



MEMORANDUM OF UNDERSTANDING (MoU)
BETWEEN
THE HOME OFFICE
AND
Westmorland and Furness Council

In respect of sharing data for the Local Authority to plan services

Contents

Paragraph Number	Title of Paragraph	Page Number
1	Participants to the MoU	7
2	Introduction	7
3	Formalities	7
4	Role of the Participants	7
5	Controller Status of the Participants	7
6	Type of Data Sharing Activity	8
7	Purpose and Intended Benefits of Data Sharing Activity	8
8	Legal Considerations/GDPR principles	8
9	Legal Powers	9
10	Lawful Bases	10
11	Fairness/Transparency	11
12	Third-Party Processing	12
13	Data Protection Impact Assessment	12
14	Scope of Data to be Shared	12
15	Handling of Data/Data Accuracy	13
16	Data Security	14
17	Data Subject Rights	15
18	Freedom of Information Act Requests	16
19	Retention and Destruction Schedule	17
20	Onward Disclosure of Data to Third-Parties	17
21	Complaints/Issues Disputes & Resolution	18

22	Monitoring and Reviewing Arrangements	18
23	Costs	19
24	Termination	19
25	Data Breaches/Information Security Incidents	19
26	Signatories	20
Annex A	Business Contacts	21
Annex B	Document Control	22

GLOSSARY AND INTERPRETATION

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

Definition	Meaning
Criminal Offence Data	Criminal offence data includes the type of data about criminal allegations, proceedings or convictions.
Data	Means any data that includes Personal data, special category data. Criminal offence data and non-Personal data that is collected for a legitimate business function by the Participants and when shared between the Participants can support the Participants to better deliver their respective business objectives and/or functions.
Data Protection Legislation	The Data Protection Legislation” means: (a) the UK GDPR; (b) the LEP; (c) any applicable national laws implementing the GDPR and LEP, as amended from time to time; (d) the Data Protection Act 2018 to the extent it relates to processing of personal data and privacy and any secondary legislation made under that Act; and (f) all applicable Law about the processing of personal data and privacy.
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 Data Sharing)
Data Subject	Means (as defined in the Data Protection Legislation) the identified or identifiable living person to whom Personal data relates.
General Data Protection Regulation 2016 (UK GDPR)	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal data and on the free movement of such data and repealing Directive 95/46/EC, as incorporated directly into UK law as the UK GDPR
Human Rights Act 1998 (HRA)	The Human Rights Act 1998 sets out the fundamental rights and freedoms that everyone in the UK is entitled to. It incorporates the rights set out in the European Convention on Human Rights (ECHR) into domestic UK law. The Human Rights Act came into force in the UK in October 2000.
Information Commissioner's Office (ICO)	The ICO is the UK's independent authority set up to uphold information rights in the public interest. authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
LEP	Law Enforcement Processing.
Memorandum of Understanding (MoU)	This Document.
Participants	Means Participants to this MoU and refers explicitly to the Home Office and the external organisation the data sharing arrangement is with.

Personal data	Means (as defined in the Data Protection Legislation) any data relating to an identified or identifiable living person ('data subject'). An identifiable living person means a living individual who can be identified, directly or indirectly, in particular by reference to: a) an identifier such as a name, an identification number, location data, an online identifier; or b) One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.
Privacy Information Notice (PIN)	A Privacy Information Notice is a publicly available statement or document that sets out some or all 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.
Processor	Means (as defined in the Data Protection Legislation), any person who processes Personal data on behalf of the Controller (other than an employee acting within the scope of their duties)
Process/Processed/Processing	Means (as defined in the Data Protection Legislation) the collecting, recording, storing, retrieving, amending altering, disclosing/sharing, deleting, archiving and destroying Personal data.
Special Category Data	Special category data is personal data which the UK GDPR says is more sensitive, and so needs more protection. The UK GDPR defines special category data as: • personal data revealing racial or ethnic origin; • personal data revealing political opinions; • personal data revealing religious or philosophical beliefs; • personal data revealing trade union membership; • genetic data; • biometric data (where used for identification purposes); • data concerning health; • data concerning a person's sex life; and • data concerning a person's sexual orientation.
Interpretation	Rules and definitions
Annexes	The Annexes form part of this MoU.
Law	Means any law, statute, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of section 2 of the European Communities Act 1972, regulation, order, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any regulatory body with which the Participants are bound to comply; and a reference to any such Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time.

