Data Protection Impact Assessment – Microsoft 365

Document Name	Data Protection Impact Assessment – Microsoft 365
Author/Owner (name and job title)	Will McLoughlin – Senior Product Owner, Productivity and Collaboration
Department/Team	Digital Data & Technology, Product and Infrastructure
Document Status (draft, published or superseded)	Published
Version Number	V1.0
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 365 (M365)
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 M365. ICO has control over what we use M365 for as well as its implementation and configuration in our business.

Our use of the services is governed by Microsoft's Product Terms[1] and Data Protection Addendum[2], 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] Microsoft Product Terms
[2] MicrosoftProductandServicesDPA(WW)(English)(Jan2023)(CR).docx (live.com)

(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). [3]

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 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.[4]

1.2 Describe your new service or process

This DPIA covers the ICO's use of the Microsoft 365 suite of applications as provided under our E5 licencing arrangement. This document substantially builds 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 2023):

Bookings
Calendar
Excel
Exchange
Forms
Kaizala
Lists
OneDrive
OneNote

[3] Guidance for Data Controllers Using M365 Section 2
[4] MicrosoftProductandServicesDPA(WW)(English)(Jan2023)(CR).docx (live.com)

Outlook
People
Planner
Power Apps
Power Automate
Power BI
PowerPoint
Power Virtual Agents
Project
SharePoint
Stream
Sway
Teams
To Do
Visio
Viva Connections
Viva Engage
Viva Insights
Whiteboard
Word

Whilst all applications listed above 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 and when our application use changes.

It is recognised that it may still be necessary to create exceptional additional DPIAs for some M365 applications, for example if and where the ICO's intended specific use of that application is significantly at variance with the contents of this DPIA, or simply where a more in-depth assessment of an application will assist with managing risks. In such cases, this master document will be updated to provide reference to the additional documentation, along with the rationale for its creation.

Some M365 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 the subject of its own DPIA Screening Assessment (as a minimum), 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 any processing activity, as well as customisations. Examples of Customer Data processed in M365 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	ICO Staff and all other data subjects whose data the ICO processes as part of its 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 Product Terms agreed	As described in their Guidance for Data Controllers using Office 365 - Microsoft GDPR | Microsoft Learn[8] and the Product Terms[9], for instances of M365 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	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

[8] Guidance for Data Controllers using Office 365 - Microsoft GDPR | Microsoft Learn
[9] Microsoft Product Terms

• Chats • Voicemail • Shared files • Recordings and transcriptions. • Profile data such as email address, profile picture and phone number • Call history		between ICO and Microsoft. All third-party sub-processors with which Customer Data from Microsoft's Core Online Services is shared are included in the Online Services Subcontractor list.[5] All third-party sub processors that may access Support Data (including only Customer Data that the ICO chooses to share during support interactions) are included in the Microsoft Commercial Support Contractors list.[6] Microsoft commit that they will not transfer to any third party (not even for storage purposes) data that we provide to them through our use of	Business, and (4) project content uploaded to Project 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. Microsoft continues to abide by the terms of the Privacy Shield framework. "Microsoft practices privacy by design and privacy by default in its engineering and business functions. As part of these efforts, Microsoft performs comprehensive privacy reviews on data processing operations that have the potential to cause impacts to the rights and freedoms of data subjects. Privacy	LinkedIn services, Microsoft will retain Customer Data stored in the Online Service 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 M365 environment should be managed by Information Asset Owners as per the ICOs Retention and Disposal Policy.

[5] Service Trust Portal (microsoft.com)

[6] Download Services Supplier List from Official Microsoft Download Center

		the business cloud services that are covered under the Microsoft Product Terms.[7]	teams embedded in the service groups review the design and implementation of services to ensure that personal data is processed in a respectful manner that accords with international law, user expectations, and our express commitments. These privacy reviews tend to be very granular—a particular service may receive dozens or hundreds of reviews. Microsoft rolls up these granular privacy reviews into Data Protection Impact Assessments (DPIAs) that cover major groupings of processing, which the Microsoft EU Data Protection Officer (DPO) then reviews. The DPO assesses the risks related to the data processing to ensure that sufficient mitigations are in place. If the DPO finds unmitigated risks, he or she recommends changes back to the engineering group. DPIAs will be reviewed and	

[7] https://www.microsoft.com/en-us/trust-center/privacy/data-location

			updated as data protection risks change."[10] 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[11] Update Sept 2023: On 8 June 2023, the UK and US governments announced their commitment in principle to establish a UK-US data bridge. This marks the UK's intention to establish a data bridge for the UK extension to the EU-US Data Privacy Framework, subject to finalising the UK's assessment of US data protection laws and	

