2.
v1.2	18/03/2021	Helen Ward	Addition of Privacy by design at the ICO (pages 2 and 3)
v1.3	24/06/2021	Steven Johnston	Section 3.0 Q13 amended. Removed request for link to security assessment.
v2.0	07/03/2022	Steven Johnston	Full document review. Simplified privacy by design explanation on page 3 and made minor format changes throughout. Guidance note for 2.0 was updated and flow headings inserted to the text box. Next review date set to 31/1/2023.
V2.1	11/05/2022	Ben Cudbertson	Amended title of section 2 from 'data flows' to 'personal data lifecycle'

Case reference

IC-203321-W1K8

Use of Teams to Host Virtual GPA - DPIA

ico.
Information Commissioner's Office

Data Protection Impact Assessment (DPIA) template

You should complete this template where there is a new (or significant change to an existing) service or process that involves the processing of personal data (whether digital or hardcopy). When dealing with an existing process, service or system **only the change should be impact assessed.**

You should start to complete the assessment at the very start of your work and plan to revisit it throughout the lifecycle. Please note that the outcome of the assessment could affect the viability of what you are planning to do. In extreme cases, you will not be able to continue with your plans without changing them, or at all.

The Information Management and Compliance team is available to assist and advise on completing this template. If required this template should be submitted to the DPSIA forum for their consideration and recommendations. For assistance or to submit a DPIA for consideration email informationmanagement@ico.org.uk.

Determining what to complete:

You should complete all aspects of **sections 1 and 2** of this form to determine if a DPIA is required.

If you answer **no** to all screening questions in section 2 a full DPIA isn't required and there is no need to complete the additional sections of this assessment (see Approval).

If you answer **yes** to any of the screening questions in section 2 you **must** complete a full DPIA. You should complete all sections of this form except for 6.3 and 6.4 (see Approval).

Approval:

If a full DPIA isn't required. Inform your IAO and retain a copy of the partially completed form (sections 1 and 2) within your department.

If a full DPIA is required, the completed form **must** be submitted to the DPSIA Forum for their consideration and recommendations.

Once complete you should send this to informationmanagement@ico.org.uk

1. Process/system overview

1.1 Summary

Project ID:	N/A – GPA 2020
Project Title:	Use of Teams to host virtual GPA
Project Manager:	GPA Secretariat Hannah McCausland. Document authors Emma Deen & Neil Smithies

1.2 Synopsis

Due to the travel restrictions and social distancing rules being adhered to in response to the COVID-19 pandemic, the ICO proposes to use Microsoft 365 Teams functionality to host a virtual GPA in 2020 for ~300 attendees. Teams has previously been signed off for use as the ICO's video conferencing platform, therefore this document does not intend to re-visit these decisions, rather focus on the data protection considerations for external parties attending the GPA via a Teams invite.

Formatted: Not Highlight

Commented [IEM1]: Please link to the assessment

There may be a requirement to record the content of some or all of the GPA sessions. Should this be required, the recording and hosting of recorded content is covered by the DPIA entitled *MS Teams Live Events and Stream* dated 15 July 2020.

Commented [IEM2]: Please add link

Forms may also be used in conjunction with Teams meetings and to poll the audiences in order to offer a more engaging experience or collect quantitative data. No personal data will be collected through forms as it should only be used, in this context, for undertaking polls or votes.

ICO staff will be using existing laptop software and hardware to access the Team meeting invites. External stakeholders will access the GPA via email invite as external guests (not federated identities) via their browser or the Teams app. Neither require a Microsoft account to be created for the purpose of attendance.

1.3 Definition of processing

Guidance: As a data controller we are required to maintain a "record of processing activities" for which we are responsible (Article 30 refers). The following table is designed to help us define the planned processing operation.

Data controller(s)	ICO
Data processor(s)	Microsoft Ireland Operations Ltd
Joint data controllers	N/A
Purpose of processing	To deliver video content – both live and recorded – to external audiences, about the work of the ICO and seek input from delegates.

Categories of data	Email addresses, name (as provided by the attendee) images (of speakers/presenters) and Teams diagnostic/service data.
Categories of subjects	Internal viewers, internal producers, internal presenters, external presenters, external viewers
Categories of recipients	ICO, Microsoft
Overseas transfers	Data is hosted in Microsoft's UK and/or EEA data centres.

Commented [IEM3]: Are we putting streams out or putting anything on you tube , twitter feed?

Commented [IEM4]: Microsoft help is in the US

1.4 Purpose for processing

Guidance: State the context and business need being pursued in the processing, including the purposes, aims and the intended benefits for you, data subjects, society or others.

Internal: The Global Privacy Assembly (GPA) is the international forum of more than 130 global data protection and privacy authorities, chaired by Elizabeth Denham. This is an important, longstanding, international channel for the ICO. The COVID-19 pandemic has meant that plans to host the GPA in Mexico in 2020 are no longer possible, therefore there is a critical need for colleagues to be able to deliver the conference remotely.

External: As above, the GPA is an important event in the worldwide data protection and privacy field, which seeks to provide leadership at international level in data protection and privacy. It is vital that, despite the restrictions placed upon us by the COVID-19 pandemic, we are able to host the conference in some way, so that we can enable authorities to come together to meet this aim.

1.5 Lawful basis

Guidance: State the basis on which the processing is lawful under GDPR Article 6 (consent, performance of contractual obligations to a data subject, compliance with legal obligations, protecting the vital interests of a natural person, public task or legitimate interests). If you are processing based on legitimate interests you must also complete a legitimate interests assessment.

If you are processing data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, data concerning a person's sex life or sexual orientation or data relating to criminal convictions or offences, you will also need to state a further basis for that processing –see GDPR Article 9 and 10.

The lawful basis for processing is Article 6(1)(e) – public task.

1.6 Mandatory requirements

Guidance: Add the following requirements to your project backlog unless they do not apply (e.g. data need not be kept up to date in a system for storing old

records). Section 4 can be used to check that these have been completed, particularly if delivery is not being managed as a project.

<u>Data Accuracy</u>
a) Data must be kept up to date
b) There must be means to validate the accuracy of any personal data collected
c) Inaccurate or incomplete personal data must be updated on receipt of a lawful request from the data subject

<u>Retention & Deletion</u>
d) All data collected will have a retention period
e) Data must be deleted at the end of its retention period unless required by the National Archives for permanent preservation
f) Data kept beyond the retention period will be pseudonymised
g) Personal data must be erased upon receipt of a lawful request from the data subject

<u>Information & Transparency</u>
h) The data subjects shall be provided with:
(i) The identity and contact details of the data controller;
(ii) The purposes of the processing, including the legal basis and legitimate interests pursued
(iii) Details of the categories of personal data collected
(iv) Details of the recipients of personal data

<u>Objection & Restriction</u>
i) There must be means to restrict the processing of data on receipt of a lawful request from the data subject
j) There must be means to stop the processing of data on receipt of a lawful request from the data subject

<u>Security</u>
k) Appropriate training and instructions will be put in place to enable staff to operate the new system / process securely
l) Identify an Information Asset Owner
m) Update the Information Asset Register
n) Access controls must be in place for both physical and digital records

<u>Is the data being transferred outside the UK and EEA? If so:</u>
o) The data subjects must be provided with information on where to obtain details of any safeguards over data transferred to non-GDPR compliant countries
p) Consult the DPO for additional requirements to ensure the processing is GDPR compliant.

<u>Is the data being transferred to or through another organisation? If so:</u>
q) There must be controls to ensure or monitor compliance by external organisations.

<u>Is consent or pursuit of a contract the lawful basis for an automated processing operation? If so:</u>

r) *There must be a means to extract and transmit the data in a structured, commonly used and machine-readable format on receipt of a lawful request from the data subject*
s) *The consent must be recorded in some manner to serve as evidence*

Does our Privacy Notice need to be updated? If so:
t) *Update the Privacy Notice*
u) *Update the records of processing activities*
v) *There must be appropriate contracts in place with data processors / sub-contractors*

2. Data protection assessment screening

Guidance: The purpose of the screening questions is to determine if a DPIA is required. As a data controller we are required to perform DPIAs where the processing is likely to result in a high risk to the rights and freedoms of individuals (Article 35 refers).

2.1 Screening questions

ID	Criteria	Y/N
1	Will the processing involve evaluation or scoring, including profiling or predicting, especially in relation to an individual's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements?	N
2	Will the processing involve automated decision making that will have a legal or similar detrimental effect on individuals? For example, decisions that lead to exclusion or discrimination.	N
3	Will the processing involve the systematic monitoring of individuals in a publicly accessible area? For example, surveillance cameras in a shopping centre or train station.	N
4	Will the processing involve sensitive personal data or data of a highly personal nature? For example, special categories of data (Article 9 refers), personal data relating to criminal convictions or offences (Article 10 refers), and personal data linked to household and private activities.	N
5	Does the processing involve large scale processing of data at a regional, national or supranational level, and which could affect a large number of data subjects?	N
6	Does the processing involve matching and combining two or more datasets that have been collected for different purposes and/or by different data controllers?	N
7	Does the processing concern vulnerable individuals who may be unable to easily give consent or object to the processing? For example, children, employees, and others who require special protection (mentally ill persons, asylum seekers, patients, the elderly).	N
8	Does the processing involve the innovative use or application of new technological or organisational solutions? For example, "Internet of Things" applications can have significant impacts on subjects' daily lives and privacy.	N

9	Does the processing prevent individuals from exercising a rights or using a service or contract? For example, where a bank screens its customers again credit reference database in order to decide whether to offer them a loan.	N

*Guidance: If you answer "Yes" to one or more questions you should complete a DPIA. If you answer "No" to all questions a full DPIA is **not** required but you must still keep a record of this document as evidence that you have considered the data processing operation against the screening questions. You can save this locally in your department and it does not need to be submitted for consideration by the DPSIA forum.*

2.2 DPIA approach and consultation

Guidance: Record which parts of the DPIA you will be completing and your rationale (especially if your choices differ from the guidance above).

Explain what practical steps you will take to ensure that you identify and address the data protection risks. Include details of:

- *Who should be consulted, internally and externally? This must include the DPO's team and Cyber Security. You should also consult data subjects or their representatives unless this is not possible or appropriate – e.g. it would be disproportionate, impractical, undermine security or compromise commercial confidentiality.*
- *If data subjects (or their representatives) will not be consulted you must document the reasons for this.*
- *Consider whether consultation with processors or sub-processors is needed.*
- *How you will carry out the consultation. You should link this to the relevant stages of your project management process or delivery plan.*

Although the screening questions indicate a DPIA isn't required we have decided to complete a full DPIA to consider any risks to conference attendees associated with our plans.

Consultation:

To confirm, this DPIA is not intended to cover the ongoing review of ICO's ~~does not revisit any decisions already taken re the ICO's~~ use of Microsoft Teams during then COVID-19 pandemic – therefore any requirement for consultation was focussed on the processing of attendee data, and any consultation required around this.

Due to the small amount of data being processed, the standard use of well-known technology, and the optional nature of attendance it is deemed to be disproportionate to consult with the data subjects. The privacy notice will be used to share relevant information to conference attendees to ensure transparency.

Microsoft will be consulted if risks, concerns or queries about the software arise during the DPIA process.

3. Data inventory

3.1 Information flows

Guidance: Provide a systematic description of the processing, including:

- *What personal data is collected*
- *The specific purpose of your processing*
- *The source of the data (including whether the data subjects are vulnerable, the relationship with the data subjects, the manner of collection and the level of control the data subjects have over the data once collected)*
- *The nature and context of the processing (including whether there are new technological developments or any relevant current issues of public concern)*
- *The scope of the processing (including the nature and volume of data, frequency and duration of processing, sensitivity of the data and the extent of the processing)*
- *The storage and transfer of the data (including details of hardware, software, networks, key people and details of any paper records or transmission channels)*
- *Responsibilities for the data (including the information asset owners, how responsibilities for information change through the data flow and the boundaries of responsibilities in any handover)*

You may find it useful to refer to a flow diagram or other way of explaining information flows. You should also say how many individuals are likely to be affected by the processing of personal data.

General background information on Microsoft Teams

Microsoft Teams 'meeting' functionality was introduced to support key activities when the ICO offices closed due to the COVID-19 pandemic. As part of the initial roll out of MS Teams ICO colleagues were provided with risks and opportunities information; this is being further expanded reviewed to incorporate the introduction of Teams 'meeting' functionality. ~~is already available to all ICO staff and is used for internal meetings~~.

In order to ensure that the GPA can continue despite the ongoing travel restrictions and social distancing rules, we are seeking to use the Teams 'meeting' functionality to host the conference remotely.

GPA attendees would be sent an invite to the session/s of their choosing, and would join via their browser or the Teams app.

As previously mentioned the meeting recording feature may be utilised for the GPA; this is covered in a separate DPIA.

Commented [IEM5]: GPA organisers need to make sure it is the PN

When a meeting organiser creates a Teams 'meeting' they can choose to use a lobby function to screen attendees before allowing them to join the meeting. ~~They can also choose to use an attendee report if required.~~

Within the chat function on a Teams 'meeting', there is a feature to share documents via OneDrive. If a staff member shares a OneDrive document via the chat function – external candidates can see the document in the chat function but they cannot access it. If the meeting organiser wishes to share a document with external attendees, then the document would be sent out as an attachment to the email containing the invite.

Commented [IEM6]: Is there a clear process to communicate this to organisers?

Chat messages are held in a hidden folder in Outlook and will be subject to a 7 day retention period, these are only searchable by IT administrators.

What personal data will be collected

We will process the names and email addresses of attendees for the purpose of facilitating access to the GPA sessions.

When people access the ICO's meetings via a browser Microsoft set Google Analytics cookies and targeting/advertising cookies. We have no control over what cookies are dropped or how and have no access to the information collected by them.

Microsoft Teams, as a cloud-based service, processes various types of personal data as part of delivering the service. In this regard they are a data processor acting on behalf of the ICO as data controller.

As a meeting attendee accessing Teams as an external attendee ~~as a guest,~~ very limited data is shared with Microsoft. The data that is transferred to Microsoft is explored in more detail below:

a. Census – This is data about the application and device used to access the meeting, encrypted user and device IDs that CANNOT be linked back to a named user.
b. Usage – Statistical data about the number of times the application has been used, the number of successful meetings and the name of the Teams Instance that they are connecting to. Usage data DOES NOT contain any information that identifies users.
c. Error Reporting – Error reporting data can include information about performance and reliability, device configuration, network connection quality, error codes, error logs, and exceptions. Error logging is not automatically on. If we switch error reporting on in group policy, AND the individual choses to enable logging for meeting diagnostics (a specific Teams setting must be selected) then personally identifiable information such as USERID and Session Initiation Protocol Uniform Resource Identifier (SIP URI) are sent to MS within error logs. We do not intend to switch on error logging.

See https://docs.microsoft.com/en-us/microsoftteams/data-collection-practices

In addition to the above, diagnostic data is collected and sent to Microsoft about Teams software being used on computers running Windows in the ICO. There are three levels of diagnostic data for Teams software:

- **Required** The minimum data necessary to help keep Office secure, up-to-date, and performing as expected on the device it's installed on.
- **Optional** Additional data that helps us make product improvements and provides enhanced information to help us detect, diagnose, and remediate issues.
- **Neither** No diagnostic data about Teams software running on the device is collected and sent to Microsoft. This option, however, significantly limits Microsoft's ability to detect, diagnose, and remediate problems your users may encounter using Teams.

Required diagnostic data could include, for example, information about the version of Teams client installed on an ICO device, or include information that indicates that the Teams application is crashing when trying to join a meeting. Optional diagnostic data could include information about the time it takes to initiate a phone call, which could indicate an issue with connectivity or network performance.

This diagnostic data doesn't include names of users, their email addresses, or the content of their Office files. The Microsoft system creates a unique ID that it associates with the user's diagnostic data. When Microsoft receive diagnostic data showing that the Teams app crashed 100 times, this unique ID lets them determine if it was a single user who crashed 100 times or if it was 100 different users who each crashed once. Microsoft don't use this unique ID to identify a specific user.

See https://docs.microsoft.com/en-us/microsoftteams/policy-control-overview

The ICO also share Required service data. Office consists of client software applications and connected experiences designed to enable us to create, communicate, and collaborate more effectively. Working with others on a document stored on OneDrive for Business or translating the contents of a Word document into a different language are examples of connected experiences.

When we use a connected experience, data is sent to and processed by Microsoft to provide that connected experience. This data is crucial because this information enables Microsoft to deliver these cloud-based connected experiences. This data is referred to as required service data.

Required service data is organized into the following categories:
- Software setup and inventory
- Product and service usage
- Product and service performance
- Device connectivity and configuration

The information in these categories enables Microsoft to assess whether a connected experience or essential service is secure, up to date, and performing as expected. We don't expect any GPA attendee data to be shared in the data sent to and processed by Microsoft in required service data.

See https://docs.microsoft.com/en-us/deployoffice/privacy/required-service-data

Note - there are also a set of services that are essential to how Microsoft 365 Apps for enterprise functions and cannot be disabled. For example, the licensing service that confirms that you are properly licensed to use Microsoft 365 Apps for enterprise. Required service data about these services is collected and sent to Microsoft, regardless of any other policy settings that we have configured. Again, no GPA attendee data would be shared within this required service data.

See https://docs.microsoft.com/en-us/microsoftteams/policy-control-overview

Source of the data

As above, and personal data in the form of email address will be collected directly from data subjects if they provide it to us.

The name of candidates can be entered into Teams when joining the sessions if the candidate choses to, but is not mandatory.