"including", "other", "in particular" and "for example"	The words "including", "other", "in particular", "for example" and similar words shall not limit the generality of the preceding words and shall be construed as if they were immediately followed by the words "without limitation".
Section or paragraph Headings	The Section and paragraph headings in this MoU are for ease of reference only and shall not affect the interpretation or construction of this MoU.
Hyperlinks	Reference to a standard, policy or document by hyperlink includes any amendments made to that standard, policy or document from time to time and/or any replacement of that hyperlink.

1	PARTICIPANTS TO THE MOU
1) THE SECRETARY OF STATE FOR THE HOME DEPARTMENT of 2 Marsham Street, London, SW1P 4DF hereafter referred to as the “Home Office” throughout this document; and 2) Westmorland and Furness Council, South Lakeland House, Lowther Street, Kendal LA9 4DQ hereafter referred to as the Local Authority throughout this document. 1.1 Collectively the Home Office and the Local Authority are referred to as “Participants” and individually are referred to as a “Participant”.	
2	INTRODUCTION
2.1 This MoU sets out the data sharing arrangement between the aforementioned Participants. This MoU is not intended to be legally binding but rather sets out the framework that governs the exchange of data between the Participants. The Participants will be expected to follow the guidelines for data sharing set out in this MoU when exchanging data to support their respective business objectives and/or functions. 2.2 For the context of this MoU, when referring to the term “Data” this will include personal data, special category data and criminal offence/criminal conviction data as defined by the Data Protection Legislation.	
3	FORMALITIES
3.1 This MoU will come into effect on 24 January 2025 3.2 The date of the review of this MoU is 24 January 2026	
4	ROLE OF THE PARTICIPANTS
<u>Role of Home Office</u> 4.1 This is a link to the <u>Home Office</u> website, which provides information on the role of the Home Office. <u>Role of the Local Authority</u> 4.2 This is a link to the Local Authority’s website www.wirral.gov.uk which provides information on the role of the Local Authority.	
5	CONTROLLER STATUS OF THE PARTICIPANTS
5.1 The Participants involved in any data sharing activities will clarify the Controller relationship for that data sharing arrangement in this MoU. i.e., whether the Participants are Joint or Independent Controllers of the data being shared. 5.2 The participants will act as independent Controllers.	

6	TYPE OF DATA SHARING ACTIVITY
6.1 Data will be shared by the Home Office on a daily basis with the Local Authority.	
7	PURPOSE AND INTENDED BENEFITS OF THE DATA SHARING
NB This section outlines compliance with the “Purpose Limitation” Principle of the GDPR. 7.1 The purpose of this data sharing arrangement is to enable the Home Office to share personal data directly with Local Authorities concerning those supported asylum seekers in their area who have been granted immigration status and will be required to ‘Move-On’ from their Home Office accommodation within their 56-day grace period. 7.2 The data sharing will support the Local Authority in its public task and statutory responsibilities regarding the prevention of homelessness by assisting the transition of supported asylum seekers from Home Office support to access to Local Authority assistance including housing. 7.3 The data sharing will enable Local Authorities to identify and contact relevant individual data subjects and offer suitably tailored assistance. 7.4 This direct data sharing agreement between the Home Office and individual Local Authorities will supplement existing processes whereby the Home Office’s asylum accommodation providers notify Local Authorities of individual cases at point of issuance of a notice to vacate.	
8	LEGAL CONSIDERATIONS /GDPR PRINCIPLES
8.1 The Participants are legally obliged to handle data in accordance with the GDPR, the DPA, all other Data Protection Legislation and the HRA. 8.2 This MoU will: • demonstrate how the data sharing activity complies with the GDPR principles. Please see <u>ICO Guidance</u> for further information on the GDPR principles • identify the legal power they will rely upon for disclosing, receiving and/or further processing the data. • identify the lawful basis for sharing any data and where applicable the processing condition where special category data and/or criminal offence/criminal conviction data is being shared as set out in the GDPR. Please see <u>ICO Guidance</u> for further guidance on the lawful basis for processing personal and special category data/criminal offence/criminal conviction data. • all public authority Participants must ensure that an individual’s right to privacy is not infringed by the data sharing by carrying out a full consideration of the HRA before entering into a data sharing activity under this MoU.	

