Ministry of Justice

HM Prison & Probation Service

**Policy name:** HMPPS Information Management Policy Framework

**Reference**: n/a

**Issue Date**: 15 April 2026 **Implementation Date**: 15 April 2026

**Replaces the following documents (e.g. PSIs, PSOs, Custodial Service Specs) which are hereby cancelled:** PSI 04/2018 PI 022018

**Introduces amendments to the following documents:** N/a

**Action required by**:

| | | | |
|---|---|---|---|
| X | HMPPS HQ | X | Governors |
| X | Public Sector Prisons | X | Heads of Group |
| X | Contracted Prisons | X | The Probation Service |
| X | Under 18 Young Offender Institutions | X | Other providers of Probation and Community Services |
| X | HMPPS Rehabilitation Contract Services Team | | HMPPS-run Immigration Removal Centres (IRCs) |

**Mandatory Actions:** All groups referenced above must adhere to the Requirements section of this Policy Framework, which contains all mandatory actions.

**For Information:** By the implementation date Governors[1] of Public Sector Prisons and Contracted Prisons must ensure that their local procedures do not contain the following:

Governors must ensure that any new local policies that they develop because of this Policy Framework are compliant with relevant legislation, including the Public-Sector Equality Duty (Equality Act, 2010).

**How will this Policy Framework be audited or monitored**: Compliance with this policy will be monitored by the Departmental Records Officer Team.

[1] In this document the term Governor also applies to Directors of Contracted Prisons.

**Resource Impact**: During the drafting of this policy there have been workshops with those that will be impacted, such as Local Information Managers (LIMs), Regional Information and Security Information Managers (RISALs) and others, so that they can feed in as the policy is being developed. The work required in relation to information management compliance is already happening everyday by staff and this policy will not impact the time already taken by staff to adhere with the policy. It is difficult to attribute time in hours spent on how this currently works or will work in the future as staff are always spending time managing records whether it is completing forms, destroying forms or arranging transfer of records. This work is completed by staff of all grades and in all areas of HMPPS. Although it is hard to quantify hours spent complying with records/information management, the clarity this policy will bring be likely to increase efficiency.

**Contact:** Records_Retention_@Justice.gov.uk

**Deputy/Group Director sign-off:** Ria Baxendale, Deputy Director Information Services Division

**Approved by OPS for publication:** Helen Judge, Chair, Operational Policy Sub-board, March 2026

**CONTENTS**

## 1. Purpose

1.1 Information underpins everything we do, including developing our policies and delivering services to our customers. It informs the evidence-based decisions that we make every day. Good information management ensures that the right information is available to the right people at the right time. This policy sets out HMPPS's information management principles and our peoples' responsibilities and is one of the policies for which the Departmental Records Officer (DRO) is responsible.

1.2 It should be read in conjunction with HMPPS Records Management handbook and the Records, Retention and Disposition Schedule (RRDS). It should also be in read in conjunction with the Government Security Classifications policy. The Government Security Classifications policy can be found at *Government Security Classifications - GOV.UK*. This policy applies to all staff employed by HMPPS, to contractors and agency staff and third-party suppliers who manage information on behalf of HMPPS.

## 2. Outcomes

2.1 Having reliable, complete and authentic records goes a long way to improving efficiency and also ensuring accountability and transparency. Information is a valuable asset that connects us to colleagues and customers and can, through analysis and evaluation, inform future delivery. Success depends on our people having the right information at the right time. HMPPS manages a lot of information which, if mishandled or mislaid, could cause harm to offenders (ex-offenders), victims, family members, staff, individual members of the public or to national security.

2.2 It also ensures we meet our legal obligations with respect to managing information and data including the Freedom of Information Act 2000 (FOIA), Environmental Information Regulations 2004 (EIR), the Data Protection Act 2018, the UK General Data Protection Regulations and the Public Records Act 1958. Section 46 of the FOIA, the Code provides guidance "to all relevant authorities as to the practice which they should follow in connection with the keeping, management and destruction of their records." Part One also states that authorities should have in place a records management policy endorsed by senior management and made readily available to staff at all levels.

## 3. Requirements

3.1 This policy should be read by all staff, particularly those responsible for handling and managing HMPPS information such as Local Information Managers (LIM), Regional Information Security and Assurance Leads (RISALs) and Head of Business Assurance (HoBA).

3.2 Governors, Directors and Deputy Directors of Probation and Heads of Group must ensure that all staff, particularly those responsible for handling and managing HMPPS information LIMs, RISALs and HoBA are familiar with the content of this policy and understand the mandatory actions set out below.

3.3 In addition to this policy, staff must also read and follow the relevant Records Retention and Disposition schedule and the HMPPS Handbook. As this will be regularly updated, staff should ensure they are referring to the most up to date version.