When joining a Teams meeting invite, the attendee provides their IP address to Microsoft to enable them to connect to the meeting. Attendee IP addresses will be used for this purpose for the duration of the Teams meeting only. This is normal practice and one we feel is reasonable for attendees to expect, we have therefore focussed this assessment specifically on the question of any telemetry data collected by Microsoft during the sessions, as the purpose for processing is different from the above, and it's collection may not be an expectation of the attendee.

Formatted: Font: 11 pt

Formatted: Space After: 10 pt, Line spacing: Multiple 1.15 li

Commented [IEM7]: The PN will have this I presume.

Formatted: Font: 11 pt

During the GPA there is the potential that a candidate's external IP address could be collected as part of diagnostic data ~~is~~ if an error is encountered during the conference, ~~and if the attendee is not joining via a proxy service.~~ This may be the IP address assigned by their internet service provider if connecting from home, or the public IP address of an organisation if connecting via a corporate proxy. Neither Microsoft Teams or the ICO will monitor or prohibit candidate's use of VPN or proxy servers to obfuscate their true IP address.

Microsoft 'Get Help' uses resources outside EEA. These can be based in the US so could access the desktop/MS applications of an ICO employee if the Get Help function were to be used during the conference.

The scope of the processing

No sensitive personal data is referenced above. Candidates are not required to register with Microsoft to attend the event, and are not required to enter personal data when joining the meeting, although it is customary to join the meeting using their given name and details of the organisation they represent . As outlined above, diagnostic and service data is provided to Microsoft in order for them to provide us with the services they are contracted to deliver.

Use of audio and camera is optional for attendees. ~~Presenters of live events will be expected to have their audio and cameras on when delivering an event and~~

~~will have their image captured as a result. For candidates attending the meetings this is optional.~~

Commented [IEM8]: I've spoken to international some time ago about voting via teams and how the vote forms can be an opinion. My understanding is that they will send voting forms by email, is this correct? If not can the use of forms for voting be tracked to an individual respondent?

Storage and transfer of data

The data will be processed through Microsoft O365 Teams. It will be stored via our Azure Secure Environment. All data is hosted in a Microsoft data centre in the UK and/or EEA.

Microsoft Teams retains data for the minimum amount of time necessary to deliver the service to the ICO.

Because this data is required to provide the service to us, this typically means that Microsoft retain personal data until we stop using Microsoft Teams, or until the we delete personal data. If a user (or an administrator on the user's behalf) deletes the data, Microsoft will ensure that all copies of the personal data are deleted within 30 days.

~~Windows 10, version 1809 and newer allows a user to delete diagnostic data collected from their device by using **Settings** > **Privacy** > **Diagnostic & feedback** and clicking the **Delete** button under the **Delete diagnostic data** heading. We~~An ICO admin has the ability to request the deletion of any diagnostic data sent to Microsoft. We recommend that this is completed with ICO attendees ~~complete this action~~ following each Teams session to minimise the potential for inclusion of candidate data within the diagnostic data~~.~~

Commented [ED9]: Does this seem like a reasonable recommendation? Wasn't sure if there were potential side-effects?

Commented [RW10R9]: Im thinking this would only clear the data collected on ICO staff device and not externals joining the GPA meeting. Would we advise attendees to clear cache in browser after GPA event?

Commented [IEM11R9]: I think yes,again in the invite or PN

If the ICO terminate service with Microsoft, corresponding personal data will all be deleted between 90 and 180 days of service termination.

In some circumstances, local laws require that Microsoft Teams retain telephone records (for billing purposes) for a specific period of time, in those circumstances Microsoft Teams follows the law for each region.

Additionally, if a company requests that Microsoft Teams hold a user's data to support a legal obligation, Microsoft will respect the company administrator's request.

In the case of the GPA, emails will be collected via the ICO's CMS Umbraco and deleted after a link to recording of the event has been sent.

Responsibilities for the data

Digital & IT Services are responsible for the relationship between the ICO and Microsoft. Raymond Wong will be the lead contact for this.

The Communications team will oversee the recording functionality in meetings. Hannah Smith will be the lead contact for Communications.

3.2 Data inventory

Guidance: Identify the personal data to be held, the recipients (those with access to the data), the retention period and the necessity of the data collection, processing and retention.

Data Type	Recipients	Retention Period	Necessity
Email addresses of attendees	GPA event organiser(s) within the ICO and IT support	The period of the GPA only	To invite attendees to event and in the case of a closed meeting validate attendees
Image of presenters (and any attendees that chose to turn on their camera)	Event organisers, IT support, attendees, presenters and viewers	Any recording created for the communication teams purposes will be deleted after 12 months. Any recording created for workforce development and planning purposes will be deleted 6 years after superseded. Knowledge sharing purposes will be deleted 12 months after last action	Presenters: to deliver a live event Attendees: The attendee can chose not to have their image captured if they chose. They will need to be informed ahead of a meeting if it is going to be recorded and published more widely after the event in order to make an informed decision.
Additional data shared verbally or in Q&A	Event organisers, IT support, attendees, presenters and viewers	As above.	Before any event attendees should be encouraged not to share personal data in these ways and informed if it will be recorded and shared.

			In the case of the moderated Q&As – moderators should be briefed to consider carefully whether to share comments with PD in them and instructed never to share comments with SCD in them.
Cookies – data collected by Microsoft from attendees joining via web browser	External attendees	Not known.	Microsoft set Google Analytics cookies and targeting/advertising cookies. We are unable to implement any technical measures to prevent this, however would refer attendees to guidance available on our website about managing cookie preferences at https://ico.org.uk/global/cookies/~~We have no control over what cookies are dropped or how and have no access to the information collected by them.~~
Diagnostic and Service data – collected by Microsoft	Microsoft	Minimum amount of time necessary to deliver the service.	ICO staff can manually ~~turn off~~set ~~optional~~ diagnostic data for the duration of the GPA to "required diagnostic data", this sends only info about the ICO device, its settings and capabilities and whether it is performing properly.~~,~~ ~~though this may impact on Microsoft's ability to support the application during the conference~~.

Formatted: Font: 11 pt

Formatted: Default Paragraph Font, Font: 11 pt

Field Code Changed

Commented [IEM12]: Do we need to add voting forms and IP addresses in limited circumstances?

Commented [ED13]: Can you check this is correct?

Commented [RW14R13]: Optional diagnostic is not available for MMD devices. Default is" Enhanced". Staff can set to "required " during the GPA and only device health is sent to MS.

Commented [ED15R13]: I'm proposing we delete this – John H's view is that if the user changes the default it will just revert back minutes later anyway…

4. Compliance measures

Guidance: Use this section to record your compliance with the requirements in section 1.6. Fill in the details of how the requirements have been met. The requirement source is a reference to GDPR unless otherwise stated.

Requirement	**Implementation Details**
Data Accuracy	
a) Data must be kept up to date	Contact email addresses can be updated with ease. Recordings will not need to be updated as they will be an accurate recording of the meeting or event.
b) There must be means to validate the accuracy of any personal data collected	It is expected that personal data will be limited to name, email address and maybe company name and the attendee will be providing the details themselves so these will be accurate. Recordings will be an accurate recording of the meeting or event.
c) Inaccurate or incomplete personal data must be updated on receipt of a lawful request from the data subject	Email addresses can be updated at any time prior to an event or meeting. It will not be possible to update event recordings.
Retention & Deletion	
d) All data collected will have a retention period	Any recording created for communication purposes will be deleted after 12 months. Email addresses collected for the purposes of sending the invite will be deleted in line with the retention period described in the privacy notice issued to all conference attendees. In the event that diagnostic or service data containing personally identifiable information is transferred to Microsoft during the GPA then this data will be held by Microsoft for the minimum amount of time necessary to deliver the service. Because these needs can vary for different data types, the context of Microsoft's interactions with the ICO or our use of products, actual retention periods can vary significantly.
e) Data must be deleted at the end of its retention period unless required by the National Archives for permanent preservation	Attendee email addresses will be deleted once invites have been sent. Microsoft will delete any telemetry data at the end of the retention policy. The user can manually delete this earlier if required.

f) Data kept beyond the retention period will be pseudonymised	N/A
g) Personal data must be erased upon receipt of a lawful request from the data subject	Requests for deletion will be addressed by the Communications department in the first instance. Any requests for deletion of telemetry data will be referred to Digital & IT for review at administrator level. Any requests for deletion of data held by Microsoft that cannot be addressed by the above will be made to Microsoft Ireland Operations Limited.
Information & Transparency	
h) The data subjects shall be provided with: ● the identity and contact details of the data controller; ● the contact details of the Data Protection Officer; ● the purposes of the processing, including the legal basis and legitimate interests pursued ● details of the categories of personal data collected ● details of the recipients of personal data	Covered in the GPA Privacy Notice and we will consider if additional fair processing information is required for each meeting / event.
Objection & Restriction	
i) There must be means to restrict the processing of data on receipt of a lawful request from the data subject	This is the responsibility of the communications department. Individuals are able to update some privacy settings themselves, these details will be included in the GPA privacy notice.
j) There must be means to stop the processing of data on receipt of a lawful request from the data subject	This is the responsibility of the communications department. Attendance at the GPA is optional
Security	
k) Appropriate training and instructions will be put in place to enable staff to operate the new system / process securely	Teams meeting guidance and training to be created and maintained.
l) Identify an Information Asset Owner	Director of Communications & Director of Resources.
m) Update the Information Asset Register	TBC

n) Access controls must be in place for both physical and digital records	IT Help will have access to all areas of Teams as the administrators of the O365 apps.
Conditional Requirements	
o) The data subjects must be provided with information on where to obtain details of any safeguards over data transferred to non-GDPR compliant countries	Covered in the Privacy Notice.
p) Consult the DPO for additional requirements to ensure the processing is GDPR compliant.	The DPO's advice shall be sought as part of the DPIA process
q) There must be controls to ensure or monitor compliance by external organisations.	N/A
r) There must be a means to extract and transmit the data in a structured, commonly used and machine-readable format on receipt of a lawful request from the data subject	N/A
s) Any consent must be recorded in some manner to serve as evidence	N/A
t) Update the Privacy Notice	A new Privacy Notice will be drafted for attendees of the GPA.
u) Update the Article 30 Records of Processing Activities	To be updated by the Information Management Service.
v) There must be appropriate contracts in place with data processors / sub-contractors	Contracts are in place with Microsoft for Office 365.

5. Data protection summary risk assessment

Guidance: Record a summary of identified and assessed risks to data subjects' rights, the actions you have taken (existing) and could take (expected) to reduce the risks. Detail any future steps that will be necessary (eg the production of new guidance or security testing for new systems). Some example risk sources have been listed to aid you below and in Appendix 2. The examples are not exhaustive. Equally not all will be relevant to your specific processing activities. See Appendix 1 for guidance on assessing impact and probability.

Risks should be considered from the data subject's perspective not the ICO's (eg a reputational risk to the ICO should not be recorded here). Some example threats to consider include:

- *Discrimination*
- *Identity theft and fraud*
- *Financial loss*
- *Damage to data subjects' reputation*
- *Loss of confidentiality of professional secrets*
- *Unauthorised reversal of pseudonymisation*
- *Social or economic disadvantage*
- *Deprivation of legal rights or freedoms*
- *Data subjects losing control over their data*
- *Loss of privacy or intrusion into private life*
- *Prevention from accessing services*

Commented [ED16]: I haven't updated from here onwards yet – think we'll need to do this in conjunction with IG once we're happy that the sections above appropriately describe the data processing taking place.

Risk Description	Response to Risk	Risk Mitigation	Expected Risk Score		
			I	P	Total
[Guidance: Describe the cause and likelihood of; and the threat to the data subjects rights, and the impact on the data subject should the risk be realised- 3 elements]	*[Guidance: Describe risk treatment (e.g. reduce, avoid, accept or transfer)]*	*[Guidance: Describe existing activity and controls to reduce risk and any further activity or controls to be taken that are expected to reduce the risk- 2 elements]*	*[Guidance: I is impact score and P is probability score and IxP is the Total Score. Probability is the likelihood of the risk being realised after Risk Mitigations have been achieved.*		
MS drop cookies without consent when users land on the Teams page on a browser. This includes dropping tracking, analytics and advertising cookies. People are unable to consent to their data being used in this way	Accept	Existing: Email Microsoft to inform them that their platform is not compliant and request they look at rectifying this. Expected: Inform users of the activity on the site before sending them to it so they can make an informed (albeit not ideal) decision.	2	5	10

An attendee might share personal data, including SCD verbally or via the Q&A function	Reduce	Expected: Producers of live events should be briefed about what to do in instances where PD is shared via Q&As. It should be at the producers discretion as to whether it is shared with the group, unless it is SCD in which case it should always be deleted. Instructions should be sent to presenters and attendees advising them not to share PD. Clear fair processing information should be shared with all attendees and presenters so they aware what will happen to any PD shared.	2	2	4

Data is stolen or mishandled	Reduce	Existing: All data is hosted in Azure Secure environment. Security assessments have been completed of the platforms. Access to the information is limited. L&D and Communications will be the only departments in the ICO with Streams channels. Only certain members of the relevant teams in those departments will be granted access to add, edit or remove the meeting and event recording. IT Help will have access to all areas of Stream as the owners of the 365 apps. Only members of the communications department have access to the ICO corporate Vimeo and YouTube channels. A policy is in place to update the passwords to these platforms quarterly and/or when a member of the team leaves the ICO. The data is minimal and not sensitive	2	1	2
Staff do not follow procedures when undertaking events meaning attendees do not have access the PN, SCD is shared via the Q&A, unauthorised people access the platforms	Reduce	Expected: IT will limit the roll out recording functionality, live events and Stream to preapproved members of staff. Procedures will be drawn up about how to conduct meetings, events etc. and will include instructions to provide fair processing information to attendees.	3	2	6

An ICO staff member asks for people to share additional personal data via a form during an event	Reduce	Expected: IT will limit the roll out of forms to a small number of approved staff. Procedures will be drawn up instructing staff to only use forms to collect non-personal data.	2	1	2
Unauthorised people attending events and meetings	Reduce	Existing mitigation: When meeting organiser creates a Microsoft Live Event, they can choose for it to be a public event, an internal meeting (where only ICO colleagues can join), or they can limited it further to only specified people or groups. When a meeting organiser creates a Microsoft Teams Meeting they can use the Lobby functionality to screen people before allowing them into the meeting. Attendees must sign in to Teams or join as a guest allowing the host to see who is joining.	2	1	2

Commented [IEM17]: If a delegate asks us for information collated about them by Microsoft during the event, can we answer this question? It will be regarding diagnostic and service data?

6. Expected residual risk and sign off

6.1 High and medium level expected residual risk

Guidance: Record details of the remaining risk. It is never possible to remove all risk so this section should not be omitted or blank. If the residual risk remains high (e.g. red on the traffic light scoring in the Appendix) then you will need to consult the ICO by following the process used by external organisations.

Residual risk is mostly assessed as low but there are two medium risks. We are progressing our enquiries with Microsoft regarding the non-essential cookies to try and reduce this risk. The remaining medium risk results from staff not following procedures. The necessary procedures will be drawn up and communicated to relevant staff and should be followed by staff for every meeting / live event.

6.2 Necessity and proportionality

Guidance: If you answered "Yes" to one or more of the screening questions in Section 2.1 you should discuss the necessity and proportionality of the collection, processing and retention of this data here, weighing the impact on data subjects rights and freedoms against the benefits of the processing activity. You should also consider whether there are other reasonable ways to achieve the same result with less impact on data subjects.

Necessity covered at 1.4 & 3.2.

6.3 DPO recommendations

Guidance: Record any recommendations from the DPO or their delegates and responses here. This serves as useful tool when reconsidering a rejected DPIA or in recording the justification if the organisation rejects the DPO's advice.

No	Recommendation	Project Team Response
1	Ensure appropriate measures are used to guard against unauthorised people accessing meetings For example the lobby feature should be used for all meetings.	Where a closed meeting is required, the Lobby feature will be used to only allow access to those who have registered. When only a small number of attendees are present for a meeting it is also possible for the participants list to be viewed. Appropriate measures available for guarding against unauthorised access will be noted in the Policy

		and Procedures documentation.
2	Consider procuring additional software that allows for the editing of videos we intend to publish so we can remove unnecessary personal data from recordings.	Communications team have editing software available if unnecessary personal data needs to be removed.
3	Develop the guidance referenced above as soon as possible so staff are properly trained and are using the additional functionality in a way that minimises risk.	This additional functionality will be limited to a small number of named staff. Policy and Procedures documentation is in progress to assist with guidance.
4	Continue to progress the query with Microsoft about the non-essential cookies and update this DPIA with the conclusion.	Issue has been submitted to the MS privacy portal – ref PRV0032076. Microsoft deployed a correction on May 20, 2020 which has resolved issue on App, still waiting for resolution for desktop.
5	Recordings should be reviewed before publication to check that there is no personal data or other content that it would be unfair to publish.	It will be the responsibility of the Event Producer to review any recordings for their suitability for publication, this will be noted in the Policy and Procedures documentation

6.4 Sign Off

Guidance: Send this to the DPSIA forum to consider the privacy and security risks involved in the processing, the solutions to be implemented and the residual risk.

Considered by	**Date**	**Project Stage**
DPIA Forum	01/07/2020	Planning
IAO - Jen Green, Director of Corporate Communications	15/07/2020	
IAO - Andrew Hubert, Director of Resources	10/07/2020	

7. Integrate the outcomes back into the plan

Guidance: Identify who is responsible for integrating the DPIA outcomes back into any project plan and updating any project management paperwork. Who is responsible for implementing the solutions that have been approved? Who is the contact for any data protection concerns which may arise in the future?