9	LEGAL POWERS
Sections 9 and 10 outline compliance with the ‘Lawful’ aspect of the Lawfulness, Fairness and Transparency Principle of the GDPR. In this section the Participants must identify the legal power they will rely upon for permitting the disclosing, receiving and/or further processing the data NB: You should seek appropriate data protection/legal advice before completing this section <u>Home Office</u> 9.1. The Home Secretary has a statutory responsibility to provide accommodation and other support to asylum seekers who would otherwise be destitute under the Immigration and Asylum Act 1999 whilst an asylum application is being considered. Support for destitute asylum seekers is generally provided under section 98, section 95 or Section 4 of the Immigration and Asylum Act 1999. Following a grant of status, accommodation and support services will continue for 28 days from when an asylum seeker has been granted asylum. 9.2 Section 59 of the Nationality, Immigration and Asylum Act 2002 allows the Home Office to share personal data in connection with the settlement of migrants. As a Crown Department the Home Office (UKVI) will also rely on its Common Law Powers to share personal data with the Local Authority. <u>Local Authority</u> 9.3 This data sharing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority. Therefore, the following legislation legitimises the sharing and processing of this data under the terms of this MOU: 1. Housing Acts 1985, 1988, 1996, and 2004, 2. Homelessness Act 2002, Landlord and Tenant Act 1985, 3. Commonhold and Leasehold Reform Act 2002, 4. Housing and Planning Act 2016, 5. Homelessness Reduction Act 2017, 6. Children Acts 1989 and 2004, 7. Equality Act 2010, 8. Human Rights Act 1998 9. Local Audit and Accountability Act 2014 and 10. Any associated regulations, statutory guidance and codes of guidance	

- necessary for the performance of a contract e.g. Tenancy Agreements
- necessary for compliance with a legal obligation e.g. Health and Safety Legislation

10 | **LAWFUL BASES**

NB: You should seek appropriate data protection/legal advice before completing this section.

Home Office

10.1 Lawful basis for processing personal data under Article 6

Public Task The relevant lawful basis for processing personal data (as set out in Article 6 GDPR) for the Home Office is Article 6(1)(e) *“Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.”* Section 8(d) of the DPA 2018 states that the Article 6(1)(e) basis includes processing of personal data that is necessary for the exercise of a function of the Crown, a Minister of the Crown or a government department”

Special category processing condition under Article 9

Substantial Public Interest: The condition for processing special category data (as set out in Article 9 GDPR) for the Home Office is Article 9(2)(g) *“processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject”.*

Local Authority

10.2 Lawful basis for processing personal data under Article 6

Public Task The relevant lawful bases for processing personal; data (as set out in Article 6 GDPR) for the CCG will be Article 6(1)(e) *“Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.”* Section 8(d) of the DPA 2018 states that the Article 6(1)(e) basis includes processing of personal data that is necessary for the exercise of a function of the Crown, a Minister of the Crown or a government department”

Special category processing condition under Article 9

Article 9(2)(g) **Substantial Public Interest** *“processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;*

Article 9(2)(b) **Employment, social security and social protection (if authorised by law)** *“processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law*

or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject”.

Article 9(2)(h) **Health or Social Care** “processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the *working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards set out in Article 9(3) of the GDPR*”

11 | FAIRNESS/TRANSPARENCY

11.1 The Participants must ensure that they comply with their obligations under the fairness and transparency requirements as set out in the first principle of the GDPR. Participants are responsible for:

- recognising that the individuals have rights of privacy and confidentiality and that sharing of person identifiable information will respect these rights
- ensuring that the individuals are informed of the purposes for processing/sharing their data through an appropriate privacy notice, unless there is a legal obligation or DPA exemption that overrides this requirement
- the individuals are informed which other organisations their data may be disclosed to and consideration is given to whether consent of the data subject is required, and if so, will be sought (and complied with), unless there is a legal obligation or DPA exemption that overrides this requirement.

