HM Prison & Probation Service

Records, Information Management and Retention Policy

This instruction applies to:		Reference:
All staff directly employed by HQ corporate; Prisons and Providers of Probation Services and other contracted services		**PSI 04/2018** **PI 022018** **AI 03/2018**
Issue Date	**Effective Date**	**Expiry Date**
25 May 2018	**25 May 2018**	
Issued on the authority of	Operational Policy Sub-Board	
For action by	All staff responsible for the development and publication of policy and instructions *(Double click in box, as appropriate)* ☒ HMPPS HQ ☒ Public Sector Prisons ☒ Contracted Prisons* ☒ National Probation Service (NPS) ☒ Community Rehabilitation Companies (CRCs) ☒ HMPPS Immigration Removal Centres (IRCs) ☒ Other Providers of Probation and Community Services ☒ Governors ☒ Heads of Groups ☒ HR Business Partners ☒ Shared Services ☒ Line Managers **** If this box is marked, then in this document the term Governor also applies to Directors of Contracted Prisons***	
Instruction type	***Information and Assurance***	
For information	All staff directly employed by Public Sector Prisons and HMPPS HQ	
Provide a summary of the policy aim and the reason for its development / revision	The purpose of this Policy is to ensure that HMPPS handles and treats information appropriately during the end-stages of the information lifecycle resulting in its eventual disposal. The Policy amalgamates and replaces three previous policies (PSI 35/2014, PI 28/2014, and PI 59/2014) with the aim to demonstrate consistent and joined up requirements across our operational Prison and Probation estates and Corporate functions.	
Contact	HMPPS Information Management and Security ☎ 0203 334 0324	
Associated documents	The Data Protection Act 2018 and General Data Protection Regulation; The Freedom of Information Act 2000 (FOIA); the Environmental Information Regulations 2004 (EIR); the Public Records Acts 1958 and 1968 (PRA); and the Public Records (Transfer to the Public Record Office) (Transitional and Savings Provisions) Order 2014.	

Replaces the following documents which are hereby cancelled: - PSI 35/2014; PI 28/2014 and PI 59/2014
Audit/monitoring: Mandatory elements of instructions must be subject to management checks (and may be subject to self or peer audit by operational line management/contract managers/HQ, as judged to be appropriate by the managers with responsibility for delivery. In addition, HMPPS will have a corporate audit programme that will audit against mandatory requirements to an extent and at a frequency determined from time to time through the appropriate governance.
Introduces amendments to the following documents
Notes: All Mandatory Actions throughout this instruction are in *italics* and must be strictly adhered to.
Glossary of terminology: Where you read Local Information Manager (LIM) maybe referred to ISM within the NPS & CRCs.

CONTENTS

1. Executive summary

Background

1.1 In the course of business, Her Majesty's Prison and Probation Service (HMPPS) collects information from Offenders in HMPPS custody, Other Government law enforcement agencies, third party contracted partners and external organisations, which subsequently generates a wide range of records. The purpose of this policy is to define the framework by which HMPPS governs Records, Information Management and Retention management and, in particular, guide in the management of paper and electronic 'digital' records with particular reference to creation, retention and disposal.

1.2 Retaining records for the right length of time is necessary to support business requirements, to comply with legislation, including the Freedom of Information Act 2000 (FOIA), Data Protection Act 2018 (DPA) and General Data Protection Regulation, Public Records Acts 1958 and 1968 (PRA); and the Public Records (Transfer to the Public Record Office) (Transitional and Savings Provisions) Order 2014.

1.3 The principal legislation governing the management of records is stipulated in Section 46 of the FOIA. This directs organisations under the Act to have records management systems, which will help them to conduct their statutory function compliance. Further information on statutory obligations can be found at Annex A in the guidance.

1.4 The DPA, which was replaced by the new regime for data protection from 25 May 2018, is an act legislating in which information about living people may be legally used and handled. The main intent is to protect individuals against misuse or abuse of information about them. HMPPS offender / service user's; corporate; project and authority data defined by an individual contract records are governed accordingly under the DPA. It sets in law how personal and sensitive personal information is handled in six major sections. The parts below outline the basic rights of data subjects, methods in which data may be handled by those who possess it, special exemptions and modes of enforcement.

