

**DATA SHARING
AGREEMENT**

between

His Majesty's Inspectorate of Prisons (HMIP)

and

**The Home Office
(Border Force and Immigration Enforcement)**

CONTENTS

Section 1	INTRODUCTION	Page 3
Section 2	DEFINITIONS	Page 4
Section 3	BASIS OF THE AGREEMENT	Page 6
Section 4	MANAGING THE AGREEMENT	Page 13
Section 5	DATA SHARING PROCEDURES	Page 15
Section 6	INFORMATION SECURITY	Page 17
Section 7	PUBLIC INFORMATION REQUESTS	Page 20
Section 8	SIGNATORIES	Page 21

This Agreement sets out the data sharing arrangements between.

- His Majesty's Inspectorate of Prisons; and
- Home Office (Border Force and Immigration Enforcement)

Each is a "Participant" to this Agreement and together "the Participants".

This Agreement 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 Agreement when exchanging data to support their respective business objectives and/or functions.

For the context of this Agreement, when referring to the term "Data" this will include personal data, special category data and criminal offence/criminal conviction data as defined by UK Data Protection Legislation, and non-personal data.

As a consequence of the requirement for information sharing to enable the Participants to perform their legal duties and exercise their lawful powers for the purposes set out in this Agreement, the Participants hereby commit to a partnership approach and recognise the invaluable contribution of collaborative working in the public interest, including sharing Personal Data.

The Participants intend that this Agreement will form the basis of the data sharing arrangements between the Participants. The intentions of the Participants are that they shall each be independent Controllers in respect of the Personal Data that they process, or that is processed on their behalf, under this Agreement.

This Agreement will be reviewed annually.

IT IS THEREFORE AGREED AS FOLLOWS

2 DEFINITIONS

In construing this Agreement, capitalised words and expressions are defined terms, having the meaning set out below:

“Agreement” means this Data Sharing Agreement, as amended from time to time in accordance with its terms, including any Schedules to this agreement;

“Data” means the information which contains Personal Data;

“Controller” has the meaning set out in UK Data Protection Law;

“UK GDPR” means the current UK data protection legislation, which save for minor amendments contained in the [Keeling Schedule](#) is equivalent to Regulation (EU) 2016/679 of the European parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

The “UK Data Protection Legislation” means:

- (a) the UK GDPR
- (b) the Data Protection Act 2018
- (c) regulation made under the DPA 2018
- (d) regulation made under section 2(2) of the European Communities Act 1972 which relate to the EU GDPR or the Law Enforcement Directive.

“Data Subject” means an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

“Information Commissioner” means the UK Information Commissioner and any successor thereof;

“Law” means any statute, directive, other legislation, law or regulation in whatever form, any delegated act (under any of the foregoing), rule, order of any court having valid jurisdiction or any other binding restriction, decision or guidance in force, from time to time;

“Legal Basis” means the lawful basis under UK Data Protection Law that is relied on for processing Personal Data by either Participant;

“Personal Data” means any data relating to an identified or identifiable living person (“data subject” - as defined in the UK Data Protection Legislation). An identifiable 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 that natural person.

“Purposes” means the purposes referred to in Section 3 of this Agreement;

“Special category” data is data which the UK GDPR says is more sensitive, and so needs more protection. The UK GDPR defines special category data as:

- data revealing racial or ethnic origin;
- data revealing political opinions;
- data revealing religious or philosophical beliefs;
- 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

“Subject Access Request” means a written request asking an organisation whether or not they are using or storing your personal information. Data Subjects can ask organisations for copies of their personal information, verbally or in writing. This is called the right of access and is commonly known as making a subject access request or SAR.

In this Agreement, unless the context requires otherwise:

- (i) words and expressions defined in UK data protection legislation have the same meanings in this Agreement;
- (ii) references to statutory provisions include those statutory provisions as amended, replaced or re-enacted for the time being in force and include any secondary legislation, rules, regulations, orders, notices, codes of practice, directions, consents, permissions and guidelines made thereunder.

3. BASIS OF THE AGREEMENT

3.1 Purposes of this Agreement

This Agreement outlines the terms and conditions agreed between the Participants under which specific Personal Data (including Special Category Data) will be shared between the Participants. It also outlines the safeguards that have been put in place by the Participants to ensure that the sharing of Data is lawful.

The Agreement exists to ensure that Personal Data can be shared in a way that satisfies the legal and professional obligations of the Participants, their respective staff and the rights, freedoms and legitimate expectations of the Data Subjects in respect of whom the Personal Data is being shared.