NB: This section outlines compliance with the ‘**Fair & Transparent**’ aspects of the **Lawfulness, Fairness and Transparency** Principle of the GDPR.

You should seek appropriate data protection advice before completing this section.

Home Office

11.2 The data on Home Office applicants is collected in line with the Borders Immigration and Citizenship System (BICS) Privacy Information Notice (PIN). The PIN sets out that data may be shared by the Home Office “*to assist other organisations in delivering their statutory functions*” including Local Authorities “*in relation to rights to access public services.*” The BIC PIN can be accessed here: [borders-immigration-and-citizenship-privacy-information-notice.](#)

Local Authority

11.3 Data subjects will be informed about the data sharing activity involved in the is MOU through the Council’s Privacy notice which is published on our website.

12 | THIRD-PARTY PROCESSING

12.2 Not applicable

13	DATA PROTECTION IMPACT ASSESSMENT																																			
13.1 The Participants will ensure that before any data sharing takes place under this MoU, consideration is given as to whether a Data Protection Impact Assessment (DPIA) should be carried out. Completion of a DPIA will, amongst other things, identify the relevant lawful basis for processing the data; assess the benefits of the data sharing, as well as identifying any privacy risks and how they might be mitigated. 13.2. A DPIA has been completed by the Home Office and is available upon request																																				
14	SCOPE OF DATA/INFORMATION TO BE SHARED																																			
NB: This section outlines compliance with the Data Minimisation Principle of the GDPR.																																				
14.1 Home Office																																				
<table><tr><th>Data Set for supported Asylum seekers</th><th>Category of data</th><th>Justification for receiving data</th></tr><tr><td>Name of main applicant</td><td>Personal Data</td><td>To address the individual or correspondence when contacting to offer services e.g. health screening, education, specialist support.</td></tr><tr><td>Address</td><td>Personal Data</td><td>Plan and consider the capacity of services based on location of potential user and to write to individuals upon Move On</td></tr><tr><td>Age/Date of Birth</td><td>Personal Data</td><td>Plan and consider the capacity of services available to age group</td></tr><tr><td>Gender</td><td>Personal Data</td><td>Plan and consider the capacity of services available by gender</td></tr><tr><td>Nationality</td><td>Special Category</td><td>link with language to ensure appropriate translation services and identify specific services to support community cohesion. To consider cultural support services.</td></tr><tr><td>Language spoken</td><td>Personal Data</td><td>link with language to ensure appropriate translation services</td></tr><tr><td>Support Termination date</td><td>Non-Personal Data</td><td>Consider LA obligations and plan for the transition within the given timeframe.</td></tr><tr><td>Family composition-Numbers</td><td>Personal Data</td><td>To identify the details of the family members to offer services.</td></tr><tr><td>Email address</td><td>Personal Data</td><td>To identify contact details of the service used to offer services</td></tr><tr><td>Phone number</td><td>Personal Data</td><td>To identify contact details of the service used to offer services</td></tr></table>				Data Set for supported Asylum seekers	Category of data	Justification for receiving data	Name of main applicant	Personal Data	To address the individual or correspondence when contacting to offer services e.g. health screening, education, specialist support.	Address	Personal Data	Plan and consider the capacity of services based on location of potential user and to write to individuals upon Move On	Age/Date of Birth	Personal Data	Plan and consider the capacity of services available to age group	Gender	Personal Data	Plan and consider the capacity of services available by gender	Nationality	Special Category	link with language to ensure appropriate translation services and identify specific services to support community cohesion. To consider cultural support services.	Language spoken	Personal Data	link with language to ensure appropriate translation services	Support Termination date	Non-Personal Data	Consider LA obligations and plan for the transition within the given timeframe.	Family composition-Numbers	Personal Data	To identify the details of the family members to offer services.	Email address	Personal Data	To identify contact details of the service used to offer services	Phone number	Personal Data	To identify contact details of the service used to offer services
Data Set for supported Asylum seekers	Category of data	Justification for receiving data																																		
Name of main applicant	Personal Data	To address the individual or correspondence when contacting to offer services e.g. health screening, education, specialist support.																																		
Address	Personal Data	Plan and consider the capacity of services based on location of potential user and to write to individuals upon Move On																																		
Age/Date of Birth	Personal Data	Plan and consider the capacity of services available to age group																																		
Gender	Personal Data	Plan and consider the capacity of services available by gender																																		
Nationality	Special Category	link with language to ensure appropriate translation services and identify specific services to support community cohesion. To consider cultural support services.																																		
Language spoken	Personal Data	link with language to ensure appropriate translation services																																		
Support Termination date	Non-Personal Data	Consider LA obligations and plan for the transition within the given timeframe.																																		
Family composition-Numbers	Personal Data	To identify the details of the family members to offer services.																																		
Email address	Personal Data	To identify contact details of the service used to offer services																																		
Phone number	Personal Data	To identify contact details of the service used to offer services																																		