The fundamental principles of DPA 2018 and General Data Protection Regulation specify that personal data must:

1. be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
2. be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
3. be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
4. be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
5. be kept in a form, which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the

appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation'); and

6. be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

1.5 All HMPPS records are Public Records under the Public Records Act. HMPPS will take actions as necessary to comply with the legal and professional obligations set out in the Records Management: Code of Practice, in particular

1.6

- The Public Records Act 1958 and 1968;
- The Public Records (Transfer to the Public Record Office) (Transitional and Savings Provisions) Order 2014;
- The Data Protection Act 2018 and General Data Protection Regulation;
- The Freedom of Information Act 2000;
- The Common Law Duty of Confidentiality;
- Copyright, Designs and Patent Act 1988; and
- Any new legislation affecting records management or other legislation concerning information / intellectual property arises.

1.7 There are potential risks associated with retaining records for too long or not long enough. If records are disposed of too soon, HMPPS may not have the evidence it requires to protect itself in the event of litigation, whilst premature destruction can also be seen as an attempt to prevent necessary disclosure leading to miscarriages of justice and / or reputational damage. If, records are retained for too long, this may hinder the retrieval of information for evidential purposes, Subject Access Requests under the DPA and for FOI requests. Unnecessary physical and digital retention may also incur HMPPS additional costs for asset storage.

1.8 This policy aims to provide an applicable framework to guide all areas managing corporate records as well as offender / service user records within their capacity of HMPPS respective to HQ corporate, prisons, both the National Probation Services (NPS) and Community Rehabilitation Company's (CRCs).

In line with the DPA principles at 1.4 above HMPPS, NPS, CRCs and contracted third parties particularly ensure that:

- Records are identified and classified to enable appropriate treatment;
- Provide clarity to HMPPS and private providers of custodial or probation services on the treatment of offender records;
- Records are retained for the right length of time;
- Records are regularly reviewed to identify retention and disposal actions;
- Destruction of records is properly documented as required;
- Corporate and offender records must be physically and digitally transported between functions in accordance with the appropriate jurisdiction and protecting both the individuals' and organisation's confidentiality and integrity; and
- Historical records are preserved and transferred to the appropriate repository (The National Archives or local Place of Deposit).

Desired outcomes

1.8 The policy and guidance document aims for an improved consolidated format and greater clarity to incorporate recent organisations that have joined the HMPPS. It takes into account present legislation and provides a coherent instruction.

Mandatory actions

1.9 All senior managers throughout HMPPS, CRCs, contracted prisons, and contracted third parties must make sure that staff and line managers apply all statutory legislation; the Data Protection Act 2018 and General Data Protection Regulation; Freedom of Information Act 2000 (FOIA); the Public Records (Transfer to the Public Record Office) (Transitional and Savings Provisions) Order 2014, the Environmental Information Regulations 2004; and Public Records Acts 1958 and 1968 (PRA) in support of keeping HMPPS records safe.

1.10 The LIM role (defined in the guidance) must be implemented within HMPPS by the Information Asset Owner (IAO) being the accountable officer. The IAO also must ensure the appointment of an Information Manager. These responsibilities should be recorded and specified in the SPDR.

Resource Impact

1.11 There should be minimal resource implications resulting from the re-issue of this policy, with no changes to existing provisions.

Simon Boddis
Executive Director
Prison Estate Transformation

2. Roles and responsibilities

Who does this policy apply to?

2.1 All staff responsible for handling HMPPS information and managing records must read this policy. The Local Information Manager (LIM) and any other member of staff who is responsible for making decisions about the retention and disposal of records must be fully versed with all sections of this policy including the disposal schedules.

2.2 Processes in this policy for managing records of offenders / service users / corporate / project data (records relating to the management of offenders as defined at 1.11 (2)) apply to public sector or private providers of prison and/or probation services / HQ corporate / contracted third parties / service users.