This Agreement has been prepared to support the regular sharing of specific Personal Data between the Participants.

This Agreement details the specific purposes for sharing Personal Data, as well as the Data being shared, the required operational procedures for that sharing to take place, the Legal Basis for sharing and what is to be done with the Data that is shared after the legitimate need for processing has ceased.

3.2 Purposes for sharing Personal Data

Immigration Enforcement (IE) is one of the principal directorates of the Home Office. It is responsible for preventing abuse of the immigration system, tracking immigration offenders and increasing compliance with immigration law. It works with partners such as the police to regulate migration in line with government policy, while supporting economic growth. Immigration Enforcement's vision is to tackle illegal migration, remove those with no right to be here, and protect the vulnerable.

Detention Services (DS) manage most of the immigration detention estate on behalf of the wider Home Office including Immigration Enforcement, Border Force and UK Visa and Immigration (Asylum & Protection). DS manage those parts of the detention estate which are contracted out to commercial partners, whereas Residential Short-term Holding Rooms and Short-term Holding Facilities are managed by International Returns Service Command (IRSC).

Border Force is a Law Enforcement arm of the Home Office with primary responsibility for UK Border Security, including counter terrorism, immigration and customs matters. Border Force are responsible for managing the UK border control by enforcing immigration and customs regulations and working with the wider Home Office on organised crime, modern slavery and trafficking.

The principal purpose of sharing Personal Data under this Agreement is to enable HMI Prisons to carry out its statutory functions. HM Chief Inspector of Prisons' responsibilities are set out in sections 5A and 43 of the Prison Act 1952 (as amended): [Criminal Justice Act 1982 \(legislation.gov.uk\)](https://www.legislation.gov.uk/ukpga/1952/11/section/5A). The information that is shared under this Agreement, including Personal Data, is necessary for the purposes of HMI Prisons carrying out its functions.

Participants may only use the Personal Data disclosed to them under this Agreement for the specific purposes set out in this document.

3.3 Relationship between the Participants

The Participants agree that the relationship between them is such that the sharing of Personal Data by them is on a Controller to Controller basis and are therefore independent Controllers.

Each Participant is responsible for ensuring that its own processing of Personal Data is compliant with UK data protection legislation (including responding to any Subject Access Request).

3.4 Benefits

This Agreement:

- assists the Participants to comply with their statutory and non-statutory duties and to perform statutory and non-statutory functions;
- clarifies the scope of what Personal Data is shared and the arrangements for sharing.

In addition to the benefits listed above, by operating within the parameters of this Agreement, the Participants will be able to demonstrate they are processing information lawfully and are complying with UK Data Protection Law. It will also enable the Participants to ensure, and be able to demonstrate, that the sharing of Personal Data is on the basis of specific and agreed categories of Personal Data.

3.5 Legal Basis for data sharing

The Legal Basis for sharing information under this Agreement is contained in the following statutes, each read together with UK data protection legislation:

- Immigration Act 1971;
- Immigration and Asylum Act 1999; and
- UK Borders Act 2007.

HMI Prisons is a “public authority” as defined by the Freedom of Information Act 2000. HMI Prisons carry out specific tasks in the public interest. The lawful basis on which HMI Prisons and HO process personal data referred to in this Agreement is Article 6(1)(e) (public task) of the UK GDPR: processing is necessary for the performance of a task carried out in the public interest as it is necessary for the administration of justice and the exercise of a function of the Crown, a Minister of the Crown or a government department (DPA 2018, Part 2, Schedule 1 (6)).

3.6 Regulatory compliance

Disclosure of Personal Data under this Agreement will be undertaken, by both Participants, within the legal framework of UK data protection Legislation and the Human Rights Act 1998; and in compliance with the common law duty of confidence. Details of compliance with each of these are set out below.

Data Protection Act 2018 (DPA) Part 2: General Processing

HM Inspectorate of Prisons for England and Wales (HMI Prisons) is an independent inspectorate whose Chief Inspector is a Crown appointment. The Chief Inspector reports on conditions for and treatment of those in prison, young offender institutions, secure training centres, immigration detention facilities, police and court custody suites, customs custody facilities and military detention. The role of HM Inspectorate of Prisons is to provide independent scrutiny of the conditions for and treatment of prisoners and other detained people, promoting the concept of 'healthy establishments' which improve outcomes for those detained and for the wider public.