Port Ref	Personal Data	To identify contact details of the service used to offer services
NASS Reference	Personal Data	To identify contact details of the service used to offer services
Latest Case Outcome	Personal Data	To identify those service users with a positive case outcome
15	HANDLING OF DATA /DATA ACCURACY	
<u>Volume</u>		
15.1 It is not possible to provide a forecast of the volume of records that may be shared under this agreement with each individual Local Authority. Volume of records will vary from week to week and area to area but is unlikely to exceed 1000 records for any individual local authority within in a twelve-month period.		
<u>Duration</u>		
15.2 This agreement will be reviewed annually, and it is envisaged that this data sharing arrangement will remain in force for as long as it is necessary for Asylum Seekers to be dispersed to the area.		
<u>Source(s) of the data</u>		
15.3 The data will be extracted from the Home Office immigration casework system ATLAS, PRAU reports and local files.		
<u>Frequency</u>		
15.4 Data will be shared daily.		
<u>Format</u>		
15.5 The personal data will be shared in an excel spreadsheet though a dedicated secure file sharing portal with the relevant local authority.		
<u>Accuracy of the shared data</u>		
15.6 The Participants will make reasonable endeavours to ensure that the data being shared under this MoU is checked before disclosure for accuracy and relevance in accordance with GDPR. 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 data that has been disclosed it will notify the other Participant; the procedures for notifying the other Participant of any inaccuracies in the data being shared (including timescales for notification) must be set out in this MoU.		
NB: Rows 15.7 to 15.9 outline compliance with the Accuracy Principles of the GDPR.		

15.7 The data has been quality assured under a comprehensive assurance regime which is used for all external reports. The quality and the accuracy of the data is dependent on the inputs made by applicants, case workers and assurance that downstream systems are free of faults. Whilst there is not a 100% guarantee that human and system error could occur resulting in inaccurate data, the data has been quality assured under a comprehensive assurance regime which is used for all external reports.
<u>Notification and rectification of errors in the data/Information shared</u> 15.8 The disclosing Participant will notify the receiving Participant of any errors within 48 hours of discovery to the designated points of contact for this data sharing activity.
<u>Rectification</u> 15.9 The disclosing Participant will rectify any errors within two working days of discovery and send an amended data set to the designated points of contact for this data sharing activity.
16 DATA SECURITY
16.1 This section outlines compliance with the Integrity and Confidentiality Principle of the GDPR. 16.2 Participants deemed to be Controllers as defined in the Data Protection Legislation must ensure that personal data is handled and processed in accordance with the requirements of the Legislation. Additionally, the Participants must process the data being shared in compliance with Her Majesty's Government Security Policy Framework (HMG SPF) guidance issued by the Cabinet Office or where a Participant is a private sector organisation it's security management arrangements must have been certified as following ISO/IEC 27001 or equivalent standard. HMG SPF guidance document can be accessed via the following link <u>Security Policy Framework</u>. 16.3 The Participants will ensure effective measures are in place to protect data in their care and manage potential or actual incidents of loss of data. Such measures may include: • data 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 MoU; • access to data received by the Participants pursuant to this MoU must be restricted to employees on a legitimate need-to-know basis, and those employees must have security clearance at an appropriate level; 16.4 the Participants will comply with the Government Security Classifications Policy (GSCP) where applicable: <u>Government Security Classification Policy</u> <u>Security standards</u> 16.5 Both participants are to follow the HMG Security Policy Framework
<u>Means of transfer of data/Information</u>

