Template for a Memorandum of Understanding

[Insert OGD/ Public Authority Logo here]



 **MEMORANDUM OF UNDERSTANDING (MoU)**

**BETWEEN**

**[Insert name of Other Government Department (OGD)/ Public Body/External Organisation]**

**AND**

**THE HOME OFFICE/ POLICE SERVICE**

**Contents**

|  |  |  |
| --- | --- | --- |
| **Paragraph Number** | **Title of Paragraph**  | **Page Number** (To insert once the final document is ready) |
| **1** | Participants to the MoU  |  |
| **2** | Introduction and functions of each Participant to the MoU  |  |
| **3** | Formalities  |  |
| **4** | Legal considerations and basis to share data between the Participants |  |
| **5** | Purpose and benefits of the data sharing |  |
| **6** | Subject Access Requests (SAR) and Freedom of Information Act (FoIA) Requests |  |
| **7** | Handling of Personal Data and Data Security |  |
| **8** | Data to be shared and the systems the data will be derived from |  |
| **9** | Type of data share |  |
| **10** | Description of how the data sharing will occur |  |
| **11** | Retention and Destruction Schedule  |  |
| **12** | Permitted uses of the data in respect of this MoU |  |
| **13** | Onward disclosure to third parties |  |
| **14** | Roles of each Participant to the MoU |  |
| **15** | Accuracy of the shared data  |  |
| **16** | Arrangements for notifying the other Participant of inaccuracies during the data sharing process |  |
| **17** | Monitoring and reviewing arrangements |  |
| **18**  | Issues, Disputes and Resolution  |  |
| **19** | Costs  |  |
| **20**  | Termination |  |
| **21** | Security Breaches, Security Incidents or loss or unauthorised disclosures of data  |  |
| **22** | Signatories |  |
| **Annex A**  | Document Control |  |
| **Annex B**  | Business Contacts  |  |
| **Annex C** | Information Assurance Top Tips for Handling Personal Data |  |
| **Annex D**  | Glossary of terms and abbreviations |  |

N.B: All grey text is for guidance purposes to help you complete the MoU. Before you finalise the MoU, all blue text must be deleted.

All text in black is pre-populated. If the OGD/External organisations require changes to these sections, please seek advice from the Data Sharing and Protocols Team (DSPT)

**1. Participants to the MoU**

Who are the Participants to the MoU?

Please update 1) and 2) below. In addition to the Departmental information you must also provide details of the respective business units responsible for delivering the information sharing activity described in the MoU.

1) **THE SECRETARY OF STATE FOR THE HOME DEPARTMENT** of 2 Marsham Street, London, SW1P 4DF, the “**Home Office[[1]](#footnote-1)” specifically [Insert name of specific Home Office business unit entering into the data sharing arrangement]** hereafter referred to as (**Insert abbreviation for specific department here]** throughout this document.

2) **[Enter the name and registered address of the OGD/External Organisation]** hereafter referred to as **[insert abbreviation for OGD/External Organisation here]** throughout this document**.**

Collectively the Home Office and **[Insert OGD/External Organisation here]** are referred to as the “Participant(s)**”.**

**2. Introduction and functions of each Participant to the MoU**

Sections 2.1-2 3 are pre-populated so you do not need to amend these sections.

2.1 This MoU sets out the information sharing arrangement between the aforementioned Participants. For the context of this MoU ‘information’ is defined as a collective set of Data[[2]](#footnote-2) and/or facts that when shared between the Participants through this MoU will support the Participants in delivering the Purpose of the data sharing activity described in section 5 below.

2.2 This MoU is not intended to be legally binding. It documents the respective roles, processes, procedures and agreements reached between the Home Office and **[Insert OGD/External Organisation**. This MoU should not be interpreted as removing, or reducing, existing legal obligations or responsibilities of each Participant, for example as data controllers under the Data Protection Act 1998 (DPA).

2.3 A glossary of terms, definitions of abbreviations and rules of interpretation of this MoU are detailed in Annex D of this MoU.

***Role of Home Office* (**Enter name of specific business unit entering into the data sharing arrangement, this should replicate the details provided at Section 1) above.)

2.4 Enter a high level summary of the functions of the specific Home Office business unit here.

***Role of OGD/External Organisation***

2.5 **[OGD/External Organisation–** [enter a high level summary of the functions of the OGD/External Organisation here]

**3. Formalities**

Date MoU comes into effect

This will be the date that the MoU is signed by both Participants.