Action to be taken	Date for completion	Responsibility for Action	Completed Date
Policy and Procedures to be drafted	24th July 2020	Sue Shepherd	
Continue to progress with Microsoft the non-compliance cookies issue		Ray Wong	

Contact point(s) for future data protection concerns	Sue Shepherd

8. Change history

Guidance: To be completed by the person responsible for delivering the system, service or process (in a project this will be the project manager).

Version	Date	Author	Change description
0.1	01/07/2020	SS/HS/SJ	First Draft
1.0	10/07/2020	AH	Final release

9. Template Document control

Title	Data Protection Impact Assessment Template
Version	2.0
Status	Final release
Owner	DPSIA Forum
Release date	17/07/19
Review date	17/07/20

Appendix 1: Risk Assessment Criteria
The following criteria are aligned with our corporate risk assessment criteria.

Impact
Impact is the consequence of a risk to the rights and freedoms of individuals being realised. Factors to consider include the financial harm or emotional distress that can be expected to occur.

Impact	Scoring criteria
Very low (1)	No discernible impact on individuals.
Low (2)	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc).
Medium (3)	Individuals may encounter significant inconveniences, which they will overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc)
High (4)	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc).
Very high (5)	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Probability
Probability is the likelihood of a risk to the rights and freedoms of individuals being realised. Factors to consider include the expected frequency of occurrence, and the motivation and capability of threat sources (eg does the threat require insider knowledge and/or significant technical resources to exploit any vulnerability?).

Probability	Scoring criteria
Very low (1)	0-5% - extremely unlikely or improbable For example, the risk has not occurred before or is not expected to occur within the next three years.
Low (2)	6-20% - low but not improbable For example, the risk is expected to occur once a year.
Medium (3)	21-50% - fairly likely to occur For example, the risk is expected to occur several times a year.

High (4)	51-80% - more likely to occur than not For example, the risk is expected to occur once a month.
Very high (5)	81-100% - almost certainly will occur For example, the risk is expected to occur once a week.

Risk level
Risk level is a function of impact and probability, and is represented by a RAG rating.

Probability / Impact	Very low (1)	Low (2)	Medium (3)	High (4)	Very high (5)
Very high (5)	Amber (5)	Amber (10)	Red (15)	Red (20)	Red (25)
High (4)	Green (4)	Amber (8)	Amber (12)	Red (16)	Red (20)
Medium (3)	Green (3)	Amber (6)	Amber (9)	Amber (12)	Red (15)
Low (2)	Green (2)	Green (4)	Amber (6)	Amber (8)	Amber (10)
Very low (1)	Green (1)	Green (2)	Green (3)	Green (4)	Amber (5)

Risk acceptance criteria
These criteria are guidelines only, and any risk treatment decisions should be made on a case-by-case basis. For example, it may be prudent to reduce a low risk because of legal and regulatory requirements.

Risk level	Acceptance criteria
Low (Green)	Within this range risks can be routinely accepted.
Medium (Amber)	Within this range risks can occasionally be accepted but shall be kept under regular review.
High (Red)	Within this range risks shall not be accepted and immediate action is required to reduce, avoid or transfer the risk.

Appendix 2: Common risks to data subjects

The following are examples of common risks associated with the processing of personal data to assist with your risk assessment. Not all of them will apply to your processing and the list is not exhaustive – you should consider any other specific risks that may apply in relation to your intended processing.

- Data is processed for unspecified / unlawful purposes/ not within expectations of data subjects
- Excessive data is processed
- Data is not kept up to date
- Data is kept for longer than is necessary by us
- Data is kept for longer than is necessary by data processor
- Data processed in contravention of data subject rights
- Data subjects unable to exercise their rights
- Data stolen or modified in transit
- Data stolen or modified at rest in our premises
- Data stolen or modified at rest in data processor premises
- Data transferred overseas to a jurisdiction that does not adequately protect data subject rights
- Re-identification of pseudonymised data by data processor or third party
- Unauthorised destruction or loss of data
- Data processor network / system / online portal not secure
- Data processor fails to process data in accordance with our instructions
- Personal data of children processed without appropriate safeguards / parental authority
- Consent of data subject not freely given (for example employer / employee processing)
- The data subject is particularly vulnerable (elderly or disabled) or is there a potential imbalance of power between the individual and the data controller (employee/employer)
- Source of data poses risks re accuracy (obtained from a unverified or old list)
- Risk to accuracy of data due to matching / combining data from different sources
- Use of new technology, e.g. fingerprinting, face recognition
- Monitoring or recording individuals
- Using profiling according to characteristics or behavior
- Non-compliance with DP principles

Case reference

IC-203321-W1K8

Windows Hello – Draft DPIA

ico.
Information Commissioner's Office

Data Protection Impact Assessment (DPIA) template

You should complete this template where there is a new (or significant change to an existing) service or process that involves the storage/processing of personal data (whether digital or hardcopy). When dealing with an existing process, service or system **only the change should be impact assessed.**

The DPO's team is available to assist and advise on completing this template.

The template should be submitted to the DPSIA Committee for their recommendations and approval.

For assistance or to submit a DPIA for approval email IGhelp@ico.org.uk.

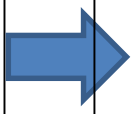
You should start to complete the template as soon as you decide to implement a new system or process. How frequently the DPIA is reviewed and the governance required will vary with the risk of the system or process. At a **minimum**:

Projects: you should produce an initial DPIA prior to finalising your requirements, complete it before finalising your design and review & update the DPIA at least once more prior to go-live. In an Agile project, you should update the DPIA at the start and end of each Epic, or where there is a significant change to the data being processed or the technology or platform. Each update should be submitted to the DPSIA Committee.

Non-projects: you should complete the DPIA prior to designing the service or seeking suppliers and update it whenever there are material changes to the planned system or process.

Screening: Determine what to complete:

1. **GDPR DPIA**: Complete all sections if you meet 2+ questions in section 2.1
2. **Full DPIA**: Complete everything but section 6.2 if you meet 2+ screening questions in any section
3. **Compliance Checklist**: Complete sections 1, 2 and 4, plus signoff, if you don't meet the screening questions



Approval: Consult the DPO's team and select an option for the approvers based on your risk:

1. **DPSIA Committee**: including Senior Information Risk Officer, Head of Cyber Security, DPO
2. **DPSIA Committee**: including DPO and Head of Cyber Security
3. Representatives of DPO and Cyber Security, who will also send it to the DPSIA Committee for their information

Regardless of the option chosen, **the DPIA should be submitted together with your SIA**.

1. Process/system overview

1.1 Summary

Guidance: For projects please provide the following key details. Non-projects should provide a key contact who is responsible for delivering the system or process.

Project ID:	
Project Title:	Windows Hello
Project Manager:	Deborah Holt

1.2 Synopsis

Guidance: Provide a summary of the process or system including any relevant background information and the key aims/objectives that the system or process must achieve. There is no need for a detailed discussion of data or data flows – these are covered later in the assessment.

The Microsoft Managed Desktop programme is currently an invite only programme where Microsoft takes responsibility for the configuration, imaging, application deployment, software updates, security and end user support of a device. The service is made up of a combination of existing Microsoft services with an additional monitoring, management and support wrapper.

The components can be summarised as follows;

- Microsoft 365 E5
    - Office 365 E5
    - Windows 10 Enterprise E5
    - Enterprise Mobility + Security E5
- Microsoft Managed Desktop IT as a Service
    - Microsoft Support ("Get Help")
    - Microsoft Operations & Monitoring
- A Microsoft Surface Device

DPSIA's have already been completed for the following areas;

- Office 365 including Enterprise Mobility + Security
- Microsoft Get Help 24x7 Support ("Get Help")
- Microsoft Windows Diagnostics and Telemetry (Advanced Threat Protection)

Additional DPSIA's will be completed for;

- Microsoft Cortana Voice Recognition
- Get Help
- MMD threat protection

Scope of this DPIA

- Windows Hello Biometric Framework

DRAFT

Windows Hello is the Microsoft Window's biometric login framework, its purpose is to provide a replacement for password based login, using your face (or on some devices, fingerprint), authentication certificates and certificates stored on the Microsoft Surface device to log you into your device, software and network resources.

Windows Hello is a faster way of logging into your device and reduces the risk associated with compromised passwords.

When you first register with Windows Hello on your new Surface device, the webcam array uses your facial geometry to create a data representation of your face, this isn't a photograph but an encrypted graph based on the distances and depths of your facial features. This encrypted graph is stored on your device only.

When you log into your device, your facial geometry is used to unlock a user authentication certificate stored in the device's TPM chip (a secure enclave on your device's motherboard), which is used to unlock your device and authenticate you to your resources.

The data representation of your face is encrypted and stored on your Surface device only, it is not sent to Microsoft or stored anywhere else, it cannot be exported from the device and is used only for the purposes of user authentication by the Windows Hello framework. Applications may talk to the Windows Hello framework to verify your identity but the framework will only respond with pass or fail for the authentication attempt.

Users have the option of falling back to PIN based authentication if they do not wish to enrol in the biometric framework, the encrypted PIN is stored on the device and is subject to same complexity requirements as the ICO's user login password.

1.3 Definition of processing

Guidance: As a data controller we are required to maintain a "record of processing activities" for which we are responsible (Article 30 refers). The following table is designed to help us define the planned processing operation.

Data controller(s)	ICO
Data processor(s)	Microsoft
Purpose of processing	Biometric User Authentication
Categories of data	Biometric graph of facial features, user telephone number.
Categories of subjects	ICO Staff
Categories of recipients	Microsoft – only the telephone number for the purpose of multi factor identification.
Overseas transfers	To Microsoft in the USA. Microsoft have a current Privacy Shield certification.

1.4 Purpose for processing

Guidance: State the business need being pursued in the processing, including the purposes, aims and the intended benefits for you, data subjects, society or others.

Windows Hello Biometrics are used to improve the security posture of the ICO by reducing the need for passwords which are often regarded as a weak point in user authentication.

The user is briefed on Windows Hello as part of on-boarding process. If a user does not wish to enrol in the biometric elements of Windows Hello, then they are free to use PIN authentication only.

1.5 Lawful basis

Guidance: State the basis on which the processing is lawful under GDPR Article 6 (consent, performance of contractual obligations to a data subject, compliance with legal obligations, protecting the vital interests of a natural person, public task or legitimate interests). If you are processing based on legitimate interests you must also complete a legitimate interests assessment.

If you are processing data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, data concerning a person's sex life or sexual orientation or data relating to criminal convictions or offences, you will also need to state a further basis for that processing – you can find a list of these in GDPR Article 9 and 10.

The lawful basis for processing is Article 6(1)(a) – consent. The basis for processing special category data is Article 9(2)(a) – explicit consent.

1.6 Mandatory requirements

Guidance: Add the following requirements to your project backlog unless they do not apply (e.g. data need not be kept up to date in a system for storing old records). Section 4 can be used to check that these have been completed, particularly if delivery is not being managed as a project.

Data Accuracy

a) Data must be kept up to date
b) There must be means to validate the accuracy of any personal data collected
c) Inaccurate or incomplete personal data must be updated on receipt of a lawful request from the data subject

Retention & Deletion

d) All data collected will have a retention period
e) Data must be deleted at the end of its retention period

f) Personal data must be erased upon receipt of a lawful request from the data subject

<u>Information & Transparency</u>
g) The data subjects shall be provided with:
(i) The identity and contact details of the data controller;
(ii) The purposes of the processing, including the legal basis and legitimate interests pursued
(iii) Details of the categories of personal data collected
(iv) Details of the recipients of personal data

<u>Objection & Restriction</u>
h) There must be means to restrict the processing of data on receipt of a lawful request from the data subject
i) There must be means to stop the processing of data on receipt of a lawful request from the data subject

<u>Security</u>
j) Appropriate training and instructions will be put in place to enable staff to operate the new system / process securely
k) Identify an Information Asset Owner
l) Update the Information Asset Register

<u>Is the data being transferred outside the UK and EEA? If so:</u>
m) The data subjects must be provided with information on where to obtain details of any safeguards over data transferred to non-GDPR compliant countries
n) Consult the DPO for additional requirements to ensure the processing is GDPR compliant.

<u>Is the data being transferred to or through another organisation? If so:</u>
o) There must be controls to ensure or monitor compliance by external organisations.

<u>Is consent or pursuit of a contract the lawful basis for an automated processing operation? If so:</u>
p) There must be a means to extract and transmit the data in a structured, commonly used and machine-readable format on receipt of a lawful request from the data subject
q) The consent must be recorded in some manner to serve as evidence

<u>Does our Privacy Notice need to be updated? If so:</u>
r) *Update the Privacy Notice*

2. Data protection assessment screening

Guidance: The purpose of the screening questions is to determine if a DPIA is required. As a data controller we are required to perform DPIAs where the processing is likely to result in a high risk to the rights and freedoms of individuals (Article 35 refers).

2.1 Screening questions

ID	Criteria	Y/N
1	Will the processing involve evaluation or scoring, including profiling or predicting, especially in relation to an individual's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements?	N
2	Will the processing involve automated decision making that will have a legal or similar detrimental effect on individuals? For example, decisions that lead to exclusion or discrimination.	N
3	Will the processing involve the systematic monitoring of individuals in a publicly accessible area? For example, surveillance cameras in a shopping centre or train station.	N
4	Will the processing involve sensitive personal data or data of a highly personal nature? For example, special categories of data (Article 9 refers), personal data relating to criminal convictions or offences (Article 10 refers), and personal data linked to household and private activities.	Y
5	Does the processing involve large scale processing of data at a regional, national or supranational level, and which could affect a large number of data subjects?	N
6	Does the processing involve matching and combining two or more datasets that have been collected for different purposes and/or by different data controllers?	N
7	Does the processing concern vulnerable individuals who may be unable to easily give consent or object to the processing? For example, children, employees, and others who require special protection (mentally ill persons, asylum seekers, patients, the elderly).	N
8	Does the processing involve the innovative use or application of new technological or organisational solutions? For example, "Internet of Things" applications can have significant impacts on subjects' daily lives and privacy. Note: Screening question not considered to be met. Whilst	N

DRAFT

	facial geometry login for electronic devices is new to the ICO this is not a recent or new technological development in the world at large.	
9	Does the processing prevent individuals from exercising a rights or using a service or contract? For example, where a bank screens its customers again credit reference database in order to decide whether to offer them a loan.	N

Guidance: If you answer "Yes" to one or more questions you should complete a DPIA. If you answer "No" to all questions please proceed to section 6.

2.2 DPIA approach and consultation

Guidance: Record which parts of the DPIA you will be completing and your rationale (especially if your choices differ from the guidance above).

Explain what practical steps you will take to ensure that you identify and address the data protection risks. Include details of:

- *Who should be consulted, internally and externally? This must include the DPO's team and Cyber Security. You should also consult data subjects or their representatives unless this is not possible or appropriate – e.g. it would be disproportionate, impractical, undermine security or compromise commercial confidentiality.*
- *If data subjects (or their representatives) will not be consulted you must document the reasons for this.*
- *How you will carry out the consultation. You should link this to the relevant stages of your project management process or delivery plan.*

Consultation will take place with the DPO Team / Cyber Security as part of completing this DPIA. There has been some consultation with end users during the proof of concept stage to understand their general views about use of this technology at the ICO. End users are given an explanation and a choice during the MMD onboarding as to whether they wish to consent. Use of biometric user authentication is entirely optional.

3. Data inventory

3.1 Information flows

Guidance: Provide a systematic description of the processing, including:

- *Whether data collected is personal data*
- *The source of the data (including whether the data subjects are vulnerable, the relationship with the data subjects, the manner of collection and the level of control the data subjects have over the data once collected)*
- *The nature and context of the processing (including whether there are new technological developments or any relevant current issues of public concern)*
- *The scope of the processing (including the nature and volume of data, frequency and duration of processing, sensitivity of the data and the extent of the processing)*

- *The storage and transfer of the data (including details of hardware, software, networks, key people and details of any paper records or transmission channels)*
- *Responsibilities for the data (including the information asset owners, how responsibilities for information change through the data flow and the boundaries of responsibilities in any handover)*

You may find it useful to refer to a flow diagram or other way of explaining information flows. You should also say how many individuals are likely to be affected by the processing of personal data.

The graph of facial features and the users telephone number are collected directly from the data subject as part of the MMD onboarding process, after the project team have explained the functionality to the user and obtained their explicit consent.

End users are asked:

Based on the information above:

☐ **I agree** to the use of Windows Hello on the understanding that the image created is only held on the device provided to me and is not stored elsewhere and also that it is not used for any other purpose other than for accessing my device.

☐ **I do not** wish to use Windows Hello at this time

Name:

Signed ……..

Date ……

The biometric graph is encypted using strong cryptography and stored on the device only, this graph is only accessible through the Windows Hello framework which will return 'pass' or 'fail' for the authentication attempt. The biometric data is not accessible outside of this framework, it cannot be exported, uploaded or transferred.

User Biometric Graph can be updated by a user as required, after failed biometric login attempts, user is prompted to update biometric graph to improve accuracy.

DRAFT

The users telephone number is obtained and is provided to Microsoft for the sole purposes of user verification as part of multi-factor authentication (an enhanced security feature used as part of the PIN reset process).

3.2 Data inventory

Guidance: Identify the personal data to be held, the recipients (those with access to the data), the retention period and the necessity of the data collection, processing and retention.