16.6 Data will be exchanged between the Participants in a secure approved format, as approved by all Participants.

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

16.8 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.

16.9 The Home Office will share via a secure data sharing platform, MOVEit. Access will only be granted to designated staff who will only be allowed to access their own data.

16.10. The Data will be automatically deleted after 30 days.

Government Security Classification

16.11 The information is classed as OFFICIAL-SENSITIVE as defined in Government Security Classification Policy

Who will have access to the shared personal data/designated points of contact

16.12 The Home Office will use an automated digital system to upload the data reports onto the Local Authority folder within MOVEit. Designated staff from the Local Authority who have the appropriate level of security clearances, will be authorised to have MOVEit accounts, to access the reports.

17 DATA SUBJECT RIGHTS

17.1 In the event a request to exercise a particular right is received from a data subject under this MoU, the Participants will respond to the request in accordance with the requirements of the Data Protection Legislation.

17.2 Individuals can request a copy of the data that either Participant holds on them, by making a Right of Access Request (RAR). This may include data that was disclosed to that Participant under this MoU. 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 data to the individual will not prejudice any ongoing investigation/proceedings.

17.3 Where a request is received to rectify, erase or restrict any data shared under MoU, the receiving Participant must inform the disclosing Participant under Article 19 of the GDPR where it is possible and proportionate to do so.

17.4 Where a Joint Controller data sharing arrangement is entered into the procedures for responding to data subject right requests under Article 26 of the GDPR must be set out in this MoU or an alternative joint controller agreement template can be used (see guidance notes at front page).

17.5 The contact for responding to Data Subject Right requests for the Participants are provided at **Annex A**

17.6 Data subject rights vary according to the data processing regime being relied upon by the Controllers. The Participants must complete the table below indicating the data processing regime, the rights applicable to each Controller and the rights that do not apply and why. See ICO Guidance for further information on Data Subject Rights.

Data Subject Right	Data Processing Regime (Part 2/Part 3 of the DPA 2018)	Applies to Home Office Y/N	Applies to Local Authority Y/N	If right does not apply provide reason why
Be Informed	<u>Part 2 DPIA 2018</u>	<u>Y</u>	<u>Y</u>	
Access	<u>Part 2 DPIA 2018</u>	<u>Y</u>	<u>Y</u>	
Rectification	<u>Part 2 DPIA 2018</u>	<u>Y</u>	<u>Y</u>	
Erasure	<u>Part 2 DPIA 2018</u>	<u>N</u>	<u>N</u>	<u>Does not apply when processing under public task</u>
Restriction	<u>Part 2 DPIA 2018</u>	<u>Y</u>	<u>Y</u>	
Portability	<u>Part 2 DPIA 2018</u>	<u>N</u>	<u>N</u>	<u>Only applies when processing under consent as lawful basis</u>
Object	<u>Part 2 DPIA 2018</u>	<u>Y – but can only object in certain cases</u>	<u>Y</u>	
Automated decision-making and profiling	<u>Part 2 DPIA 2018</u>	<u>N</u>	<u>N</u>	<u>Not Appropriate to this request.</u>

18 FREEDOM OF INFORMATION ACT (FoIA) REQUESTS

18.1 Home Office and the Local Authority shall assist and co-operate with each other to enable each department to comply with their information disclosure obligations. In the event of one Participant receiving a FoIA request that involves disclosing information that has been provided by the other Participant, the Participant in question will notify the other to allow it the opportunity to make representations on the potential impact of disclosure and will issue a formal response following its internal procedures for responding to FoIA requests within the statutory timescales.

