UMBRELLA MEMORANDUM OF UNDERSTANDING (UMOU)

BETWEEN

DEPARTMENT FOR EDUCATION AND

THE HOME OFFICE

In Respect of the Exchange

Of Information

Contents

Participants to the UMoU

1) **THE SECRETARY OF STATE FOR THE HOME DEPARTMENT** of 2 Marsham Street, London, SW1P 4DF hereafter referred to as the "**Home Office[1]"** throughout this document.

2) **THE SECRETARY OF STATE FOR THE DEPARTMENT FOR EDUCATION** of Sanctuary Buildings, Great Smith Street, London, SW1P 3BT hereafter referred to as **"DFE"** throughout this document**.**

1.1 Collectively the Home Office and DfE **are** referred to as "Participants", and individually are referred to as a "Participant."

2. Introduction

2.1 This UMoU sets out the high-level information sharing arrangement between the Home Office and DfE that governs the exchange of information between the Participants. For the context of this UMoU "information" is defined as a collective set of Data[2] and/or facts that when shared between the Participants through this UMoU or any associated purpose-specific information sharing MoUs can support the Participants to better deliver their respective business objectives and/or functions.

2.2 The aim of the UMoU is to set clear guidelines to follow when sharing information and ensuring that information is shared with appropriate safeguards and in accordance with the law.

2.3 This UMoU does not replace any specific Process Level Memoranda of Understandings (PMoUs) proposed and/or in place between DfE and the Home Office, unless specified herein.

Process Level MoUs

2.4 In addition to the UMoU, the Home Office and DfE will approve and sign any specific Process level MoUs (PMoUs) for each purpose specific information sharing activity reached between the Participants. The PMoUs will incorporate the terms of the UMoU and will include the information as set out in Annex B of this document. The PMoUs will be in the form set out in the "Process Level Template" attached to this UMoU. Each PMoU will reference the UMoU as the basis of exchange and must be read in conjunction with the UMoU.

---

[1] Home Office – for the purpose of this UMoU refers to:

- The Border, Immigration and Citizenship functions only and not the whole of the Home Office and its Executive Agencies

[2] All references to Data include Personal Data, Sensitive Personal Data, Non-Personal Information, and de-personalised Information.
"Personal data" as meaning "any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Role of Home Office

2.5 All references to the Home Office in this document refer to the **Border, Immigration and Citizenship functions,** of the Home Office, consisting of the following Home Office Directorate(s):

Border, Immigration and Citizenship

1) **Border Force (BF)**
2) **Immigration Enforcement (IE)**
3) **UK Visas and Immigration (UKVI)**
4) **Her Majesty's Passport Office (HMPO)**

2.6 This is a link to the Home Office website, which provides more information on the role of the Home Office: www.gov.uk/government/organisations/home-office.

Role of DfE

2.7 The DfE is responsible for children's services and education, including higher and further education policy, apprenticeships and wider skills in England. The department is also home to the Government Equalities Office. The DfE works to provide children's services and education that ensure opportunity is equal for all, no matter what their background or family circumstances. For more information, please see the following link:

https://www.gov.uk/government/organisations/department-for-education

2.8 A glossary of terms, abbreviations and definitions is provided at Annex C which equally applies to both the UMoU and PMoU.

3. Formalities

Date UMoU comes into effect

3.1 This UMoU will come into effect on 31st January 2019.

Date of review

3.2 This UMoU will be reviewed on 31st January 2020.

4. Aims and objectives of UMoU

4.1 Organisations which share information, particularly information that involves the sharing of personal data have a legal responsibility to ensure that the disclosure of information is both lawful and subject to adequate controls.

4.2 This UMoU aims to:

- set out the high- level principles that will govern the sharing of information between the Participants including the onward disclosure of personal data to third parties (see section 17);

- describe the processes, structures and roles that will support the exchange of information between DfE and the Home Office;
- set out the legal responsibilities which apply to disclosure and use of personal data having regard to the Data Protection legislation[3];
- describe the data security procedures necessary to ensure compliance with the Data Protection legislation and any other specific security requirements;
- describe the process for managing personal data breaches; and
- describe the process for monitoring and reviewing the use of this UMoU.

5. Legal considerations to share information between the Participants

5.1 Information will only be exchanged in a way which is compliant with the overarching principles of the Data Protection legislation, any statutory data sharing powers and where relevant the Common Law Duty of Confidentiality.

Powers to share information

5.2 Each PMoU will identify the specific statutory powers relied upon for each individual Participant for disclosing, receiving and/or further processing the information.

Lawful basis for processing personal data in accordance with Article 6 of the GDPR

5.3 In accordance with Article 6 of the General Data Protection Regulation (GDPR[4]), each PMoU will identify the lawful basis for disclosing, receiving and/or further processing the information for each Participant. Please see link to ICO Website for information on the Lawful Basis for processing personal data: *https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/#ib3*

6. Privacy Information Notices

6.1 The Participants will ensure that their respective Privacy Information Notices (PINs) are sufficiently detailed to cover the information sharing activity specified in the respective PMoUs, including the purpose of the processing and the lawful basis for the processing.

7. Third Party Processing

7.1 (Where applicable) Each PMoU will identify any instances of third party processing of personal data exchanged as a direct result of this UMoU or any associated PMoUs by either Participant. Where third parties are used, the relevant Participant will confirm that there are arrangements in place to ensure that the third party is compliant with the Data Protection legislation.

[3] In this MoU, "Data Protection Legislation" means the General Data Protection Regulation and the Data Protection Act 2018

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data

8. Data Protection Impact Assessments

8.1 The Participants will ensure that before any information sharing takes place under this UMoU, consideration is given as to whether a Data Protection Impact Assessment (DPIA) should be carried out. This will identify the relevant legal powers and assess the benefits of the information sharing, as well as identifying any privacy risks and how they might be mitigated. The DPIA is mandatory for the Home Office.

9. Controller Status in respect of the Information Sharing

9.1 Each PMoU will identify the Controller status of the receiving Participant(s) in respect of the information sharing i.e. whether the receiving Participants (s) is/are a joint or sole controller of the data received.

10. General Principles

10.1 When completing and implementing the PMoUs, regard must be had to the following:

- the Participants will cooperate in good faith to fulfil the purposes of this UMoU and any PMoUs made under it.
- the Participants will make reasonable endeavours to ensure that the information being shared is checked before disclosure for accuracy and relevance. The disclosing Participant will ensure data integrity meets their standards. In the event that a Participant becomes aware of any inaccuracy or other defect in the information which has been disclosed it will notify the Participants which disclosed it.
- where anonymised information, pseudonymised information or non-personal information is shared, the recipient of that information will not attempt to re-identify any individual by analysing or combining it with other information which is in its possession at the time of receipt or subsequently comes into its possession.
- (only applies where the lawful basis for processing is based on consent) the Participants confirm that they have the technical capability and procedures in place to sufficiently comply with all the data subject's rights under the Data Protection legislation including the technical capability to identify, provide and erase personal data should either Participant be legally required to do so.
- Any personal data shared under this UMoU and any associated PMoUs must be proportionate, necessary and appropriate for the legitimate aim pursued.

11. Freedom of Information Act (FoIA) Requests

11.1 The Participants will demonstrate a commitment to openness and transparency regarding information sharing activities under this UMoU and any associated PMoUs.

11.2 In the event that a FoI request relating to Information sharing activities under this UMoU or any associated PMoUs is received, the Participants accept to consult with the other in line with the Code of Practice made under section 45 of FoIA.

12. Subject Access Requests (SAR)

12.1 Individuals can request a copy of all the information that either Participant holds on them, by making a SAR. This may include information that was disclosed to that Participant under this UMoU or any associated PMoUs. Where this is the case, as a matter of good practice, the Participants will liaise with each other to endeavour to ensure that the release of the information to the individual will not prejudice any ongoing investigation/proceedings.

13. Handling of Personal Data and Personal Data Security

13.1 Participants will be deemed to be Controllers (as defined in the Data Protection legislation) and as such must ensure that information shared that involves the sharing of personal data is handled and processed in accordance with the Data Protection legislation. Additionally, the Participants must process the information being shared in compliance with the mandatory requirements set by Her Majesty's Government Security Policy Framework ("HMG SPF") guidance issued by the Cabinet Office when handling, transferring, storing, accessing or destroying information assets. HMG SPF guidance document can be accessed via the following link: https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework.

13.2 The Participants will ensure effective measures are in place to protect information in their care and manage potential or actual incidents of loss of information. By way of example without limitation, such measures may include:

- information not being transferred or stored on any type of portable device unless necessary, and if so, it must be encrypted, and password protected to an approved standard;
- taking steps to ensure that all relevant staff are adequately trained and are aware of their responsibilities under the Data Protection legislation and this UMoU;
- access to information received by the Participants pursuant to this UMoU must be restricted to employees on a legitimate need-to-know basis, and with security clearance at the appropriate level; and
- the Participants will comply with the Government Security Classifications Policy (GSCP) where applicable: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf

14. Method of information sharing

14.1 Information will be exchanged between Participants in a secure approved format, as approved by all Participants.

14.2 Participants will ensure that all information they transmit to each other will be marked with the appropriate security classification in accordance with the GSCP.

14.3 The method of exchange will be in accordance with the standards and benchmarks relating to the security of that transfer and in accordance with any applicable provisions of the Data Protection legislation, Cabinet Office and other HMG guidance.

15. Retention and destruction schedule

15.1 Participants undertake to keep information being shared securely stored with access restricted to personnel authorised to access the information.

15.2 Participants will have documented polices on the retention and destruction of shared information in accordance with the requirements of the Data Protection legislation and HMG Security Policy Framework. Where specific information sharing activities are entered by the Participants; the retention period should be jointly decided and set out in the respective PMoU for that information sharing activity.

15.3 Where a PMoU has been terminated, the Participants will follow any procedure set out in the PMoU in relation to the handling of information. If no specific provisions are decided, the Participants will co-operate to determine how the information shared between the Participants is handled.

15.4 Participants will retain and securely destroy shared information according to their own internal retention/destruction program/schedule in line with the Data Protection legislation and in accordance with HMG Security Policy Framework guidance.

16. Onward disclosure of information to third parties

16.1 Participants will respect the confidentiality of the information being shared and will not disclose to third parties unless required to do so by law, or with the explicit consent of the other Participant or as stipulated at section 17.3 below.

16.2 Unless otherwise stipulated within this UMoU, any information shared as a result of this UMoU and any associated PMoUs, which then forms part of the permanent record of the receiving Participant(s) becomes the responsibility of the receiving Participant (s) under the terms of the Data Protection legislation.

16.3 Participants accept that the information shared as a result of UMoU and any associated PMoUs may also be used to update their respective internal records. As Controller for that data, the receiving Participant can onwardly disclose the information to third parties (this includes the sharing of Information with external contractors who are acting as Processors as on behalf of the Controller) subject to the following conditions being met:

- the Participant wishing to make the onward disclosure must be satisfied that the information is only shared where it is necessary to carry out one of its own legitimate business functions and due regard must be had to any legal restrictions which may apply;
- the Participant wishing to make onward disclosure must be satisfied that the information is being shared lawfully and in accordance with any legal

obligations that may apply, including those set out in the Data Protection legislation;
- the Participant wishing to make the onward disclosure must be satisfied that adequate security arrangements are in place for the transmission of the data to the receiving Participant and that the receiving Participant has adequate security arrangements in place for the secure storage of the information, and
- a separate formal information sharing agreement should be put in place with the third-party organisation setting out all the above.

17. Data subject complaint resolution procedure/issues, disputes and resolution procedure between Participants

Data Subject Complaint Resolution Procedure

17.1 Complaints about the use of information in relation to this UMoU and any associated PMoUs should be dealt with under the relevant complaints procedure of the Participant whose actions are subject of the complaint.

17.2 Participants accept to co-operate with each other in the investigation of any complaint or other investigation about the use of the information shared.

17.3 The outcome/resolution of any complaint will be notified to the other Participant to this UMoU.

Issues, Disputes and Resolution between Participants Procedure

17.4 Any issues or disputes that arise as a result of exchanges covered by this UMoU or associated PMoUs must be directed to the relevant contact points listed in Annex A or as listed in the relevant PMoU. Each Participant will be responsible for escalating the issue as necessary within their given organisations.

17.5 Where an issue or dispute 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 A) 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.

17.6 Any deviation from this process that is required by either Participant in respect of a particular information sharing activity will be detailed in the relevant PMoU.

18. Monitoring and reviewing arrangements

18.1 The UMoU will run indefinitely but must be reviewed at least annually.

Review process

18.2 The review process will focus on:

- confirming whether the UMoU includes the correct contact details for key personnel;
- whether the UMoU is still necessary and fit for purpose;

- whether the existing information sharing arrangements should be extended or amended; and
- whether the legal bases relied upon by the Participants for sharing the information remain valid, including whether any legislation has been amended or enacted that would impact on any purpose-specific information sharing activities. If a Participant's legal basis for information sharing has changed, the information sharing activity in place may need to be amended to reflect this.

18.3 Any changes needed in the interim may be approved in writing and appended to this document for inclusion at the following review.

18.4 Reviews outside of the approved schedule can be called by representatives of either Participant for example where new or revised legislation or cross-government guidance necessitates an earlier review.

18.5 A record of the review will be created and retained by each Participant.

18.6 Annex D outlines the contacts for document control, the version history of this UMoU and the review dates for it.

Monitoring compliance

18.7 The Participants reserve the right to carry out a review of compliance with the terms of this UMoU and any associated PMoUs and accept to co-operate fully with any such review.

19. Costs

20.1 Participants will pay their own costs and provide adequate resources to perform their activities under this UMoU. There may, however be charges levied in specific information sharing exchanges in relation, for example, to IT development. These will be detailed in the respective PMoU.

20. Termination

20.1 The Participants will have the right to terminate this UMoU by giving three months' notice of termination in writing to the other Participants should the following circumstances arise:

- a material breach by the other Participant of any of the terms of the UMoU;

- by reason of cost, resources or other factors beyond the control of either of the Participants; and/or
- if any material change in circumstances occurs which, following negotiation between the Participants, in the reasonable opinion of either or all of the Participants significantly impairs the value of the UMoU in meeting their objectives.

20.2 Termination of the UMoU will have the effect of automatically making void all PMoUs made under the terms of the UMoU.

20.3 Where a PMoU has been terminated the Participants will follow any procedure set out in the PMoU in relation to the handling of the information shared. If no specific provisions are decided, the Participants will co-operate to determine how the information shared between the Participants is handled.

20.4 In the event of a significant personal data breach or other serious breach of the terms of this UMoU by any of the Participants, this UMoU must be reviewed immediately by the Participants.

20.5 The Participants understand that the provisions of this UMoU will continue to apply to any information previously shared pursuant to this UMoU and any of its PMoUs, notwithstanding the termination of this MoU.

21. Personal Data Breaches

21.1 A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss alteration, unauthorised disclosure of, or access to personal data transmitted stored or otherwise processed.

21.2 Examples of serious personal data breaches may include:

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

21.3 The designated points of contact (provided at Annex A of this UMoU) are responsible for notifying the other Participant in writing in the event of personal data breach within 24 hours of the event.

21.4 The designated points of contact will discuss and jointly decide 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 personal data, and assessing whether the Information Commissioner and/or the data subjects will be notified. The arrangements may vary in each case, depending on the sensitivity of the personal data and the nature of the loss or unauthorised disclosure.

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

22. Signatories

Signed on behalf of the Home Office:

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

Signature:	[redacted]
Name:	[redacted]
Date:	31st January 2019
Position:	[redacted]

Signed on behalf of DfE:

22.2 I accept the terms of the Umbrella Memorandum of Understanding on behalf of DfE.

Signature:	[redacted]
Name:	[redacted]
Date:	31 January 2019
Position:	[redacted]

Annex A - Business Contacts

Business as Usual Contacts - Home Office

Contact	Email	Responsibility
N/A	HomeOfficeCustomerComplaints@homeoffice.gov.uk	Complaints/Issues /Disputes and Resolution
[redacted]	[redacted]@homeoffice.gov.uk	Legal Issues
[redacted]	[redacted]@homeoffice.gov.uk	Freedom of Information
[redacted]	[redacted]@homeoffice.gov.uk	Review and amendments to MoU
HO Security	HOSecurity-DataIncidents@homeoffice.gov.uk	Personal Data Breaches

Business as Usual Contacts – DfE

Contact	Email	Responsibility
[redacted]	[redacted]@education.gov.uk Always copying in Data.sharing@education.gov.uk	Complaints/Issues /Disputes and Resolution
[redacted]	[redacted]@education.gov.uk Always copying in Data.sharing@education.gov.uk	Legal Issues
[redacted]	[redacted]@education.gov.uk Always copying in Data.sharing@education.gov.uk	Freedom of Information
[redacted]	[redacted]@education.gov.uk	Review and amendments to MoU

	Always copying in Data.sharing@education.gov.uk	
[redacted]	[redacted]@education.gov.uk Always copying in Data.sharing@education.gov.uk	Personal Data Breaches

Escalation Contacts – Home Office

Contact	Email	Responsibility
N/A	HomeOfficeCustomerComplaints@homeoffice.gov.uk	Complaints/Issues /Disputes and Resolution
Home Office Legal Advisors Bureau (HOLAB)	To contact [redacted] in the first instance who will consider escalation to HOLAB	Legal
Knowledge and Information Management Unit	Freedom.informationteam@homeoffice.gov.uk	Freedom of Information
[redacted]	[redacted]@homeoffice.gov.uk	Review and amendments to MoU
Home Office Security	HOSecurity-DataIncidents@homeoffice.gov.uk	Personal Data Breaches

Escalation Contacts – DfE

Contact	Email	Responsibility
[redacted]	[redacted]@education.gov.uk	Complaints/Issues /Disputes and Resolution
[redacted]	[redacted]@education.gov.uk copying in Data.sharing@education.gov.uk	Legal
[redacted]	[redacted]@education.gov.uk	Freedom of Information
[redacted]	[redacted]@education.gov.uk	Review and amendments to MoU
[redacted]	[redacted]@education.gov.uk	Personal Data Breaches

Annex B - Information exchange specific (process-level) MoUs

As a minimum all PMoUs should include:

- the purpose of the exchange;
- the physical method of exchange;
- the benefit of the exchange;
- the method by which the information shared is to be handled and kept secure by the recipient;
- the legal powers relied upon for the specific PMoU;
- the lawful basis for processing personal data;
- the fiscal cost (if appropriate);
- confirm if a PIN is in place that sufficiently covers the information sharing activity;
- confirm if DPIA has been carried out;
- the roles and responsibilities of the Participants including (if appropriate) which Participant(s) will act as a Controller or Processer; and
- a formal review date.

Where onward disclosure is envisaged, the PMoU should put in place any arrangements necessary to ensure that this occurs in accordance with the Participants' legal obligations. The PMoU should also detail reporting arrangements for any security incidents that involve exported information after onward disclosure.

Annex C - Glossary of terms, abbreviations and definitions

In this MoU the following words and phrases will have the following meanings, unless expressly stated to the contrary:

Definition	Interpretation
Controller	Has the same meaning as defined in the Data Protection Legislation, that is, the person who determines the manner in which and purposes for which personal data are to be processed either alone or jointly in common with other persons.
Processor	Has the same meaning as defined as Processor or Data Processor in the Data Protection Legislation, that is, any person who processes personal data on behalf of the Controller (other than an employee).
Data Protection Legislation	Means the General Data Protection Regulations (GDPR) and the Data Protection Act.
Guidance	(where applicable) the guidance and codes of practice issued by the Information Commissioner.
Law	means any applicable law, statute, byelaw, regulation, order.
Policy/rule of court etc	regulatory policy, guidance or industry code, rule of court or directives or requirements of any Regulatory Body, delegated or subordinate legislation or notice of any Regulatory Body.
Participants	Means Participants to this UMoU and refers explicitly to the Home Office and DfE
Data Subject	Has the same meaning as defined in the Data Protection Legislation, being an identified or identifiable natural person who is the subject of personal data.
Personal Data	Personal data means any information relating to a data subject who can be identified from it or data that can be put together with other information to identify a living individual. It covers data held in any format.
Data Protection Impact Assessment (DPIA)	A tool that can be used to identify and reduce the privacy risks of any activity where personal data is processed (including Information Sharing).
General Data Protection Regulation (GDPR)	Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

Privacy Information Notice (PIN)	A Privacy Information Notice is a publicly available statement or document that sets out some or all of the ways a party gathers, uses, discloses, and manages a customer or client's data. It fulfils a legal requirement to protect a customer or client's privacy.
Non–Personal Information	Information that has never referred to an individual and cannot be connected to an individual.
Information	Information is defined as a collective set of Data[5] and/or facts that when shared between the Participants through this UMoU or any associated purpose-specific data sharing MoUs can support the Participants to better deliver their respective business objectives and/or functions, it includes personal data, sensitive personal data, non-personal Information and de-personalised Information.
Process/Processed/ Processing	Have the same meaning as defined in the Data Protection Legislation and includes collecting, recording, storing, retrieving, amending or altering, disclosing, deleting, archiving and destroying personal data.
Umbrella MoU (UMoU)	These documents are used when entering into an information sharing activity with another government department where the intention/ expectation is that there will be a regular or significant amount of information sharing taking place involving personal data. The UMoU sets out the overarching principles of information sharing between the Participants.
Process MoU (PMoU)	Home Office terminology. A process MoU is approved and signed by the Home Office and DfE for each category of data which will be shared or for each purpose-specific information sharing activity and is in the format set out in the PMoU Template attached to the UMoU.