3.1 This MoU will come into effect on **[Insert date here].**

Date of review

This will be the date that both Participants have agreed for a review of the MoU. Generally all regular exchanges are subject to an annual review as a minimum and the review date will be one year from the date the MoU is signed by both Participants. One-off data exchanges are not subject to a review but may be evaluated to establish whether there are any benefits in sharing the data on a regular basis and this should be specified in the MoU here.

Choose one of the following options depending on whether this is a regular or one-off data sharing exercise.

3.2 The date of the review of this MoU is **[Insert date here**].

Or

3.2 This procedure relates to a one-off data sharing exercise (please see section 9 for further information on one-off exchanges). Once completed, it will be evaluated in order to establish whether there are any benefits in sharing the data on a more regular basis.

**4. Legal considerations and basis to share data between the Participants**

4.1 Data can only be shared where there is a legal basis for the exchange and for the purposes described in this MoU as specified at Section 5 below. No data should be exchanged without a legal basis and all exchanges must comply with our legal obligations under both the DPA and Human Rights Act (HRA) 1998.

Describe the legal basis/bases or legal powers of the disclosing Participant to share data; if the exchange is reciprocal the powers of the receiving should be included, for example, the source of such legal basis/bases or legal powers may be a statutory obligation, a statutory power, an implied statutory power or in respect of the Home Office (as a government department headed by a Crown Minister), Common law may be relied upon.

Statutory Obligations – Occasionally, a public body will be legally obliged to share particular data with a named organisation. This will only be the case in specific circumstances but, where such an obligation applies, it is clearly permissible to share the data.

Statutory Powers – Sometimes, a public body will have a statutory power to share or receive data. A statutory power will often be designed to allow/ permit or in some instances compel data sharing to take place

(Permissive power) rather than compel (coercive power) the disclosure of data for specific purposes. Statutory obligations and powers to share data are often referred to as “gateways”.

Implied power – Where there is an implied power to share data. The data in question must be directly linked in support of a statutory obligation or function of one or other Participant.

Common Law Applies to Crown Departments only and where there is no statutory gateway, but the public interest in sharing data outweighs Department’s duty of confidentiality. To share data under Common Law it must be in support of a statutory obligation or function of one or the other Participant.

DPA Exemptions - all instances of data sharing must have a lawful basis (see above) as required by the first data protection principle of the DPA, except where an exemption to that requirement exists. There a number of DPA exemptions from the requirement to comply with the first data protection principle and the requirement for a legal basis for the data sharing to take place, for example, the DPA deals with several situations in which personal data is processed for “crime and taxation purposes” under Section 29 DPA exemption. Section 29 permits data sharing to take place on a case-by-case basis or for specific instances of one–off disclosures and should not be relied upon for large scale data sharing. The data controller still needs to have a valid condition under Schedule 2 of the DPA for processing the data, and a further condition under Schedule 3 for sensitive personal data. Further guidance on Schedule 2 and Schedule 3 can be accessed via the following link to the gov.uk website: [http://www.legislation.gov.uk/ukpga/1998/29/schedule/3](http://www.legislation.gov.uk/ukpga/1998/29/schedule/3%20%20)

4.2 Home Office

Enter relevant Home Office legal basis/bases to share data here.

4.3 Insert **OGD/External Organisation**

Enter relevant OGD/External Organisation legal basis/bases to share data here

**5. Purpose and benefits of the data sharing**

**5.1 Purpose**

This information sharing agreement will help to identify [e.g. criminal activity] with false identity documents. This will prevent persons form using these documents to:

* gain by employment possibly with vulnerable adults or children by fraudulent representation in breach of the Fraud Act 2006;
* commit offences under the Identity Documents Act 2010;
* use fraudulently obtained genuine documents to commit Fraud and other related offences; and
* work or rent accommodation while unlawfully in the UK.

**5.2 Benefits to 1st party**

The benefits to the 1st party are as follows:

[For example]

* Crime, disorder, vulnerability and harm are prevented, disrupted and reduced;
* Improvement in security;
* Improvement in public confidence;
* Offenders are identified and brought to justice; and/ or
* Immigration abuses are tackled.

 **5.3 Benefits to 2nd party**

The benefits to 2nd party are:

[For example]

* Improvement to security and public reassurance;
* Assisting with the detection of crime;
* Reduced economic loss;
* Reduced crime; and/ or
* reduced illegal migration.