18.2 The designated contact for responding to FoI requests for the Participants are provided at **Annex A**.

19 RETENTION AND DESTRUCTION SCHEDULE

NB: This section outlines compliance with the **Storage Limitation** Principle of the GDPR.

19.1 The Participants undertake to store the data being shared securely with access restricted to appropriately authorised personnel.

19.2 Participants will not keep the data longer than necessary for the agreed purpose set out in the MoU.

19.3 The Participants will have documented policies on the retention and destruction of the shared data in accordance with the requirements of the Data Protection Legislation and where applicable HMG SPF Guidance.

Home Office

19.4 The data will be held in line with existing departmental retention and disposal policies. Electronic information will be securely erased or overwritten using an approved software utility to a standard applicable to the security classification.

Local Authority

19.5 The data will be held in line with existing departmental retention and disposal policies. The data will only be held for as long as is necessary with reference to the purpose for which it was shared. Electronic information will be securely erased or overwritten using an approved software utility to a standard applicable to the security classification.

20 ONWARD DISCLOSURE OF DATA TO THIRD-PARTIES

20.1 The receiving Participant will respect the confidentiality of the data being shared and will not disclose the other Participants data to third parties unless required to do so in accordance with the Law, for the purposes of criminal investigations or legal proceedings or with the explicit consent of the other Participant.

20.2 However, any data shared as a result of this MoU which then forms part of the permanent record of the receiving Participant, becomes the responsibility of that Participant under the terms of the Data Protection Legislation. Therefore, the receiving Participant becomes Controller for the data. In this case para 15.1 will not apply and as Controller for that data, the receiving Participant may onwardly disclose data to third parties subject to the following conditions being met:

- the Participant intending to make the onward disclosure must be satisfied that the data 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 intending to make the onward disclosure must be satisfied that the data 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 intending to make the onward disclosure must be satisfied that adequate security arrangements are in place for the transmission of the data to the

	receiving third party and that that third party has adequate security arrangements in place for the secure storage of the data; and • where necessary a separate formal data sharing agreement should be put in place with the third-party organisation setting out all the above.
21	COMPLAINTS HANDLING / ISSUES, DISPUTE RESOLUTION
	21.1 Complaints about the use of data in relation to this MoU should be dealt with under the relevant complaint's procedure of the Participant whose actions are subject of the complaint. 21.2 The Participants agree to co-operate with each other in the investigation of any complaint or other investigation about the use of the data shared. 21.3 The outcome/resolution of any complaint will be notified to the other Participant to this MoU within two months of the complaint being lodged. 21.4 Any day-to-day operational issues or disputes that arise as a result of data shared under this MoU must be directed to the relevant contact points listed in Annex A. Each Participant will be responsible for escalating the issue as necessary within their respective organisations.
22	MONITORING AND REVIEWING ARRANGEMENTS
	<u>Regular/Routine Exchanges</u> 22.1 This MoU must be reviewed before 23 December 2025. 22.2 Reviews outside of the proposed review period 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. 22.3 The MoU review process will focus on: • whether the MoU is still necessary and fit for purpose • whether the existing information sharing arrangements should be extended or amended • whether the lawful 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 lawful basis for information sharing has changed, the information sharing activity in place may need to be amended to reflect this. 22.4 In the event of a personal data breach or other breach of the terms of this MoU by any of the Participants, this MoU must be reviewed immediately by the Participants. 22.5 A record of all reviews will be created and retained by each Participant (see Annex B).

23	COSTS
	23.1 The Participants will pay their own costs and provide adequate resources to perform their activities under this MoU. There may, however, be charges levied in specific data sharing exchanges in relation, for example, to IT development. The costs should be set out if applicable at 23.2 below or cost agreements can be annexed to this MoU if preferable. 23.2 There will be no charges for this exchange of data.
24	TERMINATION
	24.1 Either Participant may terminate this MoU upon 30 days written notice to the other, or after an agreed period of time. 24.2 Termination notices must be referred to the signatories of this MoU. 24.3 The Participants will have the right to terminate this MoU should the following circumstances arise: • a material breach by the other Participant of any of the terms of the MoU; • by reason of cost, resources or other factors beyond the control of either of the Participants; or • if any material change in circumstances occurs which, following negotiation between the Participants, in the reasonable opinion of either or all the Participants significantly impairs the value of the MoU in meeting their objectives. 24.4 It is recognised that there may be circumstances where it may not be possible to terminate a data sharing activity such as set out in the situations below. Should such circumstances arise, the Participants must refer to the signatories of this MoU who will be decide on how the data sharing activity will be managed. The situations below include: • the sharing of data is essential to the Participants to provide their business service and termination of the MoU would severely impact the organisation's ability to fulfil their statutory obligations; and • the sharing of data is necessary to satisfy a legal requirement. 24.5 Where a decision is made to terminate this MoU the Participants will consult with each other to determine how the data shared between the Participants is handled.
25	DATA BREACHES/ INFORMATION SECURITY INCIDENTS
	25.1 A data breach/information security incident is a breach of security leading to the accidental or unlawful destruction, loss alteration, unauthorised disclosure of, or access to data transmitted, stored or otherwise processed. Examples of serious data breaches/security incidents may include: • accidental loss or damage to personal data; • damage or loss of personal data by means of malicious software/hacking; • deliberate or knowing 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;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission or lawful bases; and
- loss of availability of personal data.

25.3 The designated points of contact (provided at **Annex A** of this MoU) are responsible for notifying the other Participant in writing in the event of a data breach/ information security incident occurring under this MoU within 24 hours of the event.

25.4 The designated points of contact will discuss and jointly decide the next steps relating to the incident. Such steps will include (but not be limited to): containment of the incident and mitigation of any ongoing risk; recovery of the data (insofar as relevant); and assessing whether the Information Commissioner and/or the data subjects will be notified.

26 SIGNATORIES

Signed on behalf of the Home Office:

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

Signature:	
Name:	
Position:	Deputy Director for Move On Operations
Date:	Click or tap to enter a date.

Signed on behalf of the Local Authority

26.2 I accept the terms of this Memorandum of Understanding on behalf of Westmorland and Furness Council

Signature:	
Name:	
Position:	Assistant Director Safer Stronger Communities
Date:	23 January 2025

Annex A - Business Contacts**Home Office**

Contact (Name and Position)	Email	Responsibility
██████████ / Data Sharing Team	██████████@homeoffice.gov.uk	Operational Queries/ Resolving Data Quality Issues/Disputes Resolution
██████████ / Data Sharing Team	██████████@homeoffice.gov.uk	Review and amendments to MoU
Centralised Team	██████████@homeoffice.gov.uk	Personal data Breach/Security Breach
Centralised Team	██████████@homeoffice.gov. uk	Freedom of Information Act Requests
Centralised Team	██████████@homeoffice.gov.uk	Data Subject Right Requests

Local Authority

Contact (Name and Position)	Email	Responsibility
██████████ Service Manager Resettlement	██████████@westmorlandandfur ness.gov.uk	Operational Queries/ Resolving Data Quality Issues/Disputes Resolution
██████████ Service Manager Resettlement	██████████@westmorlandandfur ness.gov.uk	Review and amendments to MoU
██████████ Senior Information Governance and Data Protection Officer	██████████@westmorlandandfur ness.gov.uk	Data Protection
██████████ Service Lead I Service Centre (Information Governance and Complaints)	██████████@westmorl andandfurness.gov.uk	Access to Information i.e. FOI
██████████ ICT & Cyber Security Manager	██████████@westmorlandandfurness. gov.uk	Cyber-Security

Annex B- Document Control

Document Control Personnel

Key Personnel	Name and Position	Organisation (Team)
Author	██████████ <i>Data Compliance Asylum & Protection, RASI</i>	Home Office
Review Control	██████████ <i>Data Compliance Asylum & Protection, RASI</i>	Home Office
	██████████ <i>Resettlement Service Manager</i>	Westmorland and Furness Council

Version and review history

Version/Review	Date	Summary of changes	Changes Marked