2.3 CRCs are their own data controllers in common with but not jointly with MoJ. They are individually accountable directly to the Information Commissioner under the provisions of the DPA. As the (CRCs are data controllers in common with the HMPPS). This instruction will support their obligations outlined in Schedule 18 & 19 of the contract between each of the CRCs and the Secretary of State.

2.4 In accordance with the Public Records Act 1958, each government department must appoint a Departmental Records Officer (DRO) who leads on departmental compliance with PRA 1958 from the time of creation until disposal or transfer to the National Archives. Further information on the DRO's definition of responsibilities can be found on www.nationalarchives.gov.uk.

Statutory Responsibilities:

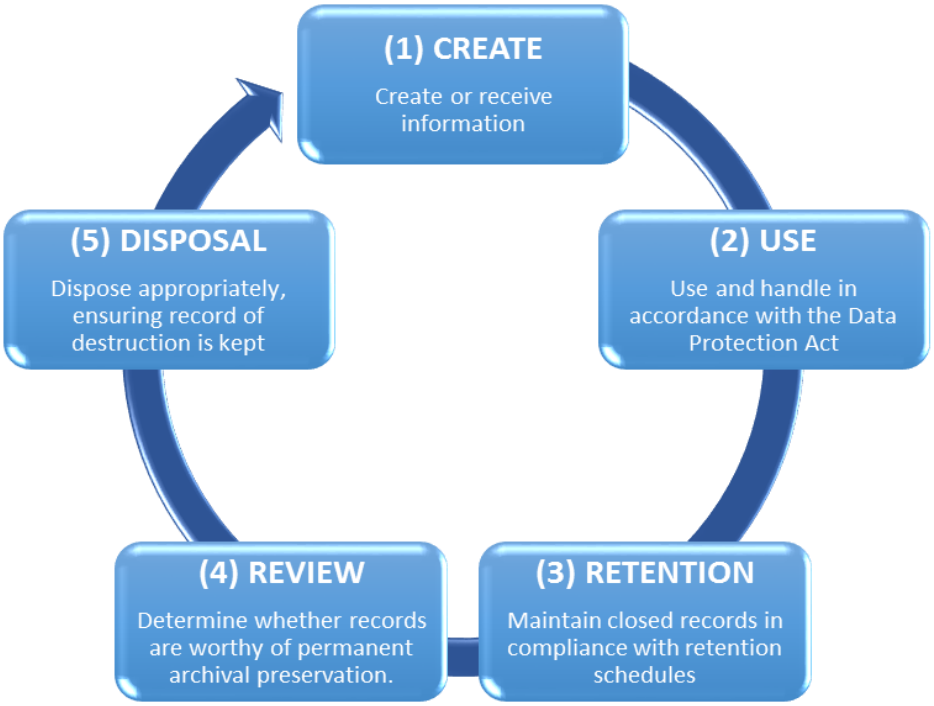
2.5 All records held are subject to The Data Protection Act 2018 and General Data Protection Regulation; the Freedom of Information Act 2000 (FOIA), the Public Records (Transfer to the Public Record Office) (Transitional and Savings Provisions) Order 2014; and Environmental Information Regulations 2004 (EIR); and must therefore be processed in such a way to facilitate access in an accurate and timely manner. In Part One of the Lord Chancellor's Code of Practice on the management of records issued under Section 46 of the FOIA, the Code provides guidance "to all relevant authorities as to the practice which it would, in the opinion of the Lord Chancellor, be desirable for them to 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.

The HMPPS is therefore required to ensure that they are compliant with this Instruction in order to meet the requirements of this Code of Practice. In addition, HMPPS has to discharge its responsibilities to the Ministry of Justice (MoJ), under Section Three of the Public Records Act 1958, which prescribes that each Government Department should appoint a Departmental Record Officer to be responsible for its records from the time they were created or first reviewed until their destruction or transfer to the Public Records Office. The MoJ Departmental Records Officer (DRO) has responsibility for all records managed by HMPPS.