**5.4 Citizen Benefits**

[For example]

* Ensuring the integrity of systems;
* Ensuring the integrity of the criminal justice system by showing the public that criminal offences and serious breaches of trust are identified, investigated and prosecuted giving full consideration as to whether criminal proceedings are necessary;
* Ensuring the prevention and detection of crimes.

**5.5 How will this information sharing arrangement further those purposes?**

[For example]

This arrangement will ensure that possible offenders who use forged, fraudulent and FOG identity documents to commit criminal offences are identified at the earliest possible opportunity, thus preventing them from causing harm to individuals and systems.

The information can be matched and potential abusers of systems identified and investigated and subsequently prosecuted/disrupted.

The sharing will detect a number of criminal offences i.e. S2 Fraud Act by False Representation, S3 Fraud Act of failing to disclose information, S4 Abuse of position and S6 Possession of an article for use in Fraud, that have been committed and will detect and disrupt future offences. This will reduce the risk of harm against individuals and financial companies.

This arrangement is necessary to provide an accountable management process to enable the partners in this information sharing agreement to distribute personal material in a lawful and proportionate manner. This agreement will establish the lawful purpose for the sharing of information and establish by which it will be defined.

The two-way sharing of Information between xx and xy will present opportunities to identify people who present a clear and present risk to the Public.

**6. Subject Access Requests (SARs) and Freedom of Information Act (FoIA) Requests**

Sections 6.1-6.5 are pre-populated so you do not need to amend these sections.

SARs for information held by receiving Participant

6.1 In the event that a SAR is received and only relates to personal information held by the receiving Participant; the receiving Participant will issue a formal response following their internal process and procedures for responding to the SAR within the statutory timescales.

SARs for information held in part by the receiving Participant

6.2 Where it is identified that the receiving Participant does not hold all the information requested; they are only expected to disclose the information they have available, in accordance with their obligations under the DPA. There is no statutory requirement to re-direct SARs or provide details other Participant in the response.

Freedom of Information Act 2000 (FoIA) Requests for information held by receiving Participant

6.3 In the event that a FoIA request is received and only relates to information held by the receiving Participant; it will issue a formal response following their internal process and procedures for responding to FoIA requests within the statutory timescales.

FoIA requests for information held by other Participant

6.4 Where it is identified that the FoIA request (in its entirety) relates to information held by the other Participant to this MoU; the receiving Participant will issue a formal response informing the requester that the information requested is held by the Participant and provide the contact details (See Annex B) for the Participant in their response.

Cross Government FoIA Requests

6.5 Where it is identified that a FoIA request relates to information held in part by both Participants to the MoU, the department in receipt of the FoIA request will notify the other to allow it the opportunity to make representations on the potential impact of disclosure. Both Participants shall also assist each other generally as regards the handling of the FoIA.

**7. Handling of Personal Data and Data Security**

Sections 7.1 –7.3 are pre-populated so you do not need to amend these sections.

7.1 Where Participants bear the responsibility of a Data Controller, they must ensure that any personal data received pursuant to this MoU is handled and processed in accordance with the current eight DPA principles (the eight DPA Principles can be accessed through the following link: <https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/>.

7.2 **[Where appropriate**] Additionally as part of the Government, **[insert OGD/External Organisation]** and the Home Office must process personal data in compliance with both the mandatory requirements set out in Information Assurance Top Tips for Handling Personal Data (Annex C) which has replaced the Information Assurance Standard 6 guidance and the Her Majesty’s Government Security Policy Framework (HMG SPF) guidance issued by the Cabinet Office (HMG SPF guidance document when handling, transferring, storing, accessing or destroying Information assets. This guidance can be accessed via the following link:

<https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework>)

7.3 Participants must ensure effective measures are in place to protect personal data in their care and manage potential or actual incidents of loss of the personal data. Such measures will include, but are not limited to:

* personal data should not be transferred or stored on any type of portable device unless absolutely necessary, and if so, it must be encrypted and password protected to an agreed standard;
* Participants will take steps to ensure that all staff are adequately trained and are aware of their responsibilities under the DPA and this MoU;
* access to personal data received by Participants pursuant to this MoU must be restricted to personnel on a legitimate need-to-know basis, and with security clearance at the appropriate level and
* Participants will comply with the Government Security Classifications Policy (GSCP) where applicable.The link to GSCP is provided below: <https://www.gov.uk/government/publications/government-security-classifications>

**8. Data to be shared and the systems the data will be derived from**

Insert a full description of the categories/ cohort/ type of data to be disclosed by each Participant e.g. absconder, asylum seeker, UK passport holder etc.

State the precise fields of data e.g. name, DOB etc, including the source of the data (i.e. from which systems, databases, the data is being extracted e.g. CID, CRS, PNC etc). For each item of data show that it is necessary to share the data in order to support the objectives of the data sharing arrangement e.g. it is necessary to share name, DOB and address to initially match the data (with the other Participant) to confirm identity; it is then necessary to share employment details to establish instances of illegal working.

The proposed volume and frequency of the flow of data sharing should also be included here, i.e. case-by case, monthly, quarterly or ad-hoc exchange.

**9. Type of data share**

State whether the data share relates to a One-off or Regular/Routine data share.

A One-off exchange can relate to a ‘pilot’ exercise, ‘proof of concept’ (PoC) or simply a one- off exchange for a specific purpose.

A Pilot exercise is generally proposed when an organisation would like to test the effectiveness of a new agreed business proposal, but where there is an intention to make the exchange a regular one.

A Proof of Concept (PoC) is generally proposed to test an idea/method to demonstrate its feasibility.

A Regular/Routine data share relates to data sharing exchanges that are expected to occur on a regular basis for a specific purpose. This type of exchange can occur as an initial one-off data share followed by a regular data share for the same purpose i.e. when a department decides to share a data set of historic cases followed by the sharing of data on live/current cases.

**10. Description of how the data sharing will occur**

This section requires a clear and concise account of the process to be followed by staff involved in delivering the data sharing arrangement described in the MoU. Please make sure you address the following points:

Provide a description of the particular means of access or transfer of data between the departments for the data sharing arrangement, i.e. electronically or physically. The guidance below relates to the movement of OFFICIAL and OFFICIAL- SENSITIVE data by both physical and electronic means. Please detail which will be the primary method of data transfer.

 Physically

Data will be moved by a trusted person in a closed container or package.

Data will be moved by post or courier in a sealed package with no security markings showing (other than PERSONAL or PRIVATE). It will be addressed to a specified individual within the partner organisation by name or appointment (add job title).

Data should not be transferred or stored on any type of portable device unless absolutely necessary, and if so, it must be encrypted and password protected to an agreed standard.

Electronically

Protectively marked data up to the level of OFFICIAL and OFFICIAL- SENSITIVE must be transferred using secure email. (Please note email addresses ending in .gov.uk nhs.uk are not secure. Examples of secure email are: .pnn, .gsi, .cjsm and nhs.net).

Avoid the use of fax for transferring protectively marked data as it is not particularly secure, however if sharing data by fax, ensure all appropriate protocols for secure transmission are followed.

Provide the format, in which the data will be shared, e.g. excel spreadsheet or a report formatted in word.

Provide any agreed designated points of contact for each department for receiving and sending the data where applicable.

Also include the Government Security Classification of the data being shared. This guidance is correct for OFFICIAL (including OFFICIAL -SENSITIVE) data under the Government Security Classification Scheme. In the event that there is a requirement to share data of a higher classification marking, please refer to the Government Security Classification Policy (GSCP). OFFICIAL-SENSITIVE marked data may require additional handling instructions, the handling instructions should be advised by the Information Asset Owner (IAO) of the data.

In the case of direct access to the disclosing Participant’s data systems, a process for auditing access must be incorporated into the MoU; the (IAO) of the system in question can advise on conducting audits.

**11. Retention and Destruction Schedule**

State how long the data will be retained for and the arrangements for secure storage and destruction of the data. This may be different for one-off exchanges as opposed to ongoing routine ones as the intention may be to destroy all data at the end of the one-off exercise if the ultimate purpose of the exchange has been achieved i.e. if it is a PoC exercise only.

For ongoing exchanges it is acceptable to state that data will be held in line with existing departmental retention and disposal policies, if that is the case. You should include the justification for retaining the data; i.e. for a specific period of time linked to a legislative requirement, or is outside existing departmental policies.

Where it is anticipated that the particular issue that the data sharing was intended to deal with will be resolved in a short period of time, and there is no requirement to retain the data for another purpose or where there is no expectation to process the data further, a shorter retention period s for the data being shared should be agreed and justified between the organisations at the outset. All the organisations involved in the data sharing should then delete their copies of the information at the end of that agreed period.