Annex D Document Control

Document Control Personnel

Key personnel	Name	Organisation (Team)
Author	[redacted]	Home Office
	[redacted]	Home Office
Approver	[redacted]	Home Office
	[redacted]	DfE
Review Control	[redacted]	Home Office
	[redacted]	DfE

Version and review History

Version/ review	Date	Summary of changes	Changes marked
Final V1	31.01.19	Umbrella MOU created setting out the high-level information sharing arrangement between the Home Office and DfE that governs the exchange of information between the Participants	No

PROCESS LEVEL MEMORANDUM OF UNDERSTANDING (PMoU)

BETWEEN

DEPARTMENT FOR EDUCATION AND

THE HOME OFFICE

In respect of the exchange of information

Contents

1. Introduction and Participants to the PMoU

1.1 This is a PMoU made under the terms of the overarching UMoU between the **Department for Education** and the **Home Office**. Any information shared pursuant to this PMoU is subject to the provisions set out in the UMoU between the Home Office and the Department for Education including any conditions set out therein and this PMoU should therefore be read in conjunction with the UMoU.

1.2 This PMoU shall be entered into by the National Pupil Database and Data Sharing Team on behalf of the Department for Education and Returns Preparation Team on behalf of the Home Office who are responsible for the purpose-specific information sharing activity to which this PMoU relates.

1.3 Hereafter the Department for Education will be referred to as "DfE" and Home Office will be referred to as "HO" throughout this document.

1.4 Collectively the HO and DfE are referred to as 'Participants', and individually are referred to as a "Participant."

2. Formalities

Date PMoU comes into effect

2.1 This PMoU will come into effect on 31st January 2019.

Date of review

2.2 The date of the review of this PMoU is 31st January 2020.

3. Powers to share personal data between the Participants

3.1 The relevant legal bases to share information involving personal data between the Participants are set out below.

Home Office

3.2 As part of the Crown, the HO has the legal power under Common Law to share information with the DfE.

Department for Education

3.3 As part of the Crown, the DfE has the legal power under Common Law to share information with the HO.

3.4 Section 20 of the Immigration and Asylum Act 1999 as amended by Section 55 of the Immigration Act 2016 allows DfE to supply information to the Home Office to use for immigration purposes as set out in that Act (below).

- the administration of immigration control under the Immigration Acts;
- the prevention, detection, investigation or prosecution of criminal offences under those Acts;
- the imposition of penalties or charges under Part II;

- the provision of support for asylum-seekers and their dependants under Part VI;
- anything else that is done in connection with the exercise of a function under any of the Immigration Acts;
- such other purposes as may be specified.

4. Lawful bases for processing personal data in accordance with Article 6 of the GDPR

Home Office

The processing is lawful as it is for the exercise of a function under a Government department which is set out in Section 8 of the Data Protection Act 2018 and meets the definition of a public task as set out in Article 6 (1)(e) of the GDPR. The HO also has a legal obligation under Section 55 of the Borders, Citizenship and Immigration Act 2009.

DfE

DfE are relying on **Article 6 (1)(e)** – processing is necessary for the performance of a task carried out in the exercise of official authority vested in the controller;

5. Privacy Information Notices

Home Office

5.1 The HO privacy Information Notice published on the HO website also provides information to individuals on how the HO users their personal information. See link below:

https://www.gov.uk/government/publications/personal-information-use-in-borders-immigration-and-citizenship

DfE

5.2 The DfE publish their personal information charter on GOV.UK at the link below:

https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter

Alongside DfE's personal information charter, the DfE also provide suggested wording for privacy notices to support schools and local authorities (who are the initial data controllers in the data supply chain and with whom parents typically have the most active and visible relationship) communicate appropriate messages about what data is collected, why it is collected and under what lawful basis such data is collected. These are available at the link below:

https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices

6. Third Party Processing

6.1 All data processing activity related to this PMoU are carried out by employees of the HO and DfE**.**

7. Data Protection Impact Assessment (DPIA)

Home Office

7.1 A Data Protection Impact Assessment is not required as this is a long-standing data sharing agreement and is covered by the data governance arrangements that pre-date the new data protection legislation. However, for completeness a DPIA has been completed by the HO and has been agreed with the HO Data Protection Officer.

DfE

7.2 The DfE have robust processes in place that encourage impact on data subject privacy to be considered and appropriate steps taken for all data sharing activities. A DPIA for the NPD has been completed and, to ensure full public transparency about the Department's processes and DPIA findings, will be made available on gov.uk during the first quarter of 2019.

8. Controller status of the receiving participant

The HO and DfE will be joint controllers for the HO data, as specified in 10.1, shared with DfE and DfE data, as specified in 10.6, shared with HO.

9. Purpose and benefits of the information sharing

9.1 The purpose of the data sharing process is to establish if the DfE hold information that will support HO Immigration Enforcement's (IE) key objectives of preventing abuse of immigration control and support the HO in its duty to have regard to the need to safeguard and promote welfare of children in the UK including:

- To locate individuals who the HO suspect have committed an immigration offence under Section 24 of the Immigration Act 1971 or 24A of the Immigration Act 1971, or section 35 of the Asylum and Immigration (Treatment of Claimants) 2004;
- To identify the most recent address and where appropriate any previous addresses that it holds for these subjects in the last five years at the date of request to maximise the success of tracing missing children and their families and those who have committed an immigration offence and
- (Where appropriate) bring the family (back) into compliant reporting.

9.2 Strategic aims of the data sharing:

- To reduce the illegal migrant population;
- Re-establish contact with children and families the HO has lost contact with and trace immigration offenders;

- To safeguard and promote the welfare of any child, and to reduce harm resulting from abuse of immigration.

9.3 The HO will request information from DfE pertaining to individuals or family members who have committed an immigration offence or are suspected of committing an immigration offence and who:

- are not in contact with the HO and the HO has no knowledge of any reasonable excuse for this and
- The HO believes the individual and family members are still in the UK.