Section 5A(5A) of the Prison Act 1952, as amended by section 152(5) of the Immigration and Asylum Act 1999, requires the Chief Inspector to report on the treatment of and conditions for detained people in immigration removal centres (IRCs).

Section 46(1) of the Immigration, Asylum and Nationality Act 2006 extended the Chief Inspector's inspection and reporting remit to immigration short-term holding facilities (STHFs) and escort arrangements throughout the UK. Paragraph 8 of Schedule 9 to the Immigration Act 2014 did the same for pre-departure accommodation.

HMI Prisons is a designated member of the UK National Preventive Mechanism (NPM). This mechanism was established in response to the UK's obligations as a party to the Optional Protocol to the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (OPCAT), an international human rights treaty designed to strengthen the protection of people deprived of their liberty.

IRCs receive a full unannounced inspection at least once every four years. The inspection is conducted over two or three weeks. During the assessment, research staff conduct confidential surveys of people in detention, and inspectors will make an initial assessment of the establishment and conduct any immediate inspection activity they consider necessary.

Facilities holding children will receive more regular inspections (approximately every two years). At least three escort inspections will be conducted every year, and may include overseas charters, scheduled flights and in-country escorts.

Non-residential STHFs, also known as holding rooms, are inspected at least once every six years, including facilities in other countries that are subject to juxtaposed controls. Residential short-term holding facilities (RSTHFs) are inspected at least once every four years.

HMI Prisons is an arms-length body of the Ministry of Justice. Both the Home Office and the Ministry of Justice are "competent authorities" as defined in Section 30 and Schedule 7 of the DPA and, for the purposes of this Agreement, both Participants are processing Personal Data (including [Special Category Data](#)) for processing in the public interest as defined in Article 6.1.e of the UK GDPR.

The processing of "special category of data" is prohibited under Article 9 of the UK GDPR, subject to certain derogations. The condition for processing this special category data is Article 9(2)(g) – "reasons of substantial public interest". For the HO and HMI Prisons this includes the exercise of a function of the Crown, a Minister of the Crown or a government department and for the administration of justice (DPA Schedule 1, Part 2 (6)).

This document sets out HMI Prison's procedures for securing compliance with the principles in Article 5 of the UK GDPR (principles relating to processing of personal data) and HMI Prison's policies as regards the retention and erasure of personal data.

HMI Prisons is registered as a Controller with the Information Commissioner's Office, to process personal information for the purposes of fulfilling its duties. It collects personal information for the performance of its tasks, carried out in the public interest. Information is collected from multiple sources and, at any one time, can involve processing personal information about various individuals including:

- people held in detention
- members of HO staff
- complainants or their representatives
- the subject of a complaint or their representatives
- individuals who may hold information which is relevant to an inspection
- service providers and their employees or employees of their contractors
- individuals captured by CCTV images
- survey respondents
- professionals with an interest in HMI Prison's publications
- copies of any Vulnerable Adult Care Plans opened
- copies of Use of Force reports, including line manager/assessor comments
- copies of all incident reports, including the management reviews and comments
- copies of all complaints
- details of those held in detention who are either an Adult at Risk (AAR), subject to Detention Centre Rule 35 or an age dispute case.
- details of those in detention including the time they have been held in detention

Personal and sensitive information is collected by HMI Prisons for the purpose of conducting inspections. The type of personal and/or sensitive information HMI Prisons may collect about any one of the individuals listed above can include:

- personal details - include name, date of birth, gender and country of origin
- family details
- lifestyle and social circumstances
- financial details
- employment and education details
- details of complaints, incidents and grievances
- visual images, personal appearance and behavior
- physical or mental health details
- racial or ethnic origin
- religious or other beliefs
- political opinions
- sexual life
- offences (including alleged offences)
- details of security categorisation and assessments of risk of harm
- criminal and legal proceedings, outcomes and sentences

All personal data held by HMI Prisons will be:

- Processed lawfully, fairly and in a transparent manner

- Collected for the purposes set out in Section 3.2 above
- Adequate and limited to what is necessary
- Accurate and kept up to date
- Kept for no longer than is necessary
- Processed securely

HMI Prisons is not responsible for any loss or damages arising from the use of the Personal Data shared by the HO except where this loss or damage arises as a direct result of negligence on the part of HMI Prisons.