You should also include the justification for retaining the data in instances where it is being retained for a particularly long period of time; i.e. for a specific period of time linked to a legislative requirement, or is outside existing departmental policies

**12. Permitted uses of the data in respect of this MoU**

State who will have access to the data being shared and confirm whether they have the appropriate security clearance to handle/access the data for example:

Access will only be permitted to authorised personnel from [Insert OGD/External Organisation] and Home Office who have:

the appropriate security clearance determined by their own department to handle the data and

a genuine business need to access the data.

**13. Onward Disclosure to third parties**

Only complete where routine onward disclosure to third parties is explicitly intended by either Participant.

The section should articulate any arrangements necessary to ensure that this takes place in accordance with both Participants’ legal obligations.

Outline the arrangements for notifying the original source of the data where an unplanned or ad-hoc secondary disclosure of the data has taken place by the recipient.

The MoU should also put in place reporting arrangements for any security incidents that involve exported data after onward disclosure.

This section may include arrangements whereby one Participant is employing a Data Processor who will be directly involved (including as a recipient of any or all of the data exchanged) with any part of the data sharing activity.

**14. Roles of each Participant to the MoU**

14.1 Role of Home Office/ Police

Summarise the main roles and responsibilities of the Home Office/ Police to the MoU; the following is the minimum expected of the Home Office, but can be added to as necessary:

Identify the appropriate data required to make the search from Home Office immigration IT systems;

Provide the data to [**insert OGD/External Organisation]** in **[agreed format]** transferred by secure **[describe method]** from and to agreed contact points;

Only allow access to that data by the team carrying out the matching;

Ensure that staff handle this data in line with the approved secure transfer method agreed by both departments and within Home Office data security instructions;

Only store the data for as long as it there is a business need to do so;

Any queries can be raised by emailing the designated points of contact for **[insert OGD/External Organisation]** at Annex B.

14.2 Role of **[insert OGD/External Organisation]**

Summarise the main roles and responsibilities of the OGD/External Organisation to the MoU; the following is minimum expected of the OGD/External Organisation, but can be added to as necessary.

Identify the appropriate data required to make the search from **[Insert OGD/External Organisation]** records;

On receipt, move the data received from the Home Office into a secure folder with the appropriate restricted access;

Only allow access to that data by the team carrying out the matching;

Ensure that staff handle this data in line with the approved secure transfer method agreed by both departments and within Home Office data security instructions

Send the data in **[agreed format]** via secure **[describe method**] agreed by both departments under the protective marking ‘Official Marked/Official-Sensitive’ where applicable;

Only store the data for as long as it there is a business need to do so;

Any queries can be raised by emailing the designated points of contact for **[insert OGD/External Organisation]** at Annex B.

**15. Accuracy of the shared data**

*Sections 15.1 –15.2 are pre-populated so you do not need to amend these sections*

15.1 Before sharing data both Participants must take all reasonable steps to ensure that the data being shared is both accurate and up-to-date in accordance with the fourth data protection principle.

15.2 In circumstances where the recipient of the data is intending to use the data to make a decision that will impact directly on the data subject, the receiving Participantmust be satisfied that there is sufficient and accurate information available to them before making a final decision and should always seek to clarify, or make further enquiries with the data subject, or with the disclosing Participant in the event that decision is subsequently disputed/appealed by the data subject.

**16. Arrangements for notifying the other Participant of inaccuracies during the data sharing process**

Data shared between Participants should be subject to procedures and validations intended to ensure data quality

State here what arrangements the disclosing Participant has put in place to ensure data quality of the data it intends to share at the point of transfer to the other Participant i.e. bulk data transfers should undergo a validation check to ensure that the data being transferred is in the correct format and meets the business specification.

You should also provide arrangements for notifying the receiving Participant of any inaccuracies and the timescales of when the error will be notified to the receiving Participant i.e. the disclosing Participant will notify the receiving Participant of any errors within one working day of discovery to the designated points of contact for this data sharing arrangement.

You should also state the arrangement for rectifying such errors of the data, i.e. incorrect data will be confirmed and rectified within 5 working days.

**17. Monitoring and reviewing arrangements**

Choose one of the following options to which the data sharing applies**:**

Option one: Regular/Routine Exchanges

17.1 This MoU relates to a regular exchange and will run indefinitely, but must be reviewed at least annually to assess whether the MoU is still accurate and fit for purpose.