Definition and lifecycle of a record

2.6 A key aim of this policy is to make clear the entire 'lifecycle' of record retention. In particular from the point of creation, receipt, through the period of its active use, then into a period of inactive retention (such as archive files which may still be referred to occasionally) and finally either disposal or permanent preservation.

"Lifecycle" of a record



2.7 British Standards ISO 15489 defines records as "information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business".

2.8 The International Council on Archives (ICA) Committee on Electronic Records defines a record as "recorded information produced or received in the initiation, conduct or completion of an institutional or individual activity and that comprises content, context and structure sufficient to provide evidence of the activity."

2.9 The key word in these definitions is *evidence*. In summary, a record can be defined as *evidence of an event*.

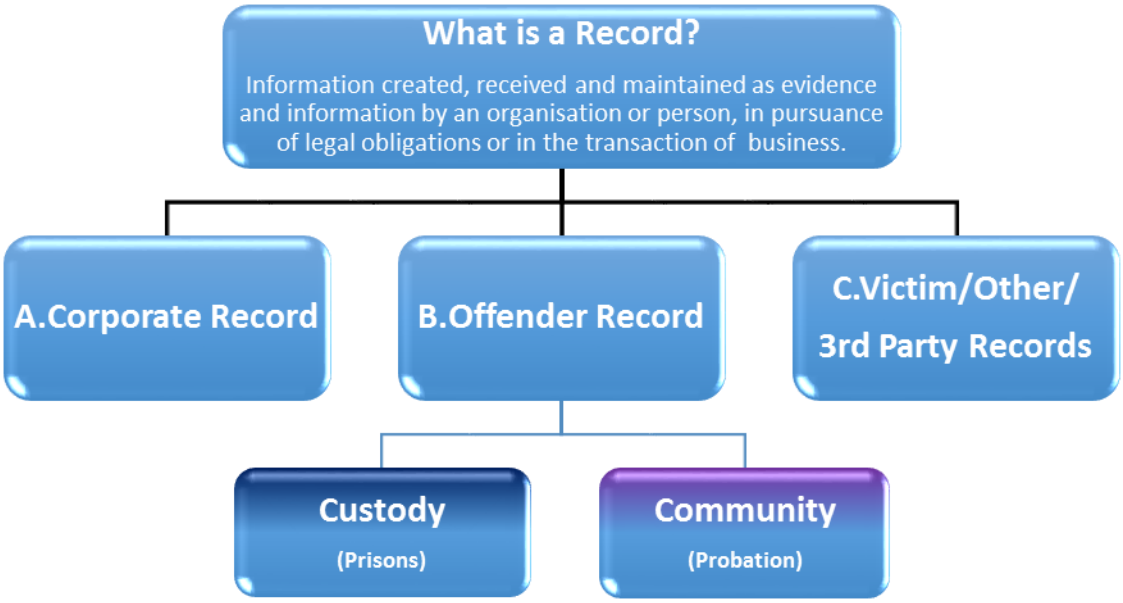
2.10 Identified records in HMPPS can be classified into three types,

A. **Corporate Record (not inclusive of CRCs)** - records that are part of the HMPPS corporate memory, providing evidence of actions and decisions that support daily functions and operations as an organisation. Records support policy formation and managerial decision-making. All administrative records (e.g. personnel, estates, financial and policy).

B. **Offender Records / Service Users** – any information that relates to the effective management of an offender and supports HMPPS in ensuring they serve the sentences and orders handed out by courts, both in prisons and in the community should be included as part of that offender record / service users and stored on the appropriate case management system and/or in the file. Paper records can be further sub divided into Custody (prisons) and Community (probation).

C. **Victim/Other/3rd Party Records** – records relating to other service users that are not defined under A or B above, i.e. are not an employee or an offender.

2.11 HMPPS record classification flowchart



Policy Statement

2.12 The Ministry of Justice Department Records Officer (DRO) has responsibility for all records managed by HMPPS. The DRO must be advised of any new business function which may create new types of HMPPS records. