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Document Status (draft, published or superseded)	Draft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

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).

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

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

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

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/

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.

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.

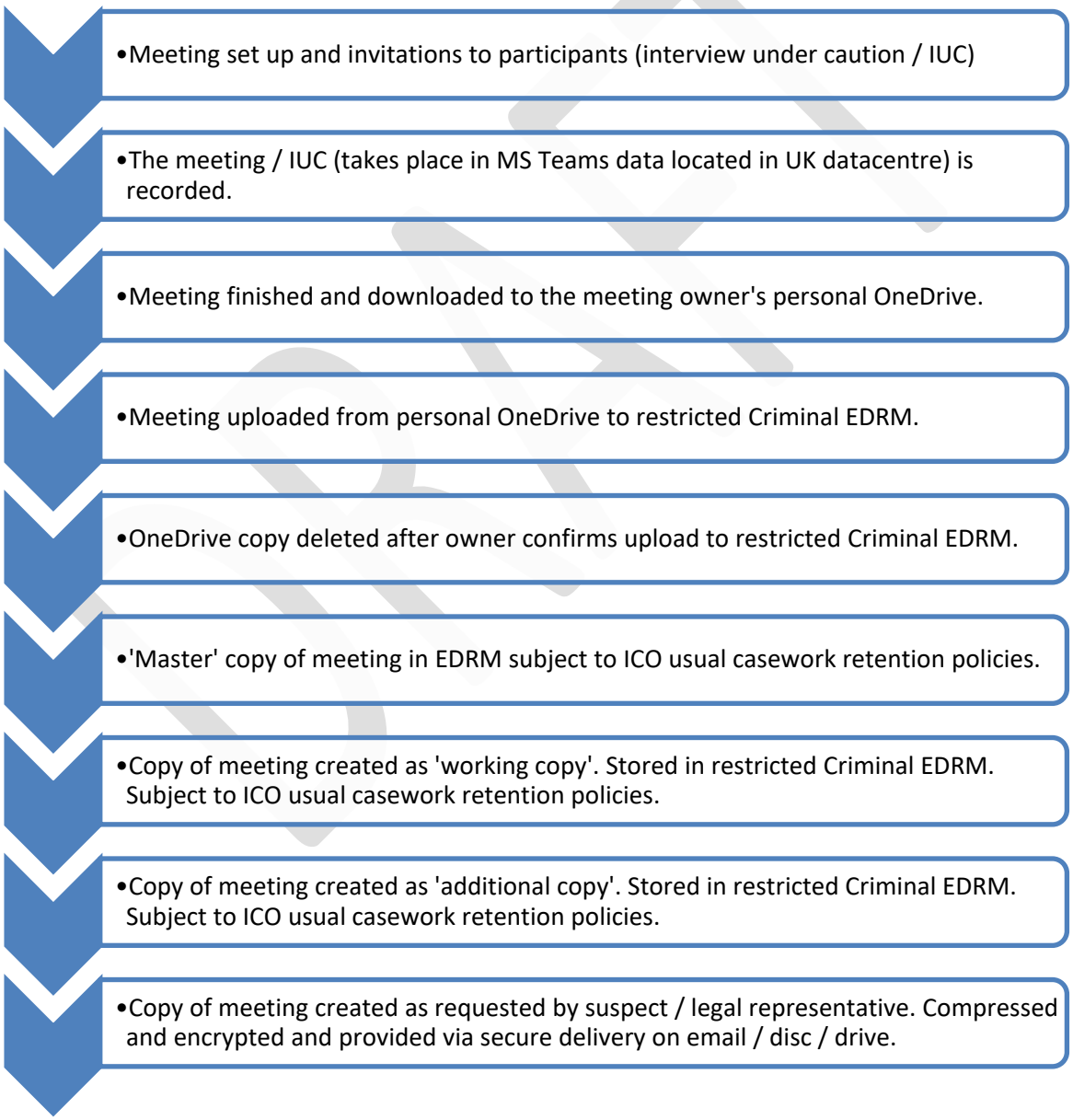
2.0 Data flows

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.

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.

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 ☐

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	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

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

		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			

		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.	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**

	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

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

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.

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.).

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 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.

- 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