17.2 Reviews outside of the proposed annual review can be called by representatives of either Participant. Any changes needed as a result of that review may be agreed in writing and appended to this document for inclusion at the formal annual review.

17.3 Technical changes necessary to improve the efficiency of the exchange that do not change the overarching purpose can be made without the requirement to review formerly the MoU during its life cycle but must be incorporated at the formal review stage.

17.4 A record of all reviews will be created and retained by each Participant.

17.5 Annex B outlines the contacts for amendments to the MoU. Annex A set out the document control, and the version history of the MoU.

Or

Option two: One-off, PoC or Pilot exchanges

17.1 This MoU relates to a one-off data sharing exchange and will be reviewed after the initial data sharing has been completed. Both Participants will then decide whether a more regular data sharing arrangement would be beneficial, in which case a new MoU will be required.

17.2 Annex B outlines the contacts for amendments to the MoU. Annex B set out the document control, and the version history of the MoU.

**18. Issues, disputes and resolution**

Sections 18.1–18.2 are pre-populated so you do not need to amend these sections.

18.1 Any issues or disputes that arise as a result of exchange covered by this MoU must be directed to the relevant contact points listed in Annex B. Each Participant will be responsible for escalating the issue as necessary within their given commands.

18.2 Where a problem arises it should be reported as soon as possible. Should the problem be of an urgent nature, it must be reported by phone immediately to the designated business as usual contact (listed in annex B) and followed up in writing the same day. If the problem is not of an urgent nature it can be reported in writing within 24 hours of the problem occurring.

**19. Costs**

State whether there will be any charges made to one Participant by the other as a direct result of this MoU. If there are no charges this should be stated here.

**20. Termination**

If the data sharing arrangement relates to a one-off exercise, select Option one.

If the data sharing arrangement relates to a regular exchange, select Option two.

Option one

20.1 This data sharing arrangement relates to a one- off exchange and will terminate upon completion of the data sharing exercise or within 14 days notice to the other in the following circumstances:

by reason of cost, resources or other factors beyond the control of the Home Office or **[insert OGD/External Organisation];**

if any material change occurs which, in the opinion of the Home Office and **[insert OGD/External Organisation**] following negotiation significantly impairs the value of the data sharing arrangement in meeting their respective objectives.

*Option two*

20.1 This MoU may be terminated by giving three months notice by either Participant.

20.2 Both Participants to this MoU reserve the right to terminate this MoU with three months notice in the following circumstances:

by reason of cost, resources or other factors beyond the control of the Home Office or **[insert OGD/External Organisation];**

if any material change occurs which, in the opinion of the Home Office and **[insert OGD/External Organisation)** following negotiation significantly impairs the value of the data sharing arrangement in meeting their respective objectives.

Section 20.3 below to amend this section is pre–populated so you do not need this section.

 20.3 In the event of a significant security breach or other serious breach of the terms of this MoU by either Participant the MoU will be terminated or suspended immediately without notice.

**21. Security Breaches, Security Incidents or loss or unauthorised disclosures of data**

Sections 21.1 21.6 are pre-populated so you do not need to amend these sections.

21.1 A security breach is a situation where the rules on handling and protecting information or equipment have been broken.

21.2 A security incident is a situation which results in the loss or theft of, or unauthorised access to, Home Office information or equipment.

21.3 Examples of serious security breaches, incidents, loss or unauthorised disclosure may include:

* accidental loss or damage to information;
* damage or loss of information by means of malicious software/hacking
* deliberate or knowingly disclosure of information to a person not entitled to receive the information; emailing classified/sensitive information to personal email accounts;
* leaving classified/sensitive papers in a unsecure or publicly accessible area;
* using social networking sites to publish information which may bring either Participant’s organisations into disrepute; and
* Direct access-inappropriately looking up or accessing data.

21.4 The designated points of contact (provided at Annex B of this MoU) are responsible for notifying the other Participant in writing in the event of loss or unauthorised disclosures of information within 24 hours of the event.

21.5 The designated points of contact will discuss and agree the next steps relating to the incident, taking specialist advice where appropriate. Such arrangements will include (but will not be limited to) containment of the incident and mitigation of any ongoing risk, recovery of the information, and notifying the Information Commissioner and the data subjects. The arrangements may vary in each case, depending on the sensitivity of the information and the nature of the loss or unauthorised disclosure.