## 4. Guidance

4.1 *Definitions*

4.1.1 ***Records***: the information or data which we need to keep in order to:

- show what decisions we have made, how we have implemented the minister's priorities and how we have spent public money;
- help us to manage our ongoing services and to provide answers required by Parliament or the public (e.g. in response to Parliamentary Questions or Freedom of Information Requests);
- comply with our responsibilities as line manager.

4.1.2 ***Information:*** any individual fact or content, number, image or sound. This can be held or used in any format.

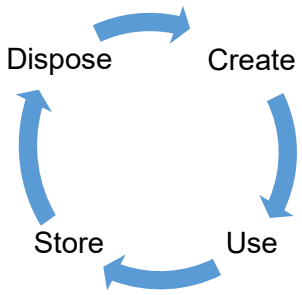
4.1.3 ***Data***: a form of information that is held digitally in a structured way.

4.1.4 ***Personal data***: information relating to an identified or identifiable natural living person.

4.2 *Information lifecycle*

This policy will help all staff manage information properly at each stage of the lifecycle.

*4.2.1*




4.2.2 ***Create*:** Information arrives or is created in a wide variety of formats (such as documents, images or audio).

4.2.3 ***Use***: Information is used, updated or shared during the course of day-to-day business.

4.2.4 ***Store***: Information is filed, stored and protected to ensure it is accessible to those who need it now and in the future.

4.2.5 ***Dispose***: Information reaches the end of its retention period and is either destroyed or preserved.

4.3 *Naming conventions (creation stage)*

4.3.1 Naming conventions make it easier for you, your colleagues and your successors to find information easily and quickly, leaving you more time to focus on the stuff that matters the most. You can share important information swiftly and avoid spending time wondering what the title should be.

4.3.2 Example:

| 2025-01-01 – Guidance – Naming Conventions – Official |
|---|

4.3.3 **Key Date** – This must be in the **YYYY-MM-DD** format. This may be the date the document was created or another relevant date to which the document relates e.g. meeting date.

4.3.4 **Document Type** – This will help narrow down the type of document e.g. Guidance, Policy, Correspondence, Submission etc…

4.3.5 **Document Title –** Clear document title describing what the document is regarding. Use full words, avoid obscure abbreviations and acronyms and use spaces between words.

4.3.6 **Classification –** If a security classification is required use it here, avoiding abbreviations.

4.4 *Legal landscape*

4.4.1 **Section 46 (1) of the Freedom of Information Act – Code of Practice ("the Code")**
Section 46 (1) of the Freedom of Information Act 2000 (FOIA) requires the Secretary of State for Digital, Culture, Media and Sport (DCMS) to issue a Code of Practice "providing guidance to relevant authorities as to the practice which should be followed with regards to the keeping, management and destruction of records."

4.4.2 **Freedom of Information Act 2000 (FOIA)**
The FOIA governs what information can be disclosed to the public.

4.4.3 **Public Records Act 1958 (PRA)**
The PRA imposes duties on government departments to select records for permanent preservation and preserve them under the guidance of the Keeper of Public Records.

4.4.4 **Constitutional Reform and Governance Act 2010.**
This legislation reduces the length of time that we hold records in the department, court or tribunal before the records are transferred to The National Archives (the '20- year rule'). For records sent to TNA, the transition period ends in 2022. For records sent to other places of the deposit (local authority archives), the transition period ends in 2024.

4.4.5 **Inquiries Act 2005**
The Inquiries Act 2005 gives statutory Public Inquiries the authority to require government departments to keep records and information that we would normally destroy (known as a moratorium).

4.4.6 **Copyright, Designs and Patents Act 1988**
This legislation sets out the legal, economic and moral rights in intellectual property, governs the reuse of information created by third parties and defines Crown and Parliamentary Copyright.

4.4.7 **Reuse of Public Sector Information Regulations 2015** (RPSI)
RPSI sets out a department's responsibilities for permitting the reuse of its Crown Copyright information.

4.4.8 **Section 45 of FOIA**
Requires the Minister for the Cabinet Office to publish a Code of Practice which provides guidance to public authorities on the discharge of their functions and responsibilities under Part I (Access to information held by public authorities) of FOIA.

4.4.9 **Regulation 16 of the Environmental Information Regulations 2004**
Requires the Secretary of State for Department for Culture Media and Sport (DCMS) to issue a Code of Practice on the discharge of the obligations of public authorities under the Regulations.

4.4.10 **Data Protection Act 2018 and UK General Data Protection Regulations 2018**
Requires everyone who is responsible for processing personal data must follow the data protection principles.