Data Type	Recipients	Retention Period	Necessity
Encrypted graph of facial geometry	None – stored on device only	The facial geometry graph is updated when manually triggered by a user ("Improve Windows Hello Recognition"). Otherwise the facial geometry graph remains encrypted on the device until the user profile is removed or the device reaches the end of its usable life. Data can be wiped from the device by a factory reset by ICO IT staff	This is required for the Windows Hello Biometric framework to support facial login to Microsoft Surface Devices.
Telephone number	Microsoft	Held by Microsoft for the period the user requires access to the device. The user device data is deleted 90 days after ICO leaver process concluded. We can add legal holds and request Microsoft retain user data for longer periods if required.	Necessary for security of the device and the multi factor identification.

DRAFT

4. Compliance measures

Use this section to record your compliance with the requirements in section 1.5. Fill in the details of how the requirements have been met or list the requirement as N/A. The requirement source is a reference to GDPR unless otherwise stated.

Requirement	**Implementation Details**
Data Accuracy	
a) Data must be kept up to date	User can update information if significant change to facial geometry occurs. The user is prompted to update this in the event that sign in fails to improve accuracy of logins. User can update multi factor authentication from Microsoft security portal in Office 365.
b) There must be means to validate the accuracy of any personal data collected	Success or failure of the login process will validate the collection of the data and the user can update when necessary as detailed above.
c) Inaccurate or incomplete personal data must be updated on receipt of a lawful request from the data subject	User can update the information as required.
Retention & Deletion	
d) All data collected will have a retention period	Data is retained for the duration of the devices assignment to a user or until the device reaches the end of it's usable life ICO IT will carry out reset of device before any assignment to a new user or at end of life.
e) Data must be deleted at the end of its retention period	Data is stored on the device and is destroyed when the device is reset or the user profile is removed.
f) Personal data must be erased upon receipt of a lawful request from the data subject	User can be unenrolled from Windows Hello Facial Recognition but will require a device rebuild.
Information & Transparency	
g) The data subjects shall be provided with: ● the identity and contact details of the data controller; ● the contact details of the Data Protection Officer; ● the purposes of the processing, including the legal basis and legitimate interests pursued ● details of the categories of personal data collected ● details of the recipients of personal data	Information is provided to users during the device onboarding process and consent to the processing of biometric data is obtained from the user.
Objection & Restriction	
h) There must be means to restrict the processing of data on receipt of a lawful request from the data subject	User can opt out of Windows Hello facial recognition process
i) There must be means to stop the processing of data on receipt of a lawful request from the data subject	User can opt out of Windows Hello facial recognition process
Security	

DRAFT

j) Appropriate training and instructions will be put in place to enable staff to operate the new system / process securely	Information is provided to users during the device onboarding process, ICO staff are available during on-boarding to support the process. Microsoft Windows has detailed instructions to support the user during the process.
k) Identify an Information Asset Owner	Director of Digital, IT and Customer Services.
l) Update the Information Asset Register	Updated by Information Management and Compliance.
<u>Conditional Requirements</u>	
m) The data subjects must be provided with information on where to obtain details of any safeguards over data transferred to non-GDPR compliant countries	Data is not transferred, it does not leave the user's device.
n) Consult the DPO for additional requirements to ensure the processing is GDPR compliant.	DPO consulted as part of DPIA process.
o) There must be controls to ensure or monitor compliance by external organisations.	N/A
p) There must be a means to extract and transmit the data in a structured, commonly used and machine-readable format on receipt of a lawful request from the data subject	N/A.
q) The consent must be recorded in some manner to serve as evidence	Users sign consent declaration during the MMD onboarding process. Consent records are retained by the project team.
r) Update the Privacy Notice	Staff privacy notice to be updated to include information about MMD devices.

DRAFT

5. Data protection risk assessment

Guidance: Identify and assess the risks to subjects' rights, the actions you could take to reduce the risks and any future steps that will be necessary (eg the production of new guidance or security testing for new systems). Some example risk sources have been listed to aid you. This list is not comprehensive and will not necessarily apply to your system or process. See Appendix for guidance on assessing impact and probability.

Risks should be considered from the data subject's perspective not the ICO's (eg a reputational risk to the ICO should not be recorded here). Some example threats to consider include:

- *Discrimination*
- *Identity theft and fraud*
- *Financial loss*
- *Damage to data subjects' reputation*
- *Loss of confidentiality of professional secrets*
- *Unauthorised reversal of pseudonymisation*
- *Social or economic disadvantage*
- *Deprivation of legal rights or freedoms*
- *Data subjects losing control over their data*
- *Loss of privacy or intrusion into private life*
- *Prevention from accessing services*

Risk Details	**Impact**	**Probability**	**Response**
[Guidance: Describe risks to data subjects]	*[Guidance: Describe consequences to data subjects if risk realised]*	*[Guidance: Describe likelihood that risk will be realised]*	*[Guidance: Describe risk treatment (eg reduce, avoid, accept or transfer)]*
Device allows access to unauthorised third party due to false positive	*High – user device and documents are accessed*	*Very low – Less than 0.001% chance of occurrence.*	*Risk level Low and is accepted.*
Device may not process biometric details correctly and blocks access to the authorised user.	Low - User will be denied access to the device and will be prompted for a PIN in the first instance or an automated phone call to a number set at enrolment if a user cannot remember their PIN	Low – processing of facial biometric data is affected by lighting conditions and presence of glasses etc however in the event of failed login user has alternative means of access via pin	*Risk level Low and is accepted.*
Data Accuracy & Sufficiency	Low - User can update biometric	Low – User can improve data	*Risk level Low and is accepted.*

	data at any time and is prompted to do so in the event of a login failure.	accuracy at any time	
Illegitimate Access to Data – A rogue application or actor may be able to access and decrypt the biometric data stored on the device. This could potentially result in a recreation of a users face.		Very Low – MMD security layer prevents non-ICO approved applications from being installed on the device and identifies 'unusual' user behaviour. There are no known methods of achieving this outcome. There are no known methods of reversing the encryption without key.	
Unauthorised / Incorrect Modification – A rogue application or actor may be able to access, decrypt and modify the biometric data stored on the device.	High – *user device and documents are accessed*	Very Low – MMD security layer prevents non-ICO approved applications from being installed on the device and identifies 'unusual' user behaviour. There are no known methods of achieving this outcome. There are no known methods of reversing the encryption without key.	*Risk level Low and is accepted.*
Destruction or Loss of Data - The biometric data stored on the device may be lost or destroyed.	Low – User will be denied access to the device and will be prompted for a PIN in the first instance or an automated phone	Low – In the event of device loss, data is inaccessible due to encryption. ICO policies are to initiate a remote	*Risk level Low and is accepted.*

DRAFT

	call to a number set at enrolment if a user cannot remember their PIN	wipe on lost devices which would reset the device to factory fresh status.	

DRAFT

6. Residual risk and sign off

6.1 Residual risk

Guidance: Record details of the remaining risk. It is never possible to remove all risk so this section should not be omitted or blank. If the residual risk remains high (e.g. red on the traffic light scoring in the Appendix) then you will need to consult the ICO by following the process used by external organisations.

6.2 Necessity and proportionality

Guidance: If you answered "Yes" to one or more of the screening questions in Section 2.1 you should discuss the necessity and proportionality of the collection, processing and retention of this data here, weighing the impact on data subjects rights and freedoms against the benefits of the processing activity. You should also consider whether there are other reasonable ways to achieve the same result with less impact on data subjects. If you have not answered "Yes" to any of the screening questions in Section 2.1 you can leave this section blank.

6.3 DPO recommendations

Guidance: Record any recommendations from the DPO or their delegates and responses here. This serves as useful tool when reconsidering a rejected DPIA or in recording the justification if the organisation rejects the DPO's advice.

No	Recommendation	Project Team Response
1	[Record any changes recommended by the DPO here]	[Record the actions taken as a result of the recommendation]

6.4 Sign Off

Guidance: Send this to the DPSIA Committee to approve the privacy and security risks involved in the project, the solutions to be implemented and the residual risk.

Considered by	Date	Project Stage
DPIA Forum	20/02/2020	

DRAFT

7. Integrate the outcomes back into the plan

Guidance: Who is responsible for integrating the DPIA outcomes back into any project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any data protection concerns which may arise in the future?

Action to be taken	Date for completion	Responsibility for Action	Completed Date

Contact point(s) for future data protection concerns	

8. Change history

Guidance: To be completed by the person responsible for delivering the system, service or process (in a project this will be the project manager).

Version	Date	Author	Change description
v.0.1	07/02/2020	Neil Smithies	First Draft

9. Template Document control

Title	Data Protection Impact Assessment Template
Version	1.1
Status	Final release
Owner	DPSIA Committee
Release date	02/04/19
Review date	10/12/20

DRAFT

Appendix: Risk Assessment Criteria
The following criteria are aligned with our corporate risk assessment criteria.

Impact
Impact is the consequence of a risk to the rights and freedoms of individuals being realised. Factors to consider include the financial harm or emotional distress that can be expected to occur.

Impact	Scoring criteria
Very low (1)	No discernible impact on individuals.
Low (2)	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc).
Medium (3)	Individuals may encounter significant inconveniences, which they will overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc)
High (4)	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc).
Very high (5)	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Probability
Probability is the likelihood of a risk to the rights and freedoms of individuals being realised. Factors to consider include the expected frequency of occurrence, and the motivation and capability of threat sources (eg does the threat require insider knowledge and/or significant technical resources to exploit any vulnerability?).

Probability	Scoring criteria
Very low (1)	0-5% - extremely unlikely or improbable For example, the risk has not occurred before or is not expected to occur within the next three years.
Low (2)	6-20% - low but not improbable For example, the risk is expected to occur once a year.
Medium (3)	21-50% - fairly likely to occur For example, the risk is expected to occur several times a year.

DRAFT

High (4)	51-80% - more likely to occur than not For example, the risk is expected to occur once a month.
Very high (5)	81-100% - almost certainly will occur For example, the risk is expected to occur once a week.

Risk level

Risk level is a function of impact and probability, and is represented by a RAG rating.

Probability / Impact	Very low (1)	Low (2)	Medium (3)	High (4)	Very high (5)
Very high (5)	Amber (5)	Amber (10)	Red (15)	Red (20)	Red (25)
High (4)	Green (4)	Amber (8)	Amber (12)	Red (16)	Red (20)
Medium (3)	Green (3)	Amber (6)	Amber (9)	Amber (12)	Red (15)
Low (2)	Green (2)	Green (4)	Amber (6)	Amber (8)	Amber (10)
Very low (1)	Green (1)	Green (2)	Green (3)	Green (4)	Amber (5)

Risk acceptance criteria

These criteria are guidelines only, and any risk treatment decisions should be made on a case-by-case basis. For example, it may be prudent to reduce a low risk because of legal and regulatory requirements.

Risk level	Acceptance criteria
Low (Green)	Within this range risks can be routinely accepted.
Medium (Amber)	Within this range risks can occasionally be accepted but shall be kept under regular review.
High (Red)	Within this range risks shall not be accepted and immediate action is required to reduce, avoid or transfer the risk.

Appendix A – Windows Hello information & agreement provided to end users

'Maintaining and increasing our technical understanding of the environment we regulate goes hand in hand with our own use of technology in our services and working practices as we continue to invest in technology and skills the public would expect of a modern regulator.'

As part of your new device roll-out we are offering you the option to use Windows Hello facial recognition authentication as a quick, modern and more secure way to access your device. For this reason it is the ICO's preferred authentication method.

However, the use of Hello is not required for your device to work, you will have the option to log in using two factor authentication such as PIN and password. This will not restrict functionality, but will require you to log in to your applications each time.

We understand that you may have some questions about the use of biometric data, so the following information is intended to explain what happens when you use Windows Hello, and enable you to make an informed decision about whether you want to activate this.

In order to ensure we are GDPR compliant we will ask you to indicate your decision below, and this information will be retained to record your consent.

Should you change your mind you may remove this functionality yourself in a few simple steps, and can retract your consent at any time by emailing ithelp@ico.org.uk

Windows Hello, Biometrics and Privacy.

Windows Hello is the Microsoft Window's biometric login framework, its purpose is to provide a replacement for password based login, using your face, authentication certificates and your new device to log you into your device, software and network resources.

Windows Hello is a faster way of logging into your device and reduces the risk associated with compromised passwords.

DRAFT

When you first register with Windows Hello on your new Surface device, the webcam array uses your facial geometry to create a data representation of your face, this isn't a photograph but an encrypted graph based on the distances and depths of your facial features. This encrypted graph is stored on your device only.

When you log into your device, your facial geometry is used to unlock a user authentication certificate stored in the device's TPM chip (a secure enclave on your device's motherboard), which is used to unlock your device and authenticate you to your resources.

The data representation of your face is encrypted and stored on your Surface device only, it is not sent to Microsoft or stored anywhere else, it cannot be exported from the device and is used only for the purposes of user authentication by the Windows Hello framework. Applications may talk to the Windows Hello framework to verify your identity but the framework will only respond with pass or fail for the authentication attempt.

For more info, please refer to the following resources on the Microsoft site:

https://support.microsoft.com/en-gb/help/4468253/windows-hello-and-privacy-microsoft-privacy

https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview

https://docs.microsoft.com/en-gb/windows-hardware/design/device-experiences/windows-hello-face-authentication

Based on the information above:

☐ **I agree** to the use of Windows Hello on the understanding that the image created is only held on the device provided to me and is not stored elsewhere and also that it is not used for any other purpose other than for accessing my device.

☐ **I do not** wish to use Windows Hello at this time

Name:

Signed ……..

Date ……

Case reference

IC-203321-W1K8

Core Cloud Services – Exchange Online - PSIA

Privacy and security impact assessment (PSIA) template

PSIA for: Core Cloud Services – Exchange Online

1. Project overview

1.1 Summary

Project ID:	BD093
Project Title:	Core Cloud Services – Exchange online
Project Manager:	Paul Lee
Purpose and Aims: To move the email service, currently provided by infrastructure within ICO's core network, to Exchange Online within Office365. Exchange Online will provide all ICO email capabilities including mailboxes, calendars, email filtering and secure email.	

1.2 Scope

The Core cloud services project will deliver Office365 to ICO, which includes an email service. A privacy and security impact assessment (PSIA) has been undertaken that covers the underlying Office365 solution[1]. In addition to this, as each service within Office365 is activated a separate PSIA will be undertaken to review the unique additional issues that arise from its use.

The scope of this PSIA is those privacy and security issues that arise from the use of the Exchange Online component of Office365. This means the features of the Exchange Online application itself, as well as, data storage and transfer capabilities specific to email content.

The Exchange Online service relies on the privacy and security of the wider Office365 solution implemented by ICO. This is composed of the ICO core network, the secure network connection to Office365 and the Office365 platform implemented by Microsoft, along with all controls to maintain those services. The ICO has purchased the E5 SPE Office 365 subscription.

The term 'Email' includes all services run as a part of an email service including: simple messages, messages with attachments, tasks, reminders, calendar entries and invitation.

1.3 Document Structure

This document follows the ICO standard PSIA process which is designed as template to be used on small and large scale projects: Section 2 is a high level assessment of risks, which has been populated for completeness; the full risk assessment then follows in Section 3. Section 4

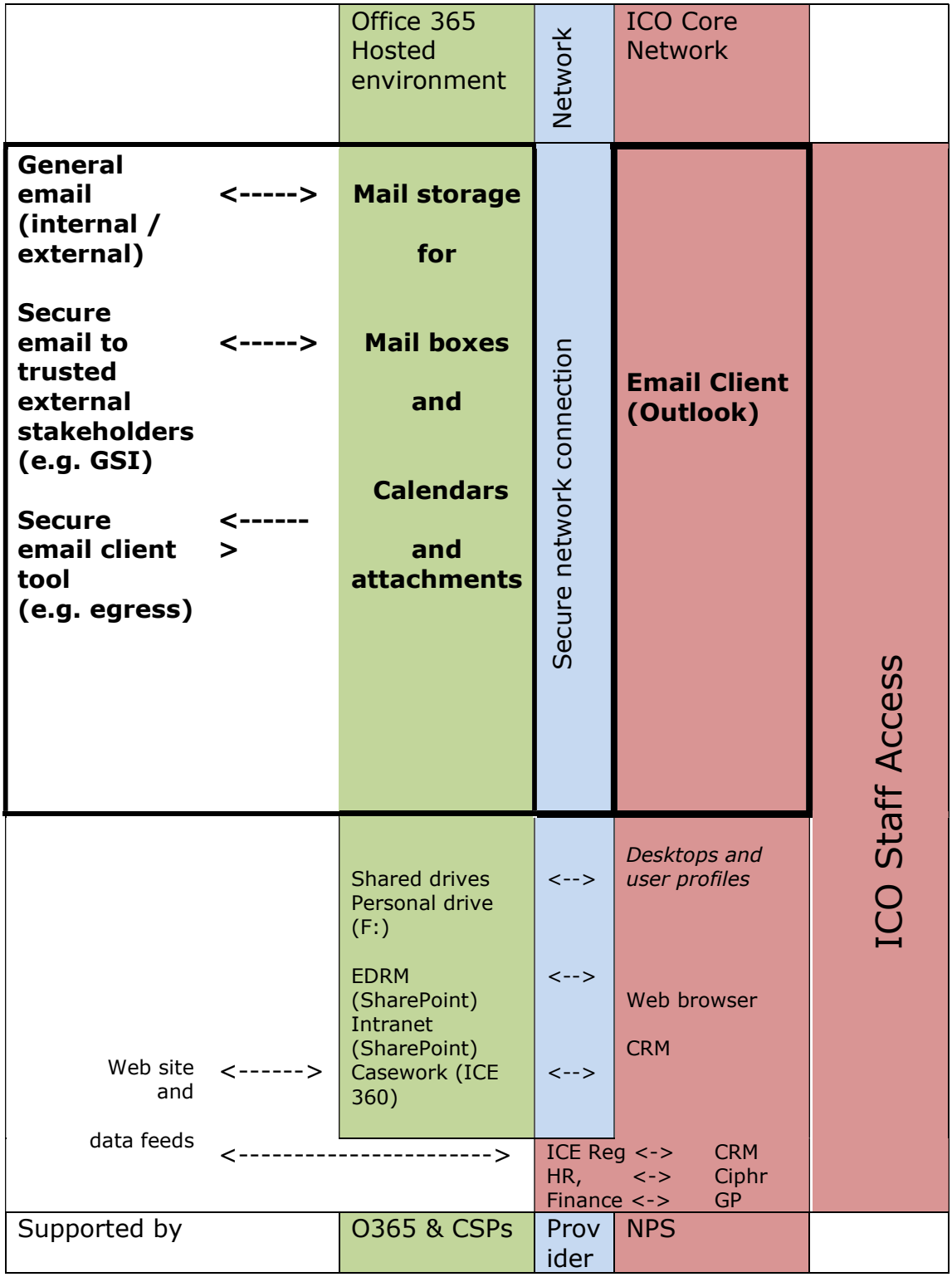
[1] PSIA – Office 365 – V2.0 which was approved by ICO change board on 17/1/2017

identifies solutions and mitigations of these risks, and Section 5 provides more in depth details of the controls to be put in place.

A Glossary is provided at the end of this document (Section 7) with many of the acronyms and a brief explanation of the technologies.

1.4 Proposed implementation and information flows

The following diagram shows the email service in its wider Office365 context and the elements covered by this PSIA are highlighted in bold. The service is accessed from the ICO core network using the familiar outlook desktop application, as it is now. The data and email capability are provided from Office365 and accessed using a secure network. The Office 365 hosted environment (is shown in green) and a new 'Secure WAN Network' (in blue) which provides the data transfers between Office 365 and the ICO Core network (in pink).


Office 365 Hosted environment
Network
ICO Core Network
General email (internal / external) <----->
Secure email to trusted external stakeholders (e.g. GSI) <----->
Secure email client tool (e.g. egress) <------>
Mail storage for Mail boxes and Calendars and attachments
Secure network connection
Email Client (Outlook)
ICO Staff Access
Shared drives Personal drive (F:) <-->
EDRM (SharePoint) Intranet (SharePoint) Casework (ICE 360) <-->
Desktops and user profiles
Web browser
CRM
Web site and data feeds <------>
<---------->
ICE Reg <-> CRM
HR, <-> Ciphr
Finance <-> GP
Supported by
O365 & CSPs
Provider
NPS

1.4.1 **Data in transit**

Security of data in transit is provided by a number of technologies depending on destination:

- The network connectivity between Exchange Online and the ICO user's desktop or other ICO application in the Core network is provided by the secure network connection (blue in the diagram above) and is discussed in the overarching PSIA.
- At the application level security is provided between Exchange online and Outlook using encrypted Secure Socket Layer (SSL) connection
- External connectivity to third party mail servers is provided by enforcing TLS 1.2 to known trusted partners, including those on the government's white list of trusted email domains; opportunistic TLS will also be available.
- Access by IOC Staff via webmail will not be permitted. (Although a later PSIA and HLD may address this)

1.4.2 **Data at rest and sovereignty**

ICO data will be held within the Office 365 environment and datacentres. Much of the security has been covered in the overarching PSIA. Microsoft commit to holding data within a particular region, within a region it may move or be spread across different data centres.

The ICO's Microsoft Tenancy is set to the UK region under which the current published locations of data for different services are as follows:

Exchange Online	- UK region
SharePoint Online	- UK region
Azure Active Directory	- Ireland
Skype for Business	- Ireland
Others	- Europe and US

Data at rest is encrypted; access will be tightly restricted and controlled. Azure Rights Management will be used to provide granular restriction depending on the classification of the data and sender/recipient.

Rights Management could be seen as intrusive by a small number of ICO stakeholders. ICO would make clear the Privacy and Security implications and benefits and offer choice so that where requested, Rights Management would only apply within the ICO's email domain.

1.5 Secure email

ICO will use the functionality provided by Exchange Online where ever possible, provided the security and functionality are adequate. Where this is not the case additional products will be brought in to supplement the functionality.

For secure email, TLS, then Azure Rights Management are the preferred approach. However, there may be circumstances, most likely when emailing small organisations or individuals, where Azure Rights Management imposes a requirement to use Microsoft office products to

open or respond, which may not be available to that individual. It is likely in these circumstances that a third party product will be used, similar to Egress which is already in use within the ICO and was seen as an interim measure until Exchange Online was implemented. The use of a third party product will be subject to a separate project with its own PSIA and HLD or as an update and new release of the overall Exchange Online documents.

1.6 Guidance sought and consultations

In understanding how Office 365 should be implemented to hold Official information, guidance from CESG/NCSC and Microsoft will be followed.

For more in depth information on the Government's 'Cloud first' strategy and best practice, the latest Government Digital Service (GDS) and Common Technology Services (CTS) guidance has been followed. We are a part of this community, receiving updates which include: the blue print for moving email from PSN and how to configure email in Office 365; registering as a government domain, this builds the new Email trust model when PSN and GSi end.

In considering how best to risk assess the services in this PSIA the current Government stance on security risk assessment has been considered and the 14 Cloud security principles have been used.

Our external IT security advisors, Auriga Consulting[2], have reviewed our overarching High Level Designs (HLD) and PSIA, and will be reviewing those for Email and SharePoint.

ICO is in discussion with the UK Microsoft Office 365 team who are providing guidance on Tenancy and licensing options as well as specific advice of configuration and migration to Exchange Online through the 'Fast track' team and potentially the MS partnership network.

Finally, there will be follow up activities to ensure that this service is maintained so as to preserve security at all times. And that the overall Office 365 environment can be accreditable as a part of ICO's overall IT environment.

[2] Auriga Consulting has undertaken a number of security reviews for the ICO.

2. Initial assessment

The purpose of the initial assessment is to determine the project's risk profile and decide whether further assessment is required to identify, assess and manage risks. For smaller projects the risk assessment may be sufficiently covered in this section.

2.1 Privacy questions

ID	Screening question	Yes/No
1.	Will the project involve the collection of new information about individuals?	N
	Comments: Project doesn't involve collecting new personal data.	
2.	Will the project compel individuals to provide information about themselves?	N
	Comments: The service will provide a mailbox from which email can be sent and received and calendar entries added. The personal information stored within it is within a user's control.	
3.	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	Y
	Comments: Personal data may be accessible by provider for purposes of service provision and maintenance.	
4.	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	N
	Comments: Project doesn't involve processing data for new purposes.	
5.	Does the project involve using new technology which might be perceived as being privacy intruding for example biometrics or facial recognition?	N
	Comments: Project doesn't involve new technology. It aims to be transparent to ICO users of our outlook client software.	
6.	Will the project result in you making decisions or taking action against individuals in ways which could have a significant impact on them?	N
	Comments: Project will reproduce all the capabilities of the existing email service	

7.	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example health records, criminal records, or other information that people are likely to consider as private?	Y
	Comments: OFFICIAL information, including sensitive personal data, will be stored and processed in the cloud. Stakeholders will need assurances the privacy of their data is protected.	
8.	Will the project require you to contact individuals in ways which they may find intrusive?	Y
	Comments: Project doesn't involve changing how we contact individuals. Rights Management could be seen as intrusive by some. ICO would make clear the Privacy and Security implications and benefits and offer choice.	

If you answer "Yes" to **one or more** of the privacy questions go to step 3 and complete the further assessment.

If you answer "No" to **all** of the privacy questions go to step 5 for sign off.

2.2 Security questions

ID	Screening question	Yes/No
1.	Will the service involve the processing and storage of large volumes (eg more than 100,000) of hardcopy and/or digital records?	Y
	Comments: The service will include all ICO email and calendars.	
2.	Will the service involve the processing and storage of very sensitive hardcopy and/or digital information classified above OFFICIAL?	N
	Comments: OFFICIAL information only (including the SENSITIVE handling caveat).	
3.	Will the service involve the addition of multiple components to the core network (eg hardware, software, etc.)?	N
	Comments: The service only utilises the hardware and software components already implemented in ICO core network and as part of the underlying Office365 solution.	
4.	Will the service be delivered by multiple suppliers?	Y

	Comments: Microsoft will be sole supplier of Office 365, on top of this will be support partners who will provide configuration, administration and support. Other suppliers may provide additional services to run alongside Office 365 were additional functionality is required	
5.	Will the service be externally hosted with multiple external connections to suppliers?	Y
	Comments: Cloud service with a small number of external connections for routine business operations.	
6.	Will the service involve the processing and storage of hardcopy records and digital storage media outside our secure premises?	N
	Comments: No storage of ICO physical assets off premises.	
7.	Can we rely on the security provided by a commercial product or service? Please note, we will still need confidence the commercial product or service fully meets our business needs (eg commercial contract).	N
	Comments: We can rely on the security of the underlying Office 365 platform but decisions must be made about how we tailor the security controls (eg identity management) to our specific needs.	
8.	Can we apply a common solution to solve a common problem? Please note, we will still need confidence the common solution fully meets our business needs (eg is there a unique asset or threat not covered by the solution?). Examples of common solutions include: • Cloud security principles • Browser security guidance • Application development guidance • End user security guidance • Solutions provided by the digital marketplace	Y
	Comments: Office 365 services provide security controls that meet all of the government's 14 Cloud Security Principles. Implementing and configuring these controls in line with government guidelines is sufficient to protect OFFICIAL information without conducting a full risk assessment to specify appropriate security controls.	

If you answer "Yes" to **any** of security questions one to six go to step 3 and complete the further assessment.

If you answer "No" to **both** security questions seven to eight go to step 3 and complete the further assessment.

If you answer "No" to **all** of security questions one to six; and, "Yes" to **one** of security questions seven to eight go to step 5 for sign off.

3. Further assessment

Identification of key privacy and security risks.

3.1 Identify the privacy risks

Many privacy issues are common to all services on the Office 365 platform. These have been addressed in the PSIA for the Office365 platform and are not repeated here.

Below are the residual privacy issue from the addition of the Exchange Online service that is addressed as part of this PSIA.

Privacy issue	Risk to individuals	Compliance risk	Corporate risk
Collection and use Collection and use of data is unfair and unlawful.	Covered within the Overarching PSIA for the Office 365 (DPA principles 1 and 2)		
Data quality Collection, use and retention of poor quality data.	Covered within the Overarching PSIA for the Office 365 (DPA principles 3, 4 and 5)		
Individual rights Data processed without regard for statutory rights.	Covered within the Overarching PSIA for the Office 365 (DPA principle 6))		
Data security Confidentiality, integrity and availability of data compromised.	Adverse impact to individuals' privacy.	Breach of legal and regulatory responsibilities (eg principles 7 of DPA).	Reputational damage and fines.
Overseas transfers Data transferred to jurisdiction that doesn't adequately protect statutory rights and freedoms.	Covered within the Overarching PSIA for the Office 365 UK hosted (DPA principle 8)		

3.2 Identify the security risks

Many security issues, together with their risks and solutions, are common to all services on the Office365 platform. Where such issues have already been identified and treated as part of the PSIA for the underlying Office365 platform, they are not repeated here. Of the 14 cloud security principles, 5 have specific area requiring assessment and 9 are covered under the overall Office365 solution. These 9 are:

3. separation between consumers
4. governance framework
6. personnel security
7. secure development

8. supply chain security
10. identify and authentication
11. external interface protection
12. secure service administration
14. secure use of the service by the consumer

The table below identifies the security issues related to the use of Exchange Online.

Security issue	Risk to information	Compliance risk	Corporate risk
Taken from the CESG 14 Cloud Security Principles			
Data protection in-transit Consumer data transiting networks should be adequately protected against tampering and eavesdropping via a combination of network protection and encryption.	If this principle is not implemented, then the integrity or confidentiality of the data may be compromised whilst in transit.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.
Asset protection and resilience Consumer data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.	If this principle is not implemented, inappropriately protected consumer data could be compromised.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.
Operational security The service provider should have processes and procedures in place to ensure the operational security of the service.	If this principle is not implemented, the service can't be operated and managed securely in order to impede, detect or prevent attacks against it.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.
Secure consumer management Consumers should be provided with the tools required to help them securely manage their service.	If this principle is not implemented, unauthorised people may be able to access and alter consumers' resources, applications and data.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.

Audit information provision to consumers Consumers should be provided with the audit records they need to monitor access to their service and the data held within it.	If this principle is not implemented, consumers will not be able to detect and respond to inappropriate or malicious use of their service or data within reasonable timescales.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.

4. Identify solutions

The requirements of the DPA and GDPR have been used as the basis to assess privacy.

The key change this project brings is to have data hosted externally rather than in ICO's Core network. This project will not add any new categories of personal data or introduce processing of data for new purposes. Any new usage would be under a separate project with its own PSIA.

The hosting within Office 365 provides many features to secure the data, some are common across the Office 365 environment and are documented in the Overarching PSIA.. There are a smaller number that relate specifically to email that are covered in this document.

4.1 Privacy solutions

Risk	Solution(s)	Result	Compliant and Proportionate?
Data Security Confidentiality, integrity and availability of data compromised.	Implement solutions identified in Office 365 PSIA to secure the common environment in which sit and is transmitted to and from the Core Network. Implement email to best practice guidance from CTS. To ensure data in transit is secure, and guarantee non repudiation. Azure rights management (ARM) provides file level encryption, prevention of data loss through forwarding and printing rules.	Treated	Yes Yes Yes Azure Rights Management is a proportionate with a good level of granularity providing additional protection from data loss or unauthorised access to information. The use of ARM with in emails outside ICO's environment will be carefully considered, with a range of options available.

4.2 Security solutions

Note in the table below the Source of information in the Solution column is identified by the following bullet heading:
M – Microsoft,
C – CESG/NCSC,

I – ICO
G – GDS/CTS

Risk	Solution(s)	Result	Compliant and Proportionate?
Data protection in-transit If this principle is not implemented, then the integrity or confidentiality of the data may be compromised whilst in transit.	M All email clients transfer email data over a secure session using SSL/TLS, securing the data in transit. M Secure TLS encrypted tunnels allow for private email traffic to pass between ICO and trusted external parties. M The secure email capability within outlook/exchange can be used to allow an outlook user to identify any email as sensitive and enforce its encryption. The email will remain encrypted until decrypted by the recipient. I Implement transport rules to detect traffic that can utilise secure site to site TLS encryption. G Follow CTS guidance on setting up email services securely.	Treated	Yes. All solutions are required for ICO email access to be implemented to maintain the Official status. The solutions ensure all traffic between an ICO email user and Exchange Online is encrypted. Options exist for all scenarios requiring secure data traffic to trusted partners, government departments, other organisations or stakeholders. And to provide secure transmission as far as possible through the email servers to the public.
Asset protection and resilience If this principle is not implemented, inappropriately protected consumer data could be compromised.	M Microsoft provides the Exchange Online email capability from UK region data centres. M Azure rights management allows files/emails to be individually encrypted at rest with processing rules to further restrict what can be done with each email e.g. forwarding, printing. M There are multiple access routes to Exchange Online. The use of Outlook Web Access (OWA) will be disabled.	Treated	Yes The use of UK data centres in line with government advice. Encryption of Office 365 storage, plus separate encryption of each individual file/email, is required to provide an on-premise equivalent level of privacy/control. Disabling of access to webmail capabilities allows controls equivalent to the current on-premise solutions.

Operational security If this principle is not implemented, the service can't be operated and managed securely in order to impede, detect or prevent attacks against it.	M Configuration, change management, incident response and protective monitoring are all demonstrated in Microsoft's compliance with the ISO-27001 information security standard. I Email filtering and scanning can be implemented to provide anti-virus, anti-spam, anti-malware capabilities. C CESG guidance on implementing Office 365 at Official. G GDS/CTS guidance on implementing Exchange Online services, including DMARC, SPF and DKIM. I ICO security and compliance questionnaires for all third parties providing parts of this service.	Treated	Yes It is justified that ICO follow all best practice solution and government issued guidance. Office 365 Exchange Online Advanced Threat Protection (ATP) will be enabled to provide email filtering, anti-virus and logging.
Secure consumer management If this principle is not implemented, unauthorised people may be able to access and alter consumers' resources, applications and data.	I All access to be granted on principal of least access rights. M ICO retains direct control over which user accounts can perform authorised administrative functions on the service. This is accomplished by federating the customer's on premise active directory. M The separation and access control within management interfaces is subjected to independent penetration testing. I Production and test/UAT environments separated through use of vlans, AD, Azure Rights Management. I ICO security and compliance questionnaires for all third parties providing parts of this email service.	Treated	Yes All solutions are necessary to maintain security compliant with email data at OFFICIAL.

Audit information provision to consumers If this principle is not implemented, consumers will not be able to detect and respond to inappropriate or malicious use of their service or data within reasonable timescales.	M Microsoft's services provide enhanced capabilities, allowing customers to audit and delegate end-user access within the service offering (details available in service descriptions).	Treated	Yes ICO to ensure the solution provides a proportional level of audit logging. This is integrated as far a possible in to existing monitoring and reporting systems.

5. Sign off and record the outcomes

Who has approved the privacy and security risks involved in the project? What solutions do you need to implement?

You should record sign-off if the initial assessment does not identify any significant risks, and further assessment is not required.