[10] GDPR Data Protection Impact Assessments, DPIA support & FAQs (microsoft.com)
[11] International data transfer agreement and guidance | ICO

			practices. This would allow for the free flow of personal data between the UK and certified organisations in the US. UK-US data bridge: joint statement - GOV.UK (www.gov.uk)	
Service-generated Data: This is data that is generated or derived by Microsoft through operation of the service, such as use or performance data. Most of these data contain pseudonymous identifiers generated by Microsoft.	ICO staff	As above	Structural transfer of Diagnostic Data to the USA.	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.
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. We only allow Microsoft to collect Required diagnostic data, which does not include personal, sensitive or identifiable data.[12]	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	ICO Staff	As above	Structural transfer of Diagnostic Data to the USA.	This data is retained for a default period of up to 180 days from collection,

[12] Required diagnostic data for Office - Deploy Office | Microsoft Learn

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			We have enabled Customer Lockbox in our Admin Portal. Customer Lockbox ensures that Microsoft can't access our content to do any service or support operations without our explicit approval.	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

M365 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 M365 to process personal data for general processing purposes 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.

For personal data processed under Part 3 DPA 18 the processing is based on law and is strictly necessary for the performance of a task carried out for that purpose. Our Safeguards Policy[13] outlines our sensitive processing for law enforcement purposes and explains:

i) Our procedures for securing compliance with the law enforcement data protection principles;

ii) Our policies as regards the retention and erasure of personal data, giving an indication of how long the personal data is likely to be retained.

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 M365 service we have chosen. It's necessary for the ICO to use M365 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

[13] Safeguards Policy | ICO

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.

Update September 2023: in updating this document I have consulted with our commercial legal team on aspects relating to the transfer of data overseas.

In assessing the potential for a subsequent restricted transfer of personal data that is processed by the ICO for law enforcement purposes, the ICO has obtained, and relies upon, Microsoft's assurances that no restricted transfer will undermine the level of protection of individuals provided for in the UK, and that all personal data that is subject to a restricted transfer will, at all times, receive the same level of protection that is provided for within the UK, regardless of whether it is at rest or in transit.

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 M365 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[14] and staff privacy notice[15].

Some additional categories of personal data are processed as a direct result of our staff using M365 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 actively and intentionally provided to Microsoft by ICO through an engagement with Microsoft in order to obtain technical support.

Technology used for the processing:

M365 suite of applications as provided under our E5 licencing arrangement (see 1.2 above).

M365 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.

M365 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 within 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. Provisions under IDTA for restricted transfer of data apply to EEA and third countries.

Usage Data is hosted[16] in Microsoft's UK and/or EMEA data centres.

[14] How do we get information? | ICO
[15] Policies - Staff Privacy Notice.pdf - All Documents (sharepoint.com)
[16] Location of data in Microsoft Teams - Microsoft Teams | Microsoft Learn

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 M365 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.[17]

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 via Purview within the M365 product set. For M365 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.

[17] Privacy & data management overview - Microsoft Service Assurance | Microsoft Learn

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 M365 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 M365 Compliance Center, now known as Purview. Currently configured for Outlook (12 months), Teams chats (7 days), and inactive 365 Groups (12 months). A proposal has been approved and is being finalised (as of September 2023) to introduce 12 months retention for Teams channel messages. 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?

M365, 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 M365; 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. Customer Lockbox enabled.	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 to remind staff about appropriate use. Expected mitigation: further guides to be produced as and when required.	1	1	1 - Low
3.	Personal information is disclosed to unauthorized third-party organization	Reduce	Existing mitigation: Usage data is only accessible via M365 administrators, it is not shared with 3rd party organisations.	2	1	2 - Low

	during diagnostic/fault resolution activities.		M365 user feature Customer Lockbox is active. Microsoft support engineers requiring access to user data must first submit a lockbox data request. This can only be approved by M365 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 Product 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 enforcement, Microsoft will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing	4	1	4 - low

			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.[18]			
6.	Microsoft security controls are not adequate resulting in a loss of confidentiality, integrity or availability of data.	Accept	<u>Existing Mitigation:</u> 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	4	1	4- low

[18] Guidance for Data Controllers using Office 365 - Microsoft GDPR | Microsoft Learn

			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 M365 to data subjects.	Accept	<u>Existing Mitigation:</u> Agreed Product 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 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.	4	1	4 - low
8.	Data transferred overseas to a non-adequate country.	Accept	<u>Existing Mitigation:</u>	3	1	3 - low

			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, and underpinned by a transfer risk assessment. We have enabled Customer Lockbox in our Admin Portal. Customer Lockbox ensures that Microsoft can't access our content to do any service or support operations without our explicit approval.			
9.	Personal data retained for longer than necessary	Accept	<u>Existing Mitigation</u> 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 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	2	3	6 - medium

			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 M365 environment should be managed by Information Asset Owners as per the ICOs Retention and Disposal Policy.[19]			

[19] Guidance for Data Controllers using Office 365 - Microsoft GDPR | Microsoft Learn

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.	There is reference to usage guides, how to policies and etiquette guides for staff to mitigate some risks yet it was noted that these aren't particularly accessible to staff and therefore their impact is limited. Consideration should be given to the creation of a guidance gateway, perhaps on IRIS, for all existing M365 guidance so staff understand where to go for information on M365 applications. Staff need to be clear about what expected use is, what is prohibited and also know when / where to raise queries if they intend new or novel uses of a particular application.	07/12/2022	We recognise the need for continuous review and refresh, and additions to policies, guides, and other resources that help colleagues get the most out of Microsoft 365. We are working with ITHelp and Business Partners to ensure the Digital Support Hub on Iris signposts to all such resources. We have also started to make use of Yammer to grow a community of Microsoft champions and ordinary users sharing best practice for usability and information security. This can also act as an open forum for queries about new or novel uses of the applications, with the answers given displayed for the benefit of everyone.
2.	The content of the DPIA completed by the Dutch Ministry of Justice and Securities was discussed which flags a	07/12/2022	This document was used for reference in the production of this DPIA, and the various risks and mitigations

	number of risks relating to M365 applications. Project team are advised to consider the measures suggested to mitigate risks identified as part of that DPIA to see if any can be implemented by ICO to further reduce risks.		considered against our own position. To briefly address those which we consider applicable here: 1. E2EE for Teams 1-2-1 calls. This has to be user enabled at both ends, so is not practically applicable at tenant level. Its use also disables transcription and recording, which are occasionally useful functions, so we do not see it proportionately necessary to recommend users enable E2EE for 1-2-1 calls at this time. 2. Structural transfer of telemetry to the USA. We only allow required diagnostic data to be collected by Microsoft, which does not include personal, sensitive or identifiable data.[20] 3. (N/A) 4. (N/A – Data Viewer Tool not enabled) 5. Difficulty to exercise data subject access rights to Required Service Data. We will monitor any developments by Microsoft of the DSAR tool. 6. Lack of control: personal data shared with Microsoft and third parties as controllers. Additional Optional Connected Experiences and Teams Third Party Apps both disabled. 7. Employee monitoring system: chilling effect. We have enabled anonymisations to data in Teams Analytics & reports, Viva Insights partially disabled. Further uses of Analytics subject to new DPIAs.

[20] Required diagnostic data for Office - Deploy Office | Microsoft Learn

3	Appendix 3 should be completed in full with text in each row so it's clearer as to whether there are / aren't any specific privacy friendly features deployed for applications that are currently blank.	07/12/2022	Accept – appendix 3 updated

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**

Training, usage policies, and How-to/etiquette guides to be reviewed regularly and made available to staff. Further support documents to be produced if M365 usage expands.	Ongoing – no fixed completion date	Will McLoughlin – M365 product owner	N/A
Continue to monitor developments regarding implementation of the EU Data Boundary by Microsoft.	Ongoing – no fixed completion date	Will McLoughlin – M365 product owner	N/A
Request a Transfer Risk Assessment for Microsoft 365 Products	31 October 2023	Will McLoughlin – M365 Product Owner	

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 expected risk score for most risks is low and these can be accepted.
There is one medium risk associated with the ICO retaining personal data for longer than is necessary.

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	22 September 2023	Review of DPIA

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
V0.1	07/12/2022	Steven Johnston	DPIA forum
V0.1	13/12/2022	Will McLoughlin / Steven Johnston	Project team responses added to 5.0, Sections 6.0 and 7.0 completed, Appendix 3 updated.
V0.2	19/09/2023	Will McLoughlin / Kate Range / Steven Johnston	Reviewed and updated to incorporate renewed Microsoft Terms and additional legal advice agreed by Kate Range – Head of Legal Services.
V1.0	22/09/2023	Mike Fitzgerald	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: 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 M365 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 M365 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 specific 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	N/A
Exchange*	Y	N	*Hybrid configuration: On Cloud side various Mail flow rules, alerts, cloud message recall configured.
Forms	Y	N	N/A
Kaizala	N	N	N/A

Lists	Y	N	N/A
OneDrive	Y	0097 - Core cloud - One Drive - DPIA.docx	N/A
OneNote	Y	N	N/A
Outlook	Y	N	N/A
People	Y	N	N/A
Planner	Y	N	N/A
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.
Power Virtual Agents	N	N	N/A
PowerPoint	Y	N	N/A
Project	Y	N	N/A

SharePoint	Y	Intranet Upgrade Data Protection Impact Assessment v0.2.docx	Group based permissions management, retention labelling.
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	N/A
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	N/A
Visio	Y	N	N/A
Viva Connections	N	N	N/A
Viva Engage	Y	N	Disabled upload of non-image file formats
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	N/A
Word	Y	N	N/A