4.5 *Roles and responsibilities*

4.5.1 Departmental Records Officer

- Overall responsibility for the management of the department's records.
- Oversee the lifecycle of information and records complies with legislation.
- Ensure the principles of the Code are adhered to so that all parts of the organisation know why we keep different categories of information and that we destroy information when they no longer need it.
- Monitor compliance with the Code, reporting to the Information Security and Risk Board and, if necessary, the Permanent Secretary and/or the Executive Committee (ExCo).
- Assess HMPPS's policies and procedures against the requirements of the Code at regular intervals and update them.
- Assess HMPPS's performance against the requirements of the Code and recommend measures to improve performance.
- Ensure that HMPPS has policies on retaining and destroying information, and that it can explain its decisions.
- Ensure HMPPS destroys information consistently and in line with its policies and the sensitivity or security classification of the information; and, where destruction is carried out by a contractor, that it is certified.

- Ensure that HMPPS's procedures mean that when information is destroyed, all known copies and versions including back-ups are also destroyed and cannot be recovered, taking into account that the efforts should be proportionate to the sensitivity and security classification of the information.
- Oversee the selection and transfer of records to The National Archives (TNA) or other places of deposit, ensuring that the sensitivity of the records is assessed and, where necessary, appropriate FOI exemptions are applied to records or parts of records selected for permanent preservation.
- Supply TNA with data on information and records on request and work with the Advisory Council on National Records and Archives as necessary.
- Be the central point of contact for enquiries about access to, or reuse of, records that have been transferred to places of deposit in The National Archives or local authority archives, where those records are not yet available to the public (except for requests from researchers applying for access through existing panels such as the HMCTS Data Access Panel and the HMPPS National Research Council).

4.5.2 Local Information Manager (LIM)

- Understanding the requirements of this policy and supporting documents on how to manage records.
- Completing the selection and transfer of records to local archives.
- Together with the Deputy LIM, identify local information assets and ensure that they are recorded in an Information Asset register on One Trust.
- Managing the storage, retention and disposition of records in line with the RRDS.

4.5.3 Regional Information Security and Assurance Leads (RISALs)

- Understanding the requirements of this policy and supporting documents on how to manage records.
- Promoting a positive information management culture. Raising awareness on best practice and individual responsibilities.
- Being the first point of contact and subject matter expert for information management related questions.
- Provide ongoing advice, guidance and support to staff in improving their knowledge and awareness of information assurance.

4.5.4 Head of Business Assurance (HoBA)

- Understanding the requirements of this policy and supporting documents on how to manage records.
- Promoting a positive information management culture. Raising awareness on best practice and individual responsibilities.
- Being the first point of contact and subject matter expert for information management related questions.

- Provide ongoing advice, guidance and support to staff in improving their knowledge and awareness of information assurance.
- Support the Business Hub Manager to investigate and report findings following an incident to the relevant team.

4.5.5 Information Asset Owner

- Responsible for ensuring specific information assets are handled and managed appropriately.
- Lead a positive information management culture that values, protects and uses information for public good.
- Ensure there are appropriate mechanisms in place to only give access to information assets on a need to know basis and monitor appropriate use.
- Identify, record, manage and mitigate risks associated with your information assets. Maintain local risk register and provide assurance to Deputy Senior Information Risk Owner.

4.5.6 Senior Information Risk Owner (SIRO)

- Accountable for the management of risks. Work with teams within the organisation to identify, understand, manage and report on the key information risks, ensuring Departmental wide risks are escalated to the Information and Security Risk Board.
- Foster a culture that protects and uses information for the public good by knowing what information is held, how it is stored, shared and protected.
- Ensure staff are aware of and understand their responsibilities for good information handling and that mechanisms are in place to enable staff to discharge these responsibilities.

4.6. *The Information Management Principles*

4.6.1. We will create, save and store information in the right location including the corporate memory repositories.

4.6.2. We will ensure that information is appropriately protected and available for use and reuse by the right people.

4.6.3. We are committed to the MoJ's (HMPPS) core values, including Openness, so we publish and disclose information when we can.

4.6.4. We update or amend information to ensure that it is accurate (when necessary).

4.6.5. We do not keep information longer than is necessary and we know how to dispose of the information (i.e. when to return it, when to pass it to someone else and when to destroy it).

4.6.6. We do not hold corporate information on personal devices, in personal email accounts or on non-corporate systems except in justified exceptional circumstances, and we transfer the information to corporate systems as soon as possible, deleting the information from its original location in line with the guidance on Using non-corporate communication channels for government business. Guidance is available at: https://www.gov.uk/government/publications/non-corporatecommunication-channels-for-government-business

4.6.7. Where the information is part of the corporate memory, we follow the relevant Records Retention and Disposition Schedule (RRDS).

4.6.8. We comply with legal requirements (see paragraph 4.4).

4.6.9. When we move to a new role, or leave HMPPS, we ensure that all information that we hold is either moved to the corporate memory or deleted in line with guidance.