21.6 Where appropriate and if relevant to the incident, disciplinary misconduct action and/or criminal proceedings will be considered.

**22 Signatories**

The final document must be signed and dated by the relevant information asset owner (IAOs) responsible for the data sharing activity. In the Home Office this is usually a Grade 5 or the Director for the business area. If necessary the IAO can nominate a delegate to sign the MoU on their behalf but understand that they will retain overall responsibility for the data sharing activity.

22.1 Signed on behalf of the Home Office:

I accept the terms of the Memorandum of Understanding on behalf of the Home Office.

|  |  |
| --- | --- |
| Signature: |  |
| Name: |  |
| Date: |  |
| Position: |  |

22.2 Signed on behalf of **[Insert OGD/External Organisation]**

I accept the terms of the Memorandum of Understanding on behalf of **[Insert OGD/External Organisation**

|  |  |
| --- | --- |
| Signature: |  |
| Name: |  |
| Date: |  |
| Position: |  |

**Annex A- Document Control**

Document Control Personnel

|  |  |  |
| --- | --- | --- |
| **Key personnel** | **Name** | **Organisation (Team)** |
| **Author** | Insert name and position here Insert name and position here  | Home Office Insert OGD/External Organisation  |
| **Approver** | Insert name and position here Insert name and position here  | Home OfficeInsert OGD/External Organisation |
| **Review Control** | Insert name and position here Insert name and position here  | Home OfficeInsert OGD/External Organisation |

Version and review history

|  |  |  |  |
| --- | --- | --- | --- |
| **Version/ review** | **Date** | **Summary of changes** | **Changes marked** |
|  |  |  |  |

**Annex B- Business Contacts**

Business as Usual Contacts –Home Office

|  |  |  |
| --- | --- | --- |
| **Contact** | **Email** | **Responsibility** |
|  Insert name of contact and position | Insert email address of contact | Operational Queries  |
|  Insert name of contact and position | Insert email address of contact | Legal Issues |
|  Insert name of contact and position | Insert email address of contact | Review and amendments to MoU  |
|  Insert name of contact and position | Insert email address of contact | Security Incidents  |
|  Insert name of contact and position | Insert email address of contact | Freedom of Information  |

Business as Usual Contacts – **Insert OGD/External Organisation**

|  |  |  |
| --- | --- | --- |
| **Contact** | **Email** | **Responsibility** |
| Insert name of contact and position | Insert email address of contact | Operational Queries  |
| Insert name of contact and position | Insert email address of contact | Legal Issues |
| Insert name of contact and position | Insert email address of contact | Review and amendments to MoU  |
|  Insert name of contact and position | Insert email address of contact | Security Incidents  |
|  Insert name of contact and position | Insert email address of contact | Freedom of Information  |

Escalation Contacts – Home Office

|  |  |  |
| --- | --- | --- |
| **Contact** | **Email** | **Responsibility** |
|  Insert name of contact and position | Insert email address of contact | Operational Queries  |
|  Insert name of contact and position | Insert email address of contact | Legal Issues |
|  Insert name of contact and position | Insert email address of contact | Review and amendments to MoU  |
|  Insert name of contact and position | Insert email address of contact | Security Incidents  |
|  Insert name of contact and position | Insert email address of contact | Freedom of Information  |

Escalation Contacts – **Insert OGD/External Organisation**

|  |  |  |
| --- | --- | --- |
| **Contact** | **Email** | **Responsibility** |
| Insert name of contact and position | Insert email address of contact | Operational Queries  |
| Insert name of contact and position | Insert email address of contact | Legal Issues |
| Insert name of contact and position | Insert email address of contact | Review and amendments to MoU  |
|  Insert name of contact and position | Insert email address of contact | Security Incidents  |
|  Insert name of contact and position | Insert email address of contact | Freedom of Information  |

1. Home Office – means the functions of Border, Immigration and Passport functions only and not the whole of the Home Office and its Executive Agencies [↑](#footnote-ref-1)
2. All references to Data include Personal Data, Sensitive Personal Data, Non Personal Information, and De-personalised Information. Personal Data As defined by the Data Protection Act 1998:

“Personal data means data which relate to a living individual who can be identified –

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual

and any indication of the intentions of the data controller or any other person in respect of the individual [↑](#footnote-ref-2)