5.1 Privacy solutions

Risk	Solution	Approved by
Collection and use Collection and use of data is unfair and unlawful.	Current mitigation adequate.	
Data quality Collection, use and retention of poor quality data.	Current mitigation adequate.	
Individual rights Data processed without regard for statutory rights.	Current mitigation adequate.	
Data security Confidentiality, integrity and availability of data compromised.	The email service will be built on the existing control identified in the overarching PSIA for use of Office 365. Implement Azure Rights Management, DMARC, SPF, DKIM and, TLS . Configure to provide control of individual emails from data loss, unauthorised access and to provide auditable logging of access.	
Overseas transfers Data transferred to jurisdiction that doesn't adequately protect statutory rights and freedoms.	Current mitigation adequate.	

5.2 Security solutions

Risk	Solution	Approved by
Data protection in-transit If this principle is not implemented, then the integrity or confidentiality of the data may be compromised whilst in transit.	Secure protocols running over a secure network between know endpoints. Wherever possible implement site to site trusts with automated TLS encryption.	

Asset protection and resilience If this principle is not implemented, inappropriately protected consumer data could be compromised.	Use UK data centres for storage of all email content. Implement Azure rights management, configure encryption of individual emails. Disable outlook webmail access.	
Separation between consumers	Current mitigation, including those in overarching build of Office 365, adequate.	
Governance framework	Current mitigation, including those in overarching build of Office 365, adequate.	
Operational security If this principle is not implemented, the service can't be operated and managed securely in order to impede, detect or prevent attacks against it.	ICO to implement anti-virus and email filtering services using Exchange Online Advanced Threat Protection (ATP). ICO to ensure that all CESG (NCSC) / CTS guidance has been followed on implementing Exchange Online services, including DMARC, SPF and DKIM. ICO to assess any third party supplying a part of this service using the supplier security questionnaire ICO to ensure ongoing compliance by regular check and reviews, including IT health checks All ICO controlled servers and Office365 services to be appropriately patched and protected from virus and spam.	
Personnel security	Current mitigation, including those in overarching build of Office 365, adequate.	
Secure development	Current mitigation, including those in overarching build of Office 365, adequate.	
Supply chain security	Current mitigation, including those in overarching build of Office 365, adequate.	

Secure consumer management If this principle is not implemented, unauthorised people may be able to access and alter consumers' resources, applications and data.	ICO to implement restricted admin access in line with current on-premise solutions. Including implementation of Office365 lockbox. ICO to ensure separation of environments and ongoing compliance by regular check and reviews, including IT health checks.	
Identify and authentication	Current mitigation, including those in overarching build of Office 365, adequate.	
External interface protection	Current mitigation, including those in overarching build of Office 365, adequate.	
Secure service administration	Current mitigation, including those in overarching build of Office 365, adequate.	
Audit information provision to consumers If this principle is not implemented, consumers will not be able to detect and respond to inappropriate or malicious use of their service or data within reasonable timescales.	Use Azure Rights Management to restrict and log access. Enable logging where available in Office 365. Configure logging information to pass to ICO centralised logging and reporting function.	
Secure use of the service by the consumer	Current mitigation, including those in overarching build of Office 365, adequate.	

6. Integrate the outcomes back into the project plan

Action to be taken	Date for completion	Responsibility for Action
All technical solutions identified in section 5 to be added to appropriate project backlogs	Upon PSIA sign-off	Paul Lee
IT Health Check on new environment to be scoped and arranged by IT assurance team	Before live emails are stored in Exchange Online	John Rackstraw

Contact point(s) for future privacy concerns	Steven Rook, Helen Ward
Contact point(s) for future security concerns	Steven Rook, David Wells

7. Glossary

Azure Rights Management Azure/Advanced Information Protection	Microsoft has renamed a number of it security components as at Dec 2016: Azure Information Protection (also referred to as Advanced Information Protection in some documentation) provides classification, labelling, and protection for an organization's documents and emails. The protection technology uses the Azure Rights Management service; now a component of Azure Information Protection.
CESG/NCSC	National Cyber Security Centre. The NCSC acts as a bridge between industry and government, providing a unified source of advice, guidance and support on cyber security
DPA GDPR	Data Protection Act General Data Protection Regulation
DMARC SPF DKIM	Domain based Message Authentication, Reporting and Conformance (DMARC) works with Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM) to authenticate mail senders and ensure that destination email systems trust message sent from the origination domain.
Egress	A secure email service provides by Egress. Currently in use by ICO to provide secure email to and from stakeholders where no existing secure means of transfer exist – it is used for emails external to GSi/PSN.
GDS CTS	Government Digital Service (GDS) Common Technology Services (CTS)
GPG13	Protective Monitoring for HMG ICT Systems
GSI / PSN	ICO's ISP providing email as in user@ico.GSI.gov.uk. This is a centrally provided government service providing a secure means of exchanging email at Official. This service ends in Mar 2017. Government Digital Service (GDS) have developed a blue print for each organisation to follow to configure their email services. This includes mandating TLS 1.2 and a number of other security features
IT Health Check ITHC IT Security Audit	Guidance from Government on operation of IT systems is to have regular security audits. These are known as IT Health Checks and should be carried out by suitably trained and accredited people. For central government the CHECK scheme, run by NCSC, provides the necessary level of assurance. The ITHC aims to provide assurance that the external systems are protected from un-authorised access or

	change, and they do not provide an un-authorised entry point into other linked Government IT systems such as PSN services. The internal systems should be tested to provide further assurance that no significant weaknesses exist on network infrastructure or individual systems that could allow one internal device to intentionally or unintentionally impact on the security of another. ICO's policy is to conduct an ITHC for significant new applications and infrastructure prior to use. And to conduct an annual ITHC with a scope taking a risk based approach favouring changes in the year, evidence of good housekeeping, and externally facing components.
Lock box	An Office 365 security feature providing an additional level of encryption of data at rest. The keys to this encryption although stored within Office 365 are only accessible by authorisation requests controlled by the ICO and are not available to Microsoft.
MS Express Route	Connections to Office 365 can be across the Internet or over a dedicated link (Express Route) see also MPLS
OWA	Outlook Web Access. Means of accessing emails held on Exchange Online over the internet. Also referred to as web mail access.
TLS SSL/TLS	Transport Layer Security Industry wider security protocol for securing connections. TLS 1.2 is the most current version.

8. Document control

Version	Date	Author	Change
V0.1	01/12/16	Paul Lee	Initial Assessment
V0.2	29/01/17	David Wells	Update to reflect overarching PSIA, and HLD

Template used

Title	Privacy and Security Impact Assessment Template
Version	1.0
Status	Released
Owner	Information Security Manager

Approved by	Information Governance Steering Group
Release date	August 2016
Review date	March 2017

Case reference

IC-203321-W1K8

Core Cloud Services – Office 365 - PSIA

Privacy and Security Impact Assessment for: Core Cloud Services – Office 365

1. Project overview

1.1 Summary

Project ID:	BD093
Project Title:	Core Cloud Services – Office 365
Project Manager:	Paul Lee
Purpose and Aims: To move services, currently provided within ICO's core network, to have these provided externally as a hosted service using Office 365. To include: Email and Calendars, EDRM, Casework, shared folders and personal F: drives, any Business Intelligence systems using this data, Email filtering and secure email, and allow for presence and functionality to support Unified Communications.	

1.2 Scope

This Privacy and Security Impact Assessment (PSIA) covers the entire hosted Office 365 environment and the secure connectivity which links to the ICO's Core network.

For this project; although the data and personal information is unchanged and the purpose we process it for remains unchanged it is the manner in which we hold it that will be significantly different.

If the planning, design, configuration and ongoing management of the ICO's use of Office 365 is not done properly, then there is a significant risk to the privacy of our customers and stakeholders which is not present in our existing isolated Core network model.

This risk assessment focuses on the overarching Office 365 environment and infrastructure. Separate PSIAs will be produced for each application as these have different specific privacy and security requirements, with controls specifically aligned to each application and mode of usage. There will be PSIAs for Email, SharePoint, EDRM, ICE360, BI and Unified Communication.

1.2.1 Document Structure

This document follows the ICO standard PSIA process which is designed as template to be used on small and large scale projects: Section 2 is a high level assessment of risks, which has been populated for completeness; the full risk assessment then follows in Section 3. Section 4 identifies solutions and mitigations of these risks, and Section 5 provides more in depth details of the controls to be put in place.

A Glossary is provided at the end of this document (Section 7) with many of the acronyms and a brief explanation of the technologies.

1.3 Description of the information flows

1.3.1 Accreditation boundaries

In considering the ICO's IT as a whole there are areas where ICO relies on the security and accreditation of others, but for the Core network it must provide its own security and assurance. ICO makes use of the Government wide PSN/GSI service for Email and WAN, ICO relies on the security and accreditation of these services. ICO has a contract with a Managed Service provider Northgate Public Services (NPS) to help maintain systems, it relies on the security of their services and the accreditation they have. ICO reports annually to the Cabinet Office on the security of its IT and as a condition of connecting to PSN must meet an annual accreditation process. This accreditation requires a regular IT Health Check and for ICO systems to be well maintained, monitored and patched to the latest levels.

In looking to move the data that the ICO is responsible for out from the Core network there is a question of how we maintain the assurance that our data is save, systems are well managed and that all relevant legislation and good practice is followed. We will need to rely on the service provided by others, and to check on their accreditations for the environment as a whole. For Office 365 there are many options available which can increase the security of the environment which falls directly under ICO's control. ICO will look to rely on the overall accreditation of the Office 365 environment but must probe in more detail in to its own environment within the global Office 365 environment ("Tenancy" in Office 365 terms), and look to how it is configured and maintained.

Office 365 provides a range of services, and a range of security products through different licensing options. ICO intends to use E5 licenses rather than E3 as there are many additional security features available in E5[1].

The ICO's web site is an entirely separate environment, it holds publicly available information, but is outside the scope of this PSIA.

To protect all ICO data and IT systems then everyone involved; third party, managed service provider, every contract, ICO IT and ICO Users at all times must operate to support the Official level.

---

[1] Additional functionality in E5 includes:
Document and email control - Rights Management Services enables you to restrict access to documents and email to specific people and to prevent anyone else from viewing or editing them, even if they are sent outside the organization

Advanced Information Protection - Data loss prevention and encryption across Exchange Online, Skype for Business and SharePoint Online help keep your content safe in email, Instant Messaging and meetings, and team sites.

Advanced security - Advanced Threat Protection helps defend users against sophisticated threats hidden in emails, attachments, and links. Customer Lockbox lets you limit data access to only pre-assigned, two-factor-authenticated administrator approvals for greater control and transparency. And the built-in features of Office 365 Advanced Security Management give you enhanced visibility and control of your Office 365 environment

1.3.2 Proposed implementation

The following diagrams show the information flows and the scope of the data at rest which comprises emails, case documentation, general documents held in the EDRM system, and data held locally in C:/ and F:/ drives.

Diagram 1.3.3 shows the existing ICO Core network, while diagram 1.3.4 shows how ICO data is expected to sit within the proposed Office 365 hosted environment (in green) and a new 'Secure WAN Network' (in blue) which provides the data transfers between Office 365 and the ICO Core network.

1.3.3 Existing ICO Core network data flows

External data		Data is held in ICO Core Network		Accessed using	
External stakeholders email	<------>	Mail storage for Mail boxes and Calendars	<-->	Email Client (Outlook)	ICO Staff Access
GSI users Secure email	<------>				
Secure email product	<------> Egress or another product				
				Desktops and user profiles	
		EDRM (SharePoint) Intranet (SharePoint)	<-->	Web browser	
		Casework (ICE 360)	<-->	CRM	
		Shared drives Personal drive (F:)	<-->	Word/ Excel	
Web site and data feeds	<------> <------>	ICE registration Nuisance calls	<-->	CRM	
		HR, Finance	<--> <-->	Ciphr GP	
		Supported by (NPS and subcontractors)			

1.3.4 Extending the scope for Official Information using Office 365

External data		Office 365 Hosted environment	Secure WAN Network	ICO Core Network	
External stakeholders email	<----->	Mail storage for Mail boxes and Calendars			ICO Staff Access
GSI users Secure email	<-----> new gov trust model		<-->	Email Client (Outlook)	
Secure email product	<-----> Egress or another product			Unified Comms (presence and Skype for business)	
				Desktops and user profiles	
		EDRM (SharePoint)	<-->	Web browser	
		Intranet (SharePoint)			
		Casework (ICE 360)	<-->	CRM	
		Shared drives Personal drive (F:)	<-->	Word/ Excel	
Web site and data feeds	<----------> <---------->			ICE Reg <-> CRM Nuisance calls <-> HR, Finance <-> Ciphr GP	
Supported by		Microsoft & CSPs	WAN provider	(NPS and subcontractors)	

1.3.5 Data in transit (Secure WAN Network)

In moving ICO data out of the Core network there is a requirement for a suitable network connection to provide reliable and resilient access but above all else to provide a secure connection. This will be in constant use for every day to day interaction with data: to retrieve an Email, run a report, open a case file, update a spreadsheet or document and read or print.

The security and accreditation of this network connection must enable ICO to be confident that the Secure Network is suitable for handling data at Official. Access to the ICO Office 365 Tenancy, and our data held in it, will only be possible over this secure network locked to ICO locations, direct access from the Internet, by-passing this connection, will not be possible.

Security of data in transit is provided by a number of cumulative technologies:

- The security of the application data. (For Email this is between Outlook and Exchange and is provided by encrypted Secure Socket Layer (SSL) connection)
- Office 365 offers connectivity over open internet and through an additional service called 'Express Route'. ICO intends to use Express Route and lock the connection between ICO's Core network and the ICO Office 365 Tenancy
- ICO has recently let a contract, through a Government framework, to supply a suitably secure network for both the interconnection of Regional Offices and for access to Office 365 and other ICO Cloud hosted service such as Unified Communications

The data on the ICO to Office 365 connection at all times passes over a network which ICO has specific contracts for; these are the MPLS network contract and Office 365 Express Route purchased as part of Office 365. The ICO has processes for checking on the overall suitability of suppliers as part of the procurement and ongoing management of the supply chain.

1.3.6 Data at rest and sovereignty

ICO data will be held within the Office 365 environment and datacentres. Microsoft commit to holding data within a particular region, within a region it may move or be spread across different data centres.

ICO will contract with Microsoft to use the UK region. It should be noted that not all Office 365 services are available from the UK region in which case data is stored in other regions. The current published locations of data for different services are as follows:

Exchange online	- UK region
SharePoint online	- UK region
Azure Active Directory	- Ireland
Skype for Business	- Ireland
Others	- Europe and US

All ICO's Emails will be held in Exchange online and all EDRM documents and casework documents in SharePoint online which will be physically held in UK data centres. Data at rest is encrypted, access can be tightly restricted and controlled.

1.3.7 Additional security features of Office 365

Office 365 has a number of security components, whose names have evolved and changed over time. Some specific products relate to email under the 'Advanced Threat Protection' banner and others to the access rights to documents at rest or when distributed more widely, generally termed Rights Management.

The more detailed PSIAs for Email and SharePoint will explore these requirements further and how the Office 365 products need to be configured to provide the level of protection and control ICO requires.

1.4 Guidance sought and consultations

In researching and planning a move to the Cloud, ICO's Internal Auditors, Grant Thornton, have provided advice and participated in workshops, the end deliverable of which was the IT Plan. This plan was signed off by IT Steering Group and SMT.

In considering the use of Office 365, and in particular information rights issues, the views of Dr Simon Rice of the ICO Technology team have been sought.

In understanding how Office 365 should be implemented to hold Official information, guidance from National Cyber Security Centre (NCSC) / CESG and Microsoft will be followed.

For more in depth information on the Government's 'Cloud first' strategy and best practice, the latest Government Digital Service (GDS) and Common Technology Services (CTS) guidance has been followed. We are a part of this community, receiving updates which include: the blue print for moving email from PSN and how to configure email in Office 365; registering as a government domain, this builds the new Email trust model when PSN and GSi end; and the creation of a pan Government DNS service which ICO will make use of.

In considering how best to risk assess Office 365 in this PSIA the current Government stance on security risk assessments, the 14 Cloud security principles and seeking Security Assurance have all been used.

Our external IT security advisors, Auriga Consulting[2], have been engaged to review our High Level Designs (HLD) and PSIA including this overarching PSIA and associated HLD, and will be reviewing those for Email and SharePoint.

[2] Auriga Consulting has undertaken a number of security reviews for the ICO.

ICO is in discussion with the UK Microsoft Office 365 team who are providing guidance on Tenancy and licensing options as well as specific advice of configuration of SharePoint online. ICO has Access to the dedicated 'Fast track' team within Microsoft to assist with Migration.

Finally, there will be follow up activities to ensure that the Office 365 environment has been built and is being maintained so as to maintain security at all times. This will ensure that the Office 365 environment can be accredited as a part of ICO's overall IT environment.

2. Initial assessment

The purpose of the initial assessment is to determine the project's risk profile and decide whether further assessment is required to identify, assess and manage risks. For smaller projects the risk assessment may be sufficiently covered in this section.

2.1 Privacy questions

ID	Screening question	Yes/No
1.	Will the project involve the collection of new information about individuals?	N
	Comments: Project doesn't involve collecting new personal data.	
2.	Will the project compel individuals to provide information about themselves?	N
	Comments: Project doesn't involve compelling individuals to provide personal data.	
3.	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	Y
	Comments: Personal data may be accessible by provider for purposes of service provision and maintenance.	
4.	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	N
	Comments: Project doesn't involve processing data for new purposes.	
5.	Does the project involve using new technology which might be perceived as being privacy intruding for example biometrics or facial recognition?	N
	Comments: Project doesn't involve new technology.	