9.4 Any information received as a result of the data sharing will be used in conjunction with other information already held by the HO or obtained by the HO, in the course of carrying out its functions, to assist in the process of identifying potential new contact details (including addresses) for the individual(s) and their family members. In addition, the HO may request information from DfE on unaccompanied minors who have either gone missing from care or who are not in contact with the HO and where the HO has no knowledge of any reasonable justification for this. These requests will be made in circumstances where it is the interests of safety, or wellbeing of the child.

9.5 The HO will utilise the information provided by DfE to contact Local Authorities and Other Government Departments (OGDs)/Agencies to carry out its existing functions in a way that takes into account the need to safeguard and promote the welfare of children in accordance with Section 55 of the Borders, Citizenship and Immigration Act 2009.

10. Information to be shared and the systems the information will be derived from

10.1 The details supplied (the 'HO Request information') will be extracted from the HO Casework Information Database (CID) and will include:

- Surname
- Middle Name (if known)
- Forename
- Alias (any former names)
- Gender
- Address (for up to the last five years where held)
- Post Code (if available)
- Date of Birth
- CID Person Identifier (CID PER ID)
    - Purpose of the individual request in accordance with the criteria set out in paragraph 4.3 above

10.2 The DfE will match this data against their records held on the National Pupil Database (NPD) and then in response provide the HO with information relating to those individuals that matched DfE records. Information on individuals will only be

provided to the HO by DfE where an exact match, using the forename/surname, middle name/surname, date of birth and postcode is found. The address will be used as supplementary information to endorse the match.

10.3 To minimise the risk of identifying incorrect individuals within the NPD, there will be no assumptions made throughout this process. In the case of multiple individuals matching the same information or, where a spelling or variation which hasn't been provided by the HO provides a potential match, no data will be automatically returned for that individual record. Instead, the record will be flagged as a possible match by DfE and HO will carry out further investigations. When the HO are satisfied that they have evidence to support an accurate match, they will resubmit the individual record in the following month's exercise.

10.4 The number of records to be shared will be no more than 300 in any given month. This volume can only be increased by exception (for example, where there are safeguarding concerns over the wellbeing of children) after consultation and prior agreement with DfE.

10.5 DfE will extract the information required for this exchange from records held on the NPD collections held by DfE.

10.6 Where a positive match is made, DfE will update the HO Request information with the following pupil/child and school(s) information (the "DfE Return Information"):

- Multiple or sole addresses (where held, for the last five years)
- House number/name, street name and town/ city
- Post code (if available)
- Relevant census collection date for this record
- Multiple or sole school information to include for all
    - School name
    - School post code
    - LA Establishment number
    - Earliest known pupil date at school
    - Latest known pupil date at school

10.7 For quality assurance purposes the DfE and HO will jointly review the request and return information to ensure that data totals match at each stage of the process. The data totals will include monthly requests and urgent ad hoc HO referrals. Any discrepancies will be followed up immediately by the HO and DfE.

11. Type of information sharing activity

11.1 The data will be shared on a monthly basis and on an ad-hoc basis in exceptional circumstances for the purposes set out in paragraph 18.4 below. The DfE will provide the HO with the results of the data share on a monthly basis within

10 working days of receipt. Ad-hoc cases will be dealt with within five working days of receipt.

12. Freedom of Information Act (FoIA) Requests

Please refer to section 11 of the UMoU for the process of handling FoI Act requests.

13. Subject Access Requests (SARs)

Please refer to section 12 of the UMoU for the process of handling SARs.

14. Handling of personal data and personal data security

Please refer to Section 13 of the UMoU for the protocols of handling personal data securely.

15. General Principles

Accuracy of the shared data

15.1 Before sharing information that includes personal data, the Participants must take all reasonable steps to ensure that the information being shared is both accurate and up to date in accordance with the Data Protection Legislation.

15.2 In circumstances where the recipient of the information is intending to use the information to make a decision that will impact directly on the data subject, the receiving Participant must 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 the decision is subsequently disputed/appealed by the data subject.

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

16.1 Any issues regarding ongoing delivery aspects of the information supply, such as data integrity or quality, should be addressed through “business as usual” channels as detailed in Annex C.

16.2 Where a problem arises it should be reported immediately, in writing to the designated contacts listed in Annex C.

16.3 The Points of Contact (SPOC’s) for DfE and the HO will endeavour to resolve the problem within two working days.

16.4 Where it is not possible to resolve the issue within two working days the issue will be escalated to the senior management team for each partner. They will be notified with an explanation of why the dispute has not been resolved so that they can take appropriate action for resolution or plan contingency arrangements.

16.5 Where the “business as usual” channels fail to reach agreement; the Participants will attempt to negotiate a settlement in the spirit of joint resolution within

20 working days of a formal notification being received. Contacts detailed in Annex C.

16.6 Specific strands of activity that may affect this PMoU should be discussed at a "business as usual" level to consider the possible impact on the PMoU. Once the potential changes have been identified then a formal change notification should be sent to the "PMoU Document Control Personnel" details provided in Annex B.

16.7 External changes affecting the operational delivery responsibilities of the Participants will also necessitate the reviewing and potential amendment of this PMoU.

16.8 All bulk data transfers will undergo a validation check to ensure that the data being transferred is in the correct format and meets the business specification. A HO manager will provide clearance prior to the data being forwarded to DfE once satisfied that the data meets the data sharing criteria as described in this PMoU.

17. Data subject's rights

Both Participants confirm that they have the technical capability and procedures in place to sufficiently comply with all the data subject's rights under the Data Protection Legislation including the technical capability to identify, provide and erase personal data should either Participant be legally required to do so.