Human Rights Act 1998

Disclosure of Personal Data will be conducted within the legal framework of the Human Rights Act 1998 (HRA) and any law which amends or replaces this Act. The HRA gives further effect in domestic law to Articles of the European Convention on Human Rights (ECHR). The Act requires all domestic law to be compatible with the Convention Articles and places a legal obligation on all public authorities to act in a manner compatible with the Convention.

Article 8 of the ECHR, set out in Schedule 1 to the Human Rights Act, states that:

(1) Everyone has the right to respect for his private and family life, his home and his correspondence.

(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The Participants confirm that their processing of this information complies with the requirements of the HRA in that sharing of Personal Data is proportionate and in accordance with one or more of the circumstances set out Article 8(2) above.

Common law duty of confidence

Disclosure of information containing Personal Data will be conducted in compliance with the common law duty of confidence. The duty of confidence falls within common law as opposed to statutory law and derives from cases considered by the courts. There are generally three categories of exception to the duty of confidence, where:

- there is a legal duty to disclose;
- there is an overriding duty to the public; and/or
- the individual to whom the Personal Data relates consented.

The Participants to this Agreement confirm that their processing of Personal Data complies with the requirements of the common law duty of confidence in that there is a legal duty to disclose the Personal Data falling within the scope of the Agreement.

3.7 Retention of Personal Data

Data Protection Law does not set out any specific minimum or maximum periods for retaining Personal Data. However, a principle of data protection contained within Article 5.1.e (UK

GDPR) is that Personal Data should not be kept for longer than is necessary for the purposes for which the Personal Data are processed. For the purposes of sharing Personal Data under this Agreement, and in line with each Participants records management policies, the Participants will:

- consider the purposes they hold the Personal Data for in deciding how long to retain it;
- securely delete Personal Data that is no longer needed for these purposes; and
- update, archive or securely delete Personal Data, if it goes out of date.

3.8 Fairness and Transparency

A basic requirement of Data Protection Law is that individuals should be told who is holding their information, what the Controller intends to do with the information and who else they may share it with. For the purposes of this agreement both Participants are Controllers of the Personal Data they hold, including Data that they receive from each other. Each Participant must ensure that they have appropriate policies and procedures in place to facilitate both the protection and the exercising of rights of individuals under UK data protection legislation. Each Participant will comply with the rights of the individuals in a fair and consistent manner and in accordance with any specific legislative requirements, regulations or guidance.

3.9 Privacy Notice

Each Participant will have in place a Privacy Notice which explains how they will collect, use and disclose Personal Data and it should be in a form that complies with UK data protection legislation.

The Borders, Immigration and Citizenship System (BICS) Privacy Notice can be found [here](#), and the HMI Prison's Privacy Notice is published [here](#)

4 MANAGING THE AGREEMENT

4.1 Management Structure

This Agreement will be managed through a process of engagement and negotiation between Single Points of Contact from each Participant:

Single Points of Contact:		
Participant	Title	Contact Details
HMIP	Data Protection Officer (DPO)	DataProtection@justice.gov.uk
HO	Data Protection Lead, DS	scott.rowan@homeoffice.gov.uk

It is the responsibility of each Participant to advise the other Participant if their Single Point of Contact changes.

4.2 Dispute Resolution

If circumstances arise in which either Participant has concerns in relation to the operation of this Agreement, every effort should be made to resolve this so that information exchange is not disrupted. If Single Points of Contact are not available, then concerns may be escalated to:

- martin.lomas@hmiprisons.gov.uk (HMI Deputy Chief Inspector) and/or
- DetentionServicesDataProtection@homeoffice.gov.uk
- mike.coombes@homeoffice.gov.uk

Either Participant may suspend this agreement for up to 30 days at any time, if their view is that security has been seriously breached. This will only be considered as a last resort and on the undertaking that the 30-day period will be used to resolve the issue. The suspension may be extended beyond 30 days if the situation is not resolved to the satisfaction of either Participant. If an extension to suspension is applied, both Participants will bring together senior agency representatives to seek a resolution with a view to re-commencing Personal Data sharing.

4.3 Review

This Agreement will continue until it is superseded by another agreement at a later date, or if either Participant decides to terminate this Agreement, by giving notice in writing. The first, collective review of this Agreement should take place 12 months after it has been signed, and thereafter every year, or sooner if appropriate or if legislation dictates. The Agreement will be subject to document control and approval procedures agreed by the Participants.

4.4 Breaches

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 organisation into disrepute
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission or lawful bases
- loss of availability of personal data

The designated single points of contact are responsible for notifying the other Participant in writing in the event of a data breach / information security incident occurring under this Agreement within 24 hours of the event (via contact details shown in sections 4.1 and 4.2 above).

The single points of contact will discuss and jointly decide the next steps relating to the incident. Such steps will include (but are 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.

5. DATA SHARING PROCEDURES

5.1 Overview

Only the minimum necessary Personal Data will be shared under this Agreement and only when it supports the delivery of the purposes and functions set out in this Agreement.

All reasonable steps must be taken to ensure that anyone who has received Personal Data from either Participant is notified of any relevant changes or inaccuracies.

Each Participant must follow their own organisation's procedures relating to the handling of Personal Data.

5.2 Departments and Business Areas sharing Personal Data

The following departments or business areas of each Participants organisation will share Personal Data under this Agreement:

Organisation	Department or Business Area
HMI Prisons	HMI Prisons
Home Office	Detention Services, International Returns Service Command, Foreign National Offenders Removals Command and Border Force

5.3 Categories of Personal Data to be shared

The Personal Data, including Special Category Data that will be shared under the terms of this Agreement will include, but not be limited to, that set out within Section 3.6. The far-reaching nature of HMI Prison's inspections necessitates the sharing of a wide variety of data that may be relevant to the investigation. However, only the minimum necessary Personal Data, consistent with the purposes set out in this Agreement, will be shared.

5.4 Data Sharing Process

The data sharing process is as follows:

In addition to the documentary evidence provided prior to the inspection, inspectors will look at detention records such as observation books, detainee management systems, performance data, daily wing entries, care plans and detention and training orders, to corroborate their findings. The inspection team may also gather photographic evidence to illustrate conditions that cannot be adequately described or to emphasise a finding, governed by protocols agreed with the Home Office departments in their respective MoUs.

The majority of HO data shared with HMI Prisons will be sent via secure, auditable email accounts - either from HO email mailboxes or from those of contracted commercial suppliers who run HO detention facilities or provide other support services under contract. Where personal data is shared in other ways, either in hard-copy or in other media such as encrypted USB storage devices to share CCTV footage, each party should ensure that a

written record is made of the information that has been shared and taken off site by HMI Prisons' inspectors. In most instances the written record will be in the form of an email between the parties confirming that specific personal data has been requested, shared or received.

The manner in which inspections are conducted is set out in an inspection framework published on the HMI Prisons website. The inspection team will ask the establishment to make available a range of information to assist the inspection process and the documentation will be delivered to the team's base room for the first day of the inspection. Inspectors will be familiar with the information provided which relates to their inspection areas. The documents will be checked before further information is requested from the establishment. Every effort is made to keep requests for documentary evidence and data to a minimum.

6.1 Data Security

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 His Majesty's Government Security Policy Framework (HMG SPF) guidance issued by the Cabinet Office.

HMI Prisons will meet all legal and government requirements for the protection of personal information, records and images accessed on inspection, and will ensure that it uses suitably encrypted media when sharing sensitive electronic data. Detention data will be used, kept or destroyed in accordance with relevant HMI Prisons policy. Both parties to the DSA will ensure that personal data is processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the complementary Law Enforcement Directive (LED), which since May 2018 have been signed into domestic law by primary legislation.

HMI Prisons will ensure that all staff, including partners, have appropriate security vetting, personal photographic identification and security training. HMI Prisons will convey items in and out of the facility related to their designated duties. This will include mobile phones and cameras. HMI Prisons and its partners will take in secure laptops/tablet devices with secure internet access and related mobile media devices as part of the inspection process without the need for individual authorisations.

From time to time, HMI Prisons will be accompanied by visitors who are observing their work, e.g. from other inspectorates, ministers or officials from government departments, or from third sector organisations. In these circumstances the inspection team will contact a senior member of staff (Grade 6 or equivalent) from the respective Home Office department concerned to advise them of which organisations will be accompanying the inspection team, and where any Home Office information is shared with any third-party subsequently provide details to the relevant Home Office department, as set out in Section 5.2.

All third-parties will also be subject to a confidentiality agreement with HMI Prisons, and the personal data supplied to HMI Prisons for the purposes of inspection will not be shared with individuals or organisations who are not exercising a statutory or public function, in accordance with the [BICS Privacy Notice](#).

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 Agreement;
- access to data received by the Participants pursuant to this Agreement must be restricted to employees on a legitimate need-to-know basis, and those employees must have security clearance at an appropriate level;
- the Participants will comply with the Government Security Classifications Policy (GSCP) where applicable.

6.2 Government Security Classifications

Emails used to share Personal Data under the terms of this Agreement will be marked OFFICIAL or equivalent and will only be sent between secure email addresses. Any personal data shared which could have more damaging consequences (for individuals, an organization or government generally) if it were lost, stolen or published in the media should be marked OFFICIAL: SENSITIVE in accordance with the latest Government Security Classifications.

Electronic media must be securely disposed of when no longer required. Breaches of security, confidentiality and other violations of this agreement will be reported in line with each Participant's incident reporting procedures.

6.3 Electronic Storage

The most effective method of storing documents (in respect of this Agreement) will be digital. Protectively marked documents must be stored securely, i.e. in a password protected secure IT system. The use of removable / portable storage devices is to be discouraged but where this is unavoidable this must be on encrypted devices or media which must be securely disposed of when no longer required.

6.4 Mail

As noted in the previous point, the use of digital mechanisms to share information is the first choice. However, it is acknowledged that, at a local level, it is possible that this has to happen *via* standard mail systems. Protectively marked documents that are being mailed internally or externally should be double-enveloped. The inside envelope should have the name and address of the intended recipient and the protective marking – for example **OFFICIAL**. The outside envelope should have the name and address of the intended recipient and a return address in the event that the delivery cannot be made. The outer cover should not show the security marking but should be marked **ADDRESSEE ONLY**.

Special Category Data sent externally should be carried by trusted hand or sent using a courier.

Where paper documents have been created that contain Special Category Data, and they require to be removed from any office for meetings or approved home working, they must be carried securely, preferably in a secure receptacle such as a secure briefcase, box or pouch. The information must remain in the possession of the responsible individual at all times unless it requires to be stored in a secure location.

Special Category Data must not be worked on anywhere where the contents might be seen or viewed by any other person and the information must not be left unattended in any public place. The information must not be entrusted to the custody of a member of the public or left locked in an unattended vehicle.

6.4 Email

All emails should have the appropriate protective marking. Those which do not contain any restricted information do not require a protective heading.

Personal Data, including Special Category Data, may only be exchanged by email if both the sender and the recipient's email systems comply with the Government Secure Email Blueprint or equivalent.

6.5 Retention and Destruction

Once physical documents and electronic data containing Personal Data are no longer required, they must be disposed of in accordance with the internal procedures of the Participants.

7.1 Data Protection Act – Subject Access Requests

Under the Data Protection Act 2018 and the UK GDPR, a Data Subject (or authorised individuals acting on their behalf) has the right to make a Subject Access Request and (subject to certain exemptions) to receive a copy of the Personal Data relating to them which is processed by an organisation. Dealing with such requests is the responsibility of each individual Controller.

If a Participant receives a Subject Access Request, it will be the responsibility of that Participant to follow its organisational guidelines and to deal with the request in line with the Data Protection Act 2018 and the UK GDPR.

7.2 Freedom of Information – Information Requests

HMI Prisons is a Public Authority for the purposes of the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIRs), both as amended or repealed from time to time, and is therefore obliged to respond to information requests in accordance with all provisions of FOIA and the EIRs

Home Office is a Public Authority for the purposes of the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIRs), both as amended or repealed from time to time, and is therefore obliged to respond to information requests in accordance with all provisions of FOIA and the EIRs.


In the event that either Participant receives a request under FOISA, FOIA, EISRs or EIRs and information which is in scope for that request originated from the other Participant, the Participant receiving the request shall seek the views of the originating Participant as to whether the originating Participant considers any of the information to be exempt from the request, and if so the reason why they consider it exempt. It shall remain the responsibility of the Participant receiving the request to determine whether it considers any information to be exempt and to respond to the request accordingly

7.3 Complaints


Any concerns or complaints received from individuals relating to the processing or sharing of their Personal Data will be dealt with promptly and in accordance with the internal complaints procedures of the Participants.

Signed on behalf of the Home Office:

I accept the terms of this Data Sharing Agreement on behalf of the Home Office.

Signature:	
Name:	Basit Javid
Position:	Director General Immigration Enforcement
Date:	21 December 2023

I accept the terms of this Data Sharing Agreement on behalf of HMI Prisons.

Signature:	
Name:	Charlie Taylor
Position:	HM Chief Inspector of Prisons
Date:	17 January 2024