6.	Will the project result in you making decisions or taking action against individuals in ways which could have a significant impact on them?	N
	Comments: Project doesn't involve making decisions about individuals that could have a significant impact on them.	
7.	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example health records, criminal records, or other information that people are likely to consider as private?	Y
	Comments: OFFICIAL information, including sensitive personal data, will be stored and processed in the cloud. Stakeholders will need assurances the privacy of their data is protected.	
8.	Will the project require you to contact individuals in ways which they may find intrusive?	N
	Comments: Moving existing systems and services to cloud. Project doesn't involve changing how we contact individuals.	

If you answer "Yes" to **one or more** of the privacy questions go to step 3 and complete the further assessment.

If you answer "No" to **all** of the privacy questions go to step 5 for sign off.

2.2 Security questions

ID	Screening question	Yes/No
1.	Will the service involve the processing and storage of large volumes (eg more than 100,000) of hardcopy and/or digital records?	Y
	Comments: The service will include email, emailed attachments calendars, and documents storage.	
2.	Will the service involve the processing and storage of very sensitive hardcopy and/or digital information classified above OFFICIAL?	N
	Comments: OFFICIAL information only (including the SENSITIVE handling caveat).	
3.	Will the service involve the addition of multiple components to the core network (eg hardware, software, etc.)?	Y
	Comments: Additional or as a minimum different components will be used.	

4.	Will the service be delivered by multiple suppliers?	Y
	Comments: Microsoft will be sole supplier of Office 365. On top of this will be support partners who will provide configuration, administration and support. Other suppliers may provide add on or specific services to run alongside or over Office 365 in the future. Any additional service will be subject to its own PSIA.	
5.	Will the service be externally hosted with multiple external connections to suppliers?	Y
	Comments: Cloud service with multiple external connections for routine business operations.	
6.	Will the service involve the processing and storage of hardcopy records and digital storage media outside our secure premises?	N
	Comments: No storage of ICO physical assets off premises.	
7.	Can we rely on the security provided by a commercial product or service? Please note, we will still need confidence the commercial product or service fully meets our business needs (eg commercial contract).	N
	Comments: Potentially we could rely on the security of Office 365 services but decisions must be made about how we tailor the security controls to our specific needs.	
8.	Can we apply a common solution to solve a common problem? Please note, we will still need confidence the common solution fully meets our business needs (eg is there a unique asset or threat not covered by the solution?). Examples of common solutions include: • Cloud security principles • Browser security guidance • Application development guidance • End user security guidance • Solutions provided by the digital marketplace	Y
	Comments: Office 365 services provide security controls that meet all of the government's 14 Cloud Security Principles. Implementing and configuring these controls in line with government guidelines is sufficient to protect OFFICIAL information without conducting a full risk assessment to specify appropriate security controls.	

*If you answer "Yes" to **any** of security questions one to six go to step 3 and complete the further assessment.*

*If you answer "No" to **both** security questions seven to eight go to step 3 and complete the further assessment.*

*If you answer "No" to **all** of security questions one to six; and, "Yes" to **one** of security questions seven to eight go to step 5 for sign off.*

For this project Sections 3-4 which provides a more detailed risk assessment are required.

3. Further assessment of risks

Identification of the key privacy and security risks.

3.1 Identify the privacy risks

Privacy issue	Risk to individuals	Compliance risk	Corporate risk
Collection and use Collection and use of data is unfair and unlawful.	Adverse impact to individuals' privacy.	Breach of legal and regulatory responsibilities (eg principles 1 and 2 of DPA).	Reputational damage and fines.
Data quality Collection, use and retention of poor quality data.	Adverse impact to individuals' privacy.	Breach of legal and regulatory responsibilities (eg principles 3, 4 and 5 of DPA).	Reputational damage and fines.
Individual rights Data processed without regard for statutory rights.	Adverse impact to individuals' privacy.	Breach of legal and regulatory responsibilities (eg principles 6 of DPA).	Reputational damage and fines.
Data security Confidentiality, integrity and availability of data compromised.	Adverse impact to individuals' privacy.	Breach of legal and regulatory responsibilities (eg principles 7 of DPA).	Reputational damage and fines.
Overseas transfers Data transferred to jurisdiction that doesn't adequately protect statutory rights and freedoms.	Adverse impact to individuals' privacy.	Breach of legal and regulatory responsibilities (eg principle 8 of DPA).	Reputational damage and fines.

3.2 Identify the security risks

The CESG/NCSC guidance for use of Cloud services identifies areas of risk and provides guidance on assessing and mitigating these. The 14 Cloud Security Principles cover all aspects of using a Cloud service and are sufficient to cover the scope of the entire Office 365 service.

When considering using a specific Cloud hosted service ICO has developed an Information Assurance Questionnaire, based on the 14 principles. This allows a more detailed assessment of how these principles have been implemented and for ICO to determine whether or not that implementation is sufficient.

Risks against the CESG 14 Cloud Security Principles

Security issue	Risk to information	Compliance risk	Corporate risk
Data protection in-transit Consumer data transiting networks should be adequately protected against tampering and eavesdropping via a combination of network protection and encryption.	If this principle is not implemented, then the integrity or confidentiality of the data may be compromised whilst in transit.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.
Asset protection and resilience Consumer data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.	If this principle is not implemented, inappropriately protected consumer data could be compromised.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.
Separation between consumers Separation should exist between different consumers of the service to prevent one malicious or compromised consumer from affecting the service or data of another.	If this principle is not implemented, service providers cannot prevent a consumer of the service affecting the confidentiality or integrity of another consumer's data or service.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.
Governance framework The service provider should have a security governance framework that coordinates and directs their overall approach to the management of the service and information within it.	If this principle is not implemented, any procedural, personnel, physical and technical controls in place will not remain effective when responding to changes in the service and to threat and technology developments.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.

Security issue	Risk to information	Compliance risk	Corporate risk
Operational security The service provider should have processes and procedures in place to ensure the operational security of the service.	If this principle is not implemented, the service can't be operated and managed securely in order to impede, detect or prevent attacks against it.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.
Personnel security Service provider staff should be subject to personnel security screening and security education for their role.	If this principle is not implemented, the likelihood of accidental or malicious compromise of consumer data by service provider personnel is increased.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.
Secure development Services should be designed and developed to identify and mitigate threats to their security.	If this principle is not implemented, services may be vulnerable to security issues which could compromise consumer data, cause loss of service or enable other malicious activity.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.
Supply chain security The service provider should ensure that its supply chain satisfactorily supports all of the security principles that the service claims to implement.	If this principle is not implemented, it is possible that supply chain compromise can undermine the security of the service and affect the implementation of other security principles.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.
Secure consumer management Consumers should be provided with the tools required to help them securely manage their service.	If this principle is not implemented, unauthorised people may be able to access and alter consumers' resources, applications and data.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.

Security issue	Risk to information	Compliance risk	Corporate risk
Identity and authentication Access to all service interfaces (for consumers and providers) should be constrained to authenticated and authorised individuals.	If this principle is not implemented, unauthorised changes to a consumer's service, theft or modification of data or denial of service may occur.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.
External interface protection All external or less trusted interfaces of the service should be identified and have appropriate protections to defend against attacks through them.	If this principle is not implemented, interfaces could be subverted by attackers in order to gain access to the service or data within it.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.
Secure service administration The methods used by the service provider's administrators to manage the operational service should be designed to mitigate any risk of exploitation that could undermine the security of the service.	If this principle is not implemented, an attacker may have the means to bypass security controls and steal or manipulate large volumes of data.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.
Audit information provision to consumers Consumers should be provided with the audit records they need to monitor access to their service and the data held within it.	If this principle is not implemented, consumers will not be able to detect and respond to inappropriate or malicious use of their service or data within reasonable timescales.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.

Security issue	Risk to information	Compliance risk	Corporate risk
Secure use of the service by the consumer Consumers have certain responsibilities when using a cloud service in order for this use to remain secure, and for their data to be adequately protected.	If this principle is not implemented, the security of cloud services and the data held within them can be undermined by poor use of the service by consumers.	If realised this could adversely affect the privacy of our customers; and, result in a breach of our legal and regulatory responsibilities.	If realised this could damage our reputation.

4. Identified solutions

4.1 Privacy solutions

The requirements of the DPA and GDPR have been used as the basis to assess privacy.

The key change this project brings is to have data hosted externally rather than in ICO's Core network. The key privacy risks this brings relate to data security, sovereignty and overseas transfers. This project will not add any new categories of personal data or introduce processing of data for new purposes. Any new usage would be under a separate project with its own PSIA.

Risk	Solution(s)	Result	Compliant and Proportionate?
Collection and use Collection and use of data is unfair and unlawful. (DPA principles 1 and 2)	We currently process personal data for specified and lawful purposes, and make fair processing information available to individuals. The new service will not affect the categories or specified purposes for which we process personal data. Ensure the entire ICO IT environment is suitable for and maintained at a level of Official. This includes all support, bought in, manged and hosted services. Ensure that sufficient controls are in place to support the additional handling requirements of Official Sensitive information.	Treated	Yes Current mitigations adequate
Data quality Collection, use and retention of poor quality data. (DPA principles 3,4 and 5)	We have processes to ensure the data we collect and use is adequate, accurate and not kept for longer than is necessary. The new service will not affect data quality.	Treated	Yes Current mitigations adequate
Individual rights Data processed without regard for individuals' rights. (DPA principles 6)	We have processes to recognise and respond to information requests. The new means of storing data will not in any way diminish individuals' rights.	Treated	Yes Current mitigations adequate

Data security Confidentiality, integrity and availability of data compromised. (DPA principle 7)	The service will provide appropriate security in line with the government's Cloud Security Principles. Please refer to section 4.2 for detail.	Treated	Yes Any processing of personal data by the provider must be carried out under contract in compliance with principle 7 of the DPA; and, include provisions regarding control of the data in the event we want to terminate or transfer the service.
Overseas transfers Data transferred to jurisdiction that doesn't adequately protect statutory rights and freedoms. (DPA principle 8)	The service will not process personal data outside the EEA, and UK data centres will be used wherever possible. Any new usage or functionality to be subject to its own PSIA	Treated	Yes Current mitigations adequate

4.2 Security solutions

Note in the table below the Source of information in the Solution column is identified by the bullet heading. M – Microsoft, C – CESG, I - ICO

Risk	Solution(s)	Result	Compliant and Proportionate?
Data protection in-transit If this principle is not implemented, then the integrity or confidentiality of the data may be compromised whilst in transit.	M All customer-facing servers negotiate a secure session using SSL/TLS 1.2 with client machines, securing the data in transit. M This applies to various protocols such as HTTP(S), POP3, etc. that are used by clients such as Skype for Business, Outlook and Outlook Web App (OWA) on any device. M Microsoft has support for strong encryption using TLS 1.2 across all workloads. The use of TLS/SSL establishes a highly secure client-to-server connection to help provide data confidentiality and integrity between the desktop and the data centre. I Microsoft provide a connection method called 'Express Route' which allows connection to an MPLS network which can be accredited to Official.	Treated	Yes ICO access to be built and maintained to maintain the Official status. Preferred implementation will be using an 'Official' accredited MPLS network to Office 365 Express route.

Asset protection and resilience If this principle is not implemented, inappropriately protected consumer data could be compromised.	M For government data classified as OFFICIAL, Microsoft use datacentres in Dublin and Amsterdam and provide the additional assurance of complying with EU model clauses in order meet data protection legislation. I New (Sept 16) UK data centres are available for Office 365. M Microsoft's data centre security is evidenced by compliance with the ISO-27001 and SASE-16 information security standards. M Customer-authored data is encrypted at rest for all cloud services. M When hard disks are taken out of service they are demagnetised and destroyed on site. M Microsoft provides a contractually-backed SLA to a minimum of 99.9%. Auriga – RMADS to be amended to reflect Office 365 and associated connectivity.	Treated	ICO to use UK data centres wherever possible. Where certain functionality is not provided from UK centres, then EU centres will be used.

Separation between consumers If this principle is not implemented, service providers cannot prevent a consumer of the service affecting the confidentiality or integrity of another consumer's data or service.	C Microsoft conducts ongoing penetration tests of their environment in line with the dynamic nature of the cloud, ensuring that a customer's data remains private to them. C Microsoft also conducts annual independent CREST penetration tests. C Residual risks are published in Microsoft's Risk Management and Accreditation Document Set (RMADS) and Residual Risk statement, available under NDA. C Follow CESG guidance on implementing Office 365 at Official.	Treated	Yes
Governance framework If this principle is not implemented, any procedural, personnel, physical and technical controls in place will not remain effective when responding to changes in the service and to threat and technology developments.	M Microsoft complies with the ISO-27001 information security standard, covering the scope of the service delivered. M Microsoft is regularly audited by independent external auditors who are recognized by UKAS. M The Statement of Applicability for Microsoft's ISO controls is available under NDA.	Treated	Yes

Operational security If this principle is not implemented, the service cannot be operated and managed securely in order to impede, detect or prevent attacks against it.	M Configuration, change management, incident response and protective monitoring are all demonstrated in Microsoft's compliance with the ISO-27001 (information security standard). M In addition to Microsoft's ISO-27001 compliance, and their use of independent 3rd party penetration tests, they operate an assumed breach model and use active red-team penetration testing and vulnerability management as part of their Operational Security Assurance (OSA). C CESG guidance on implementing Office 365 at Official. I ICO security and compliance questionnaires for all third parties providing parts of this service.	Treated	Yes ICO to ensure that CESG/NCSC guidance has been followed ICO to assess any third party supplying a part of this service using the supplier security questionnaire ICO to ensure ongoing compliance by regular checks and reviews, including IT Health Checks

Personnel security If this principle is not implemented, the likelihood of accidental or malicious compromise of consumer data by service provider personnel is increased.	M Customer authored data can only be accessed by suitably cleared Engineering and Operation support staff. M Staff are subject to pre-employment and on-going background check for social security; criminal convictions; the Office of Foreign Asset Control list; the Bureau of Industry and Security list and the Office of Defence Trade Controls debarred list. M New hires are also subject to education history and employment history checks. M Contractors and others who may have access to customer authored data are subject to these same checks. I ICO security and compliance questionnaires for all third parties providing parts of this service.	Treated	Yes ICO to ensure ongoing compliance by regular checks and reviews
Secure development If this principle is not implemented, services may be vulnerable to security issues which could compromise consumer data, cause loss of service or enable other malicious activity.	M Windows has a Commercial Product Assurance Build Standard verification. This is the same development practice used throughout Microsoft for all products and services. M The Security Development Lifecycle was the precursor to ISO-27034 and is used as the standard development practice for all Microsoft Products and Services.	Treated	ICO to ensure ongoing compliance by regular check and reviews, including IT health checks

Supply chain security If this principle is not implemented, it is possible that supply chain compromise can undermine the security of the service and affect the implementation of other security principles.	M The majority of technologies used in the delivery of Microsoft's cloud services are developed by them in-house or through acquisitions. M Microsoft applies EU Model Clauses to their services. All suppliers must sign and abide by their security controls. M Microsoft's services are certified against the ISO-27001 Information Security standard. I ICO security and compliance questionnaires for all third parties providing parts of this service.	Treated	Yes ICO to assess any third party supplying a part of this service using the supplier security questionnaire ICO to ensure ongoing compliance by regular checks and reviews
Secure consumer management If this principle is not implemented, unauthorised people may be able to access and alter consumers' resources, applications and data.	M Customers maintain direct control over which user accounts can perform authorised administrative functions on the service. This is accomplished by federating the customer's on premise active directory. M The separation and access control within management interfaces is subjected to independent penetration testing. I ICO security and compliance questionnaires for all third parties providing parts of this service.	Treated	Yes ICO to ensure that CESG/NCSC guidance has been followed ICO to assess any third party supplying a part of this service using the supplier security questionnaire ICO to ensure ongoing compliance by regular check and reviews, including IT health checks

Identity and authentication If this principle is not implemented, unauthorised changes to a consumer's service, theft or modification of data or denial of service may occur.	M Microsoft's services support 2 factor authentication. M Active Directory Federation Services provides a SAML access mechanism. M Username and password policies remain under the customer's control. M Authentication tokens are passed over an encrypted channel. C CESG guidance on implementing Office 365 at Official.	Treated	Yes ICO to undertake to have a security design review of its specific implementation, and to have the system built IT Health checked
External interface protection If this principle is not implemented, interfaces could be subverted by attackers in order to gain access to the service or data within it.	M Microsoft conducts annual independent CREST penetration tests. M Residual risks are published in Microsoft's Risk Management and Accreditation Document Set (RMADS) and Residual Risk statement, available under NDA. I ICO to conduct independent annual penetration tests using government approved testers.	Treated	Yes
Secure service administration If this principle is not implemented, an attacker may have the means to bypass security controls and steal or manipulate large volumes of data.	M Microsoft evidences their service administration model with ISO-27001 certification. I ICO to conduct independent annual IT Health Checks using government approved testers.	Treated	Yes

Audit information provision to consumers If this principle is not implemented, consumers will not be able to detect and respond to inappropriate or malicious use of their service or data within reasonable timescales.	M	Microsoft's services provide enhanced capabilities, allowing customers to audit and delegate end-user access within the service offering (further details available in service the descriptions).	Treated	Yes
Secure use of the service by the consumer If this principle is not implemented, the security of cloud services and the data held within them can be undermined by poor use of the service by consumers.	M M C	Microsoft provide outline guidance as part of a service's RMADS. Individual devices should be configured in line with CESG's end user device guidance. CESG guidance on implementing Office 365 at Official.	Treated	Yes

5. Sign off and record the outcomes

Who has approved the privacy and security risks involved in the project? What solutions do you need to implement?

You should record sign-off if the initial assessment does not identify any significant risks, and further assessment is not required.

5.1 Privacy solutions

Risk	Solution	Approved by
Collection and use Collection and use of data is unfair and unlawful.	Current mitigations adequate.	
Data quality Collection, use and retention of poor quality data.	Current mitigations adequate.	
Individual rights Data processed without regard for statutory rights.	Current mitigations adequate.	
Data security Confidentiality, integrity and availability of data compromised.	Put strong contracts and supplier management in place to ensure processing of personal data by all providers is carried out in compliance with principle 7 of the DPA; and, include provisions regarding control of the data on contract end or transfer of the service. Implement granular access controls giving restricted access to Official Sensitive data. Provide secure means to email and exchange data with external stakeholders. Implement Azure Rights Management to give further control and logging.	
Overseas transfers Data transferred to jurisdiction that does no t adequately protect statutory rights and freedoms.	Current mitigations adequate.	

5.2 Security solutions

Risk	Solution	Approved by
Data protection in-transit If this principle is not implemented then the integrity or confidentiality of the data may be compromised whilst in transit.	Secure protocols running over a secure network between known endpoints. Network layer: Implement 'Office 365 Express Route' to connect Office 365 to ICO's MPLS network. Applications layer: Use secure protocols for all traffic between ICO Core network and Office 365. HTTPS SSL, TLS1.2.	
Asset protection and resilience If this principle is not implemented, inappropriately protected consumer data could be compromised.	ICO's Office 365 Tenancy to be based on UK region with as many applications as possible storing data in UK including all Official Sensitive data. As a minimum Email and SharePoint data to be held in UK. All ICO controlled servers in the Office 365 environment will be patched and have Anti-virus enabled in a similar manner to the core network. Patching will fall in line with the monthly cycle based on Microsoft's patch Tuesday releases. RMADS to be amended to reflect Office 365 and associated connectivity.	

Separation between consumers If this principle is not implemented, service providers cannot prevent a consumer of the service affecting the confidentiality or integrity of another consumer's data or service.	ICO Tenancy protected by firewall, certificate / encryption and lockbox. Inter-connections of email and SharePoint in hybrid environments protected by certificates / encryption, AD, firewalls, Azure rights management. Separation of Production and Test environments through distinct Active Directory domains, vlans & transport rules, as well as, Azure rights management and file level encryption on production data. Dummy data only is permitted within the transition test environment.	
Governance framework If this principle is not implemented, any procedural, personnel, physical and technical controls in place will not remain effective when responding to changes in the service or to threat and technology developments.	The ICO has existing change control procedures and a Change Advisory Board (CAB). New process will need to be put in place to integrate changes initiating in Office 365. The existing change process is adequate for ICO changes when using Office 365. Regular IT Health Checks will be carried out in line with existing practices: A check prior to using with live information; A check that the configurations and operation are as expected as a part of the next full annual IT Health Check; Subsequent annual checks based on risk, key vulnerabilities or areas subject to change.	
Operational security If this principle is not implemented, the service can't be operated and managed securely in order to impede, detect or prevent attacks against it.	Suppliers to complete ICO security and compliance questionnaires for: • Secure network - MPLS provider • Unified Communications • Third parties having access to Office 365 email	

Personnel security If this principle is not implemented, the likelihood of accidental or malicious compromise of consumer data by service provider personnel is increased.	ICO to hold regular supplier reviews (from monthly to annual based on complexity of solutions and risk). Quarterly reviews of people with elevated access rights across the entire IT environment will include Office 365. The use of 2 Factor Authentication will be included in the design of how elevated access rights are set up. Restrict access to Office 365 by enabling Lock box. This allows the ICO to grant 'one time access' only when required to Microsoft or others providing support.	
Secure development If this principle is not implemented, services may be vulnerable to security issues which could compromise consumer data, cause loss of service or enable malicious activity.	ICO to IT Health Check Office 365 environment, including access rights and permissions, ahead of storing data. Include Office 365 as a part of ICO's Annual IT Health Check.	
Supply chain security If this principle is not implemented, it is possible that supply chain compromise can undermine the security of the service and affect the implementation of other security principles.	ICO to have regular supplier reviews (from monthly to annual based on complexity of solutions and risk). Office 365 Email will initially be operated under the NPS contract which has Monthly supplier meetings. There is an existing Security Working Group attended by significant suppliers. ICO will consider requiring new suppliers to attend where appropriate.	
Secure consumer management If this principle is not implemented, unauthorised people may be able to access and alter consumers' resources, applications and data.	All access granted on principal of minimum access rights required. Very tight control of System Admin privileges by ICO. Quarterly reviews of elevated permissions. Review starter/leaver/transfer process to reflect use of Office 365.	

Identity and authentication If this principle is not implemented, unauthorised changes to a consumer's service, theft or modification of data or denial of service may occur.	Implement ADFS. All data in Office 365 accessible only from ICO Core environment. Webmail turned off. Implement Azure Rights Management.	
External interface protection If this principle is not implemented, interfaces could be subverted by attackers in order to gain access to the service or data within it.	Following best practices from Microsoft and NCSC/CESG in setup of Office 365. Designed to allow the minimum connectivity necessary between the Core network and Office 365 to prevent unauthorised access in either direction. Some configurations are required to make services 'Internet facing'. However, the actual connections will be restricted entirely to within the ICO Office 360 Tenancy and Core network. Initial IT Health check to validate build, the follow Annual IT Health Check and penetration test policy.	
Secure service administration If this principle is not implemented, an attacker may have the means to bypass security controls and steal or manipulate large volumes of data.	All access granted on principal of minimum access rights required. Annual IT Health check and penetration test. Strong boundary controls enforcing access from ICO network, restricting Office 365 access to within the Tenancy and Core network. All changes subject to ICO Change management.	

Audit information provision to consumers If this principle is not implemented, consumers will not be able to detect and respond to inappropriate or malicious use of their service or data within reasonable timescales.	Use Azure Rights Management to restrict and log access. Enable logging where available in Office 365. The ICO will use GPG13 as the model, then to define precise details of logging for each part of the service subject to an overarching policy on access to this information and retention and disposal.	
Secure use of the service by the consumer If this principle is not implemented, the security of cloud services and the data held within them can be undermined by poor use of the service by consumers.	Use PSIAs to identify risks and appropriate controls. Designs to incorporate security settings and configurations. Independent validation of PSIAs and High Level Designs. IT Health Check of the environment built.	

For each component enabled and configured in Office 365, the latest guidance from Microsoft, CESG/NCSC and the CTS (Common Technology Services) must be followed.

6. Integrate the outcomes back into the project plan

Action to be taken	Date for completion	Responsibility for Action
All technical solution identified in section 5 to be added to appropriate project backlog	On sign off of this PSIA	Paul Lee
IT Health Check of new environment to be scoped and arranged by IT Assurance team	Before live data is stored in Office 365	John Rackstraw
Supplier Assurance Questionnaires to be tailored, issued and evaluated for any new services or suppliers	Prior to contracting for a service	Steven Rook

Contact point(s) for future privacy concerns	Steven Rook, Helen Ward
Contact point(s) for future security concerns	Steven Rook, David Wells

7. Glossary

AD ADFS	Active Directory – Within a Micro soft environment is a central repository for security, access controls and configuration Active Directory Federated Service extends AD to Office 365, provides synchronisation of passwords and single sign on
Azure Rights Management Azure/Advanced Information Protection	Microsoft has renamed a number of it security components as at Dec 2016: Azure Information Protection (also referred to as Advanced Information Protection in some documentation) provides classification, labelling, and protection for an organization's documents and emails. The protection technology uses the Azure Rights Management service; now a component of Azure Information Protection.
BI BI/MI	Business Intelligence and Management Information
C:/ F:/ drive, Shared folders	Locations where people store data on their desktop PC. This may be a physical location on a laptop but is most commonly held centrally but appears and is used as a local hard drive
CESG/NCSC	National Cyber Security Centre. The NCSC acts as a bridge between industry and government, providing a unified source of advice, guidance and support on cyber security
CREST	CREST– a CESG recognised level of penetration testing
CIPHR	ICO's HR software
CRM	ICO's software used in the ICE registration system, Stakeholder system and the new ICE360 casework system
DPA GDPR	Data Protection Act General Data Protection Regulation
EDRM	ICO's Electronic Document and records Management System (known as Meridio)
Egress	A secure email service provides by Egress
GDS CTS	Government Digital Service (GDS) Common Technology Services (CTS)
GP	ICO's Finance system software
GPG13	Protective Monitoring for HMG ICT Systems
GSI / PSN	ICO's ISP providing email as in user@ico.GSI.gov.uk. This is a centrally provided government service providing a secure means of exchanging email at Official. This service ends in Mar 2017. Government Digital Service (GDS) have developed a blue print for each organisation to follow to configure their email services. This includes mandating TLS 1.2 and a number of other security features
IT Health Check	Guidance from Government on operation of IT systems is to have regular security audits. These are known as IT

ITHC IT Security Audit	Health Checks and should be carried out by suitably trained and accredited people. For central government the CHECK scheme, run by NCSC, provides the necessary level of assurance. The ITHC aims to provide assurance that the external systems are protected from un-authorised access or change, and they do not provide an un-authorised entry point into other linked Government IT systems such as PSN services. The internal systems should be tested to provide further assurance that no significant weaknesses exist on network infrastructure or individual systems that could allow one internal device to intentionally or unintentionally impact on the security of another. ICO's policy is to conduct an ITHC for significant new applications and infrastructure prior to use. And to conduct an annual ITHC with a scope taking a risk based approach favouring changes in the year, evidence of good housekeeping, and externally facing components.
Lock box	An Office 365 security feature providing an additional level of encryption of data at rest. The keys to this encryption although stored within Office 365 are only accessible by authorisation requests controlled by the ICO and are not available to Microsoft.
MS Express Route	Connections to Office 365 can be across the Internet or over a dedicated link (Express Route) see also MPLS
MPLS	Multiprotocol Label Switching is a type of data-carrying technique for high-performance telecommunications networks providing 'private' WANS and links through known providers. ICOs new external WAN and internet circuits will be built on MPLS.
RMADS	ICO has a single Risk Management and Accreditation Documentation Set which includes a residual risks / risk treatment plan. The RMADS are reviewed annually and when there are significant systems of data processing changes.
SAML SAML SSO 2 Factor Authentication	Secure protocols for logging in to system SAML Security Assertion Markup Language SSO Single Sign On 2 Factor Authentication, an additional means of verification; including tokens (RSA), One time passcodes sent to phones or email
TLS SSL/TLS	Transport Layer Security Industry wider security protocol for securing connections. TLS 1.2 is the most current version.

8. Document control

Version	Date	Author	Change
V0.1	16/9/16	Steven Rook	Initial Assessment (section 2), identify security risks (section 3.2), security solutions (section 4.2)
V0.2	19/9/16	David Wells	Data Flows, Privacy solutions and Security solutions, added CESG guidance
V0.3	20/9/16	David Wells	Add consultations section
V1.0	21/9/16	David Wells	Distributed to ITSG and SMT
V1.1	05/12/16	David Wells	Add details of controls to be implemented Expanded Privacy risk assessment
V1.2	11/01/17	David Wells	Incorporating points raised in review by external security advisors – Auriga Consulting

Template used

Title	Privacy and Security Impact Assessment Template
Version	1.0
Status	Released
Owner	Information Security Manager
Approved by	Information Governance Steering Group
Release date	August 2016
Review date	March 2017

Case reference

IC-203321-W1K8

Use of Biometrics to Authenticate to Apple Mobile Devices - PSIA

ico.
Information Commissioner's Office

Privacy and security impact assessment (PSIA)

Use of Biometrics to authenticate to Apple mobile devices – November 2018

Background

The ICO started to use iPads and iPhones in 2015. Access to the devices is secured by using the device's pass code or PIN code, respectively. To provide greater flexibility in using these devices a change is proposed to allow fingerprint recognition (Touch ID) or facial recognition (Face ID) to be used for authentication.

iPads will be replaced over the next eighteen months by laptops, a number of iPhones and a small number of iPads are likely to remain. Laptops also have the fingerprint security feature.

The devices are managed and secured using the Airwatch MDM product, this will change to Microsoft Intune through 2018 and 2019, with Airwatch being retired completely. Enabling the use of Touch ID or Face ID can be done in both Airwatch and Intune.

Security Assessment

The use of biometrics as the sole authentication mechanism to unlock mobile devices is judged to be an acceptable option (NCSC view[1]) provided the risks are understood. Although they do note that in a targeted attack it may be more vulnerable. The ICO accepts this risk, but would review if the Security threat level were raised to Critical or there was a risk to particular members of staff. The biometric information is stored and used in the same place and way that the pass and PIN code is[2].

Privacy Assessment

[1] Guidance on Biometrics from NCSC for iOS 11 from Nov 2017 is:
iOS 11 devices can use Touch ID or Face ID for biometric authentication which happens within the Secure Enclave Processor. This means that a physical attack on a locked device should not result in compromise of data.
The fingerprint reader has a 0.002% false acceptance rate for a random fingerprint, but there have been published attacks on the feature using artefacts taken from the device. No independent information on the security posture of the facial recognition capabilities has been published at present. Using such attacks, a targeted physical attack on a specific user could result in the attacker gaining access to the device. You should consider these limitations when devising an authentication policy which permits the use of biometrics.

[2] Secure Enclave details available from Apple:
The chip in your device includes an advanced security architecture called the Secure Enclave, which was developed to protect your passcode and fingerprint data. Your fingerprint data is encrypted, stored on device, and protected with a key available only to the Secure Enclave. Your fingerprint data is used only by the Secure Enclave to verify that your fingerprint matches the enrolled fingerprint data.

The ICO does not currently use any form of bio-metrics. This document covers the privacy and security concerns for introducing this technology for the limited specific use of authentication.

The following controls are in place to safeguard the use of a fingerprint:

- The feature to use biometrics to authenticate is a user selectable option. There will be no compulsion to use this technology, the two means (pass/PIN code and biometrics) for authentication coexist and can be used interchangeably or separately.

- The actual fingerprint and facial pattern is not stored[3].

- The resulting code generated from the facial pattern/fingerprint and the algorithm is stored in the Secure Enclave chip only. It never leaves the device and is not accessible through or to any applications or held externally.[4]

In deterring whether it is appropriate to use of biometrics for this purpose the GDPR required screening questions, as published in the DPIA template, have been used:

ID	Screening question	Yes/No
1.	Does the system/process use systematic and extensive profiling or automated decision-making to make significant decisions about people?	No
	Comments:	
2.	Does the system/process involve large scale processing of data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, data concerning a person's sex life or sexual orientation or data relating to criminal convictions or offences?	No
	Comments:	
3.	Will you be systematically monitoring a publicly accessible place on a large scale?	No
	Comments:	
4.	Will you be implementing novel technologies or new applications of existing technologies?	No
	Comments: Although this technology is new to the ICO	
5.	Will the system / process help to make decisions about access to	No

[3] Touch ID doesn't store any images of your fingerprint, and instead relies only on a mathematical representation. It isn't possible for someone to reverse engineer your actual fingerprint image from this stored data.
Your fingerprint data is encrypted, stored on device, and protected with a key available only to the Secure Enclave.

[4] Your fingerprint data is used only by the Secure Enclave to verify that your fingerprint matches the enrolled fingerprint data. It can't be accessed by the OS on your device or by any applications running on it. It's never stored on Apple servers, it's never backed up to iCloud or anywhere else, and it can't be used to match against other fingerprint databases.

	services, opportunities or benefits using automated decision-making, profiling or special category data (see list in question 2)? Comments:	
6.	Will you be profiling using personal data on a large scale, taking into account the number of individuals involved, the volume and range of personal data, the duration of the processing and the geographical area covered? Comments:	No
7.	Will you be processing biometric or genetic data? Comments: Although biometrics are personal data the way it is held (locally) and used (exclusively to grant or deny access to a specific device in the possession of that person a specific person) does not raise any privacy concerns. Its use is optional	Yes, see comment
8.	Will you be matching or combining data from sources collected for other purposes or by other data controllers? Comments:	No
9.	Will the system / process include 'invisible processing' of personal data (processing without providing a privacy notice to the individual)? Comments:	No
10.	Will you be processing personal data in a way which involves tracking individuals' location or behaviour? Comments:	No
11.	Will you be processing children's personal data for profiling, automated decision-making or marketing purposes or to offer them a service directly? Comments:	No
12.	Will the system / process involve personal data which could result in a risk of physical harm in the event of a security breach? Comments:	No

Advised screening questions which are relevant.

19.	Will you be implementing technological or organisational solutions which are new to the organisation? Updated or alternative versions of technologies currently in use are not to be considered new unless they include changes with considerable privacy implications (e.g. adding cloud storage to a previously local application). Comments: The privacy notice will be updated	Yes

DPO recommendations

Record any recommendations from the DPO or their delegates and responses here. This serves as useful tool when reconsidering a rejected DPIA or in recording the justification if the organisation rejects the DPO's advice.

No	Recommendation	Project Team Response

1	DPO noted that there was also a requirement to use fingerprints for authentication to Laptops.	Agreed that laptops will be subject to a further update to this document

Sign Off

Send this to the DPSIA Committee to approve the privacy and security risks involved in the project, the solutions to be implemented and the residual risk.

Approved by	Role	Date	Project Stage
Louise Byers	DPO	9/11/18	Approval to implementation on Apple devices
David Wells	Group Manager Cyber Security	9/11/18	Approval to implementation on Apple devices

Change history

Version	Date	Author	Change description
V0.1	11 Nov 2018	David Wells	Initial document, with scope: Use of fingerprints for authentication to Apple devices.
V1.0	11 Nov 2018	David Wells	DPO sign off
V1.1	14 Jan 2019	Steven Rook	Amendments to include Facial Recognition (Face ID) for Apple devices