18. Method of information sharing

18.1 Data will be shared electronically between Participants. The HO will provide DfE with the information on an excel spreadsheet (hereafter referred to as 'the file') on a monthly basis, including in each instance confirmation of the purpose for which the information is requested. The file will contain details of those individuals the HO wishes to match against DfE records. The HO will transfer the file following the secure file transfer protocol described at Paragraph 18.2 and 18.7 below. At the same time, the HO will also provide DfE with a completed request template (See Annex A); including details required for the matching and serving as notice that the file has been sent via a secure encrypted transfer process. The request template will be sent by secure e-mail to the data sharing mailbox at: (data.sharing@education.gov.uk).

18.2 As an additional layer of security, all files made available to DfE are sent from the HO by a secure email enabled encryption protocol – Transport Layer Security (TLS).

18.3 DfE will aim to respond to each monthly request within 10 working days of receipt. DfE will use the same file (previously referred to as 'the file') when responding and will insert the agreed information in cases where there is a positive match. If there is no positive match, DfE will confirm this in their response. DfE will transfer the file using a secure file transfer system (EGRESS). DfE will also return the original request template serving as notice that the file has been uploaded to the secure file transfer system. The request template will be sent by secure e-mail to the nominated individual in HO and will provide the HO with notice that the file has been uploaded to the secure file transfer system.

18.4 In exceptional circumstances the HO are able to make case-by-case ad-hoc requests to DfE utilising the same process with the exception of using the DfE ad-hoc form (see Annex A). These exceptional circumstances include but are not limited to:

- The HO believes there is significant and imminent physical risk to the child or parent/guardian and
- Issues of national security.

18.5 In these instances, the HO will ensure that they specify the exceptional circumstances in the ad-hoc form.

18.6 DfE will aim to respond to each ad-hoc request within five working days of receipt. DfE will use the same file (previously referred to as 'the file') when responding and will insert the agreed information in cases where there is a positive match. If there is no positive match DfE will confirm this in their response. DfE will transfer the file using the secure file transfer system. DfE will also return the original ad-hoc form, serving as notice that the file has been uploaded to the secure file transfer system. The ad-hoc form will be sent by e-mail to the nominated individual in HO and provide HO with notice that the file has been uploaded to the secure file transfer system.

18.7 HO Returns Preparation will facilitate the transfer of the file in all instances (both monthly and ad-hoc) via the secure email enabled encryption protocol – TLS and will WinZip the file before forwarding the file to DfE.

18.8 The NPD and Data sharing team will facilitate the 'return' transfer of the file in all instances (both monthly and ad-hoc) via EGRESS to the HO and will WinZip, encrypt and password protect the file before returning to the HO.

18.9 EGRESS is an online encryption system provided by DfE. The HO has access to EGRESS in order to access the returned data by logging into the system.

19. Retention and destruction schedule

19.1 Once DfE have carried out the matching exercise, they will retain and securely store details of the individuals requested, the purpose for which the data is requested, whether a match was achieved, and in cases of a positive match, what data was shared. To support its DPA responsibilities with regards to data subjects' right to access, DfE will retain this information for a minimum of seven years at which point the business need will be reviewed as per DfE retention policy.

19.2 Once HO receives the DfE Return Information; HO will bear responsibility of Data Controller for the DfE Return Information and will adopt the associated DPA obligations in respect of further processing of the data.

19.3 The HO will update the HO Casework Information Database (CID) on cases where there is a confirmed match from DfE at which point the data will become a permanent HO record.

19.4 In instances where the DfE Return Information received from DfE does not become part of a permanent HO record, the returned data will be securely destroyed by the HO within three months of receipt in accordance with HO's own retention and destruction polices and in line with HMG guidelines.

20. Permitted uses of the information in respect of this PMoU

20.1 Access will only be permitted to authorised personnel from DfE and HO who have:

- the appropriate security clearance determined by their own department to handle the data and
- a genuine business need to access the data.

Data Analysts for HO specifically in relation to the physical data transfer

Returns Preparation:

- [redacted]

Data Analysts for DfE

National Pupils Database and Data Sharing Team:

- [redacted]
- [redacted]

21. Onward disclosure to third parties

21.1 All HO staff and contractors have a duty of care under section 55 of the Borders, Citizenship and Immigration Act 2009 to ensure that immigration, asylum, and nationality functions are discharged having due regard to the need to safeguard and promote the welfare of children in the UK.

21.2 On a case-by-case basis the HO may share information obtained under this agreement with other OGD's including, Local Authorities, and Police where safeguarding obligations need to be applied to ensure the safety of the person(s) concerned and where that sharing is directly linked to the original purpose or purposes for which it was obtained under this agreement.

22. Roles of each Participant to the PMoU

22.1 ***Role of Home Office***

- Identify the appropriate data required to make the search from HO immigration data systems;
- Provide monthly and ad-hoc requests to DfE in an excel spreadsheet which will be win zipped and encryption protected before forwarding to DfE from and to agreed contact points under the protective marking 'Official-Sensitive' where applicable;
- Only allow access to that data by the team carrying out the data matching;
- Only store the data for as long as there is a business need to do so as set out in Section 8 of this PMoU;
- Any queries can be raised by emailing the designated points of contact for the HO at Annex C.

22.2 ***Role of DfE***

- On receipt, move the data received from the HO into a secure folder with the appropriate restricted access;
- Only allow access to that data by the team carrying out the matching;
- Send the data using EGRESS online encryption system agreed by both departments under the protective marking 'Official-Sensitive' where applicable;
- Only store the data for as long as there is a business need to do so as set out in Section 8 of this PMoU;
- Any queries can be raised by emailing the designated points of contact for DfE provided at Annex C.

22.3 Participants will work together to produce the best outcome for data subjects and the Departments to minimise any potential damage/distress.

23. Monitoring and reviewing arrangements

Regular/Routine Exchanges

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

23.2 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 approved in writing and appended to this document for inclusion at the formal annual review.

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

23.4 Annex A and B outline the contacts for amendments to the PMoU, document control, and the version history of the PMoU.

24. Complaints handling/issues, disputes and resolution

24.1 Any issues or disputes that arise as a result of the exchange covered by this PMoU must be directed to the relevant contact points listed in Annex C. Each

Participant will be responsible for escalating the issue as necessary within their given commands.

24.2 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 C) 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.

25. Costs

No charges will be made by either party in relation directly to this PMoU.

26. Termination

26.1. This PMoU may be terminated by giving a minimum of three months' notice by either Participant.

26.2 The Participants to this PMoU reserve the right to terminate this PMoU in the following circumstances:

- by reason of cost, resources or other factors beyond the control of the HO or the DfE.

- if any material change occurs which, in the opinion of the HO and the DfE following negotiation significantly impairs the value of the information sharing activity in meeting their respective objectives.

26.3 Where the information sharing relates to a one- off information sharing activity, the PMoU will terminate upon completion of the exercise.

26.4 In the event of a significant personal data breach (see section 22 of UMoU) or other serious breach of the terms of this PMoU by either Participant the PMoU will be terminated or suspended immediately without notice.

27. Personal Data Breaches

Please refer to Section 22 of the UMoU for the process of handling personal data breaches.

28. Signatories

Signed on behalf of the Home Office:

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

Signature:	[redacted]
Name:	[redacted]
Date:	31st January 2019
Position:	[redacted]

Signed on behalf of the Department for Education:

28.2 I accept the terms of the Process Memorandum of Understanding on behalf the Department for Education.

Signature:	[redacted]
Name:	[redacted]
Date:	31 January 2019
Position:	[redacted]

Annex A – Monthly and ad hoc request application forms

Monthly Request Template.docx

DfE Ad-Hoc form.docx

HO and DfE datashare spreadshe

Annex B – Document Control

Document Control Personnel

Key personnel	Name	Organisation (Team)
Author	[redacted]	HO
	[redacted]	HO
Approver	[redacted]	HO
	[redacted]	DfE
Review Control	[redacted]	HO
	[redacted]	DfE

Version and review history

Version/ review	Date	Summary of changes	Changes marked
0.1, 0.2, 0.3	11/12/14	Draft version	Y
0.4	12/01/15	Draft version	Y
0.5	05/03/15	Draft version	Y
0.6	12/03/15	Draft version	Y
0.7	18/05/15	Draft version	Y
0.8	01/06/15	Draft version	Y
0.9	04/06/15	Draft version	Y
1.0	05.06.15	Final	N
1.1	27/11/15	New draft version including updated purpose	Y
1.2	16/12/15	Responding to previous comments	N
Final V 2.0	18.12.15	Final version	N

Final V2.1	7.10.16	Updated version to reduce scope of elements sent to HO and transfer mechanism to EGRESS	No
Final V3.0	31.01.19	Updated final version addressing purpose, legal gateways and transfer mechanism following period of review carried out by Home Office and DfE Officials.	No

Annex C - Business Contacts

Business as Usual Contacts –Home Office

Contact	Email	Responsibility
N/A	HomeOfficeCustomerComplaints@homeoffice.gov.uk	Complaints Issues/Disputes/Resolution
[redacted]	[redacted]@homeoffice.gov.uk	Legal Issues
[redacted]	[redacted]@homeoffice.gov.uk	Freedom of Information
[redacted]	[redacted]@homeoffice.gsi.gov.uk	Review and amendments to PMoU
Home Office Returns Preparation Team	[redacted]@homeoffice.gov.uk [redacted]@homeoffice.gov.uk [redacted]@homeoffice.gov.uk	Operational Queries

HO Security	HOSecurity-DataIncidents@homeoffice.gov.uk	Personal Data Breach

Business as Usual Contacts – Department for Education

Contact	Email	Responsibility
[redacted]	[redacted]@education.gov.uk Always copying in data.sharing@education.gov.uk	Complaints Issues/Disputes/Resolution
[redacted]	[redacted]@education.gov.uk Always copying in data.sharing@education.gov.uk	Legal Issues
[redacted]	[redacted]@education.gov.uk Always copying in data.sharing@education.gov.uk	Freedom of Information
[redacted]	[redacted]@education.gov.uk Always copying in data.sharing@education.gov.uk	Review and amendments to PMoU
[redacted]	[redacted]@education.gov.uk Always copying in data.sharing@education.gov.uk	Personal Data Breach

Escalation Contacts – Home Office

Contact	Email	Responsibility

N/A	HomeOfficeCustomerComplaints@homeoffice.gov.uk	Complaints/ Issues/Disputes/Resolution
Home Office Legal Advisors Bureau (HOLAB)	To contact [redacted] in the first instance who will consider escalation to HOLAB [redacted]@homeoffice.gov.uk	Legal Issues
Knowledge and Information Management Unit	Freedom.informationteam@homeoffice.gov.uk	Freedom of Information
[redacted]	[redacted]@homeoffice.gov.uk	Review and amendments to PMoU
HO Security	HOSecurity-DataIncidents@homeoffice.gov.uk	Personal Data Breach

Escalation Contacts – Department for Education

Contact	Email	Responsibility
[redacted]	[redacted]@education.gov.uk	Complaints/Issues/Disputes/Resolution
[redacted]	[redacted]@education.gov.uk copying in data.sharing@education.gov.uk	Legal Issues
[redacted]	[redacted]@education.gov.uk	Freedom of Information
[redacted]	[redacted]@education.gov.uk	Review and amendments to PMoU
[redacted]	[redacted]@education.gov.uk	Personal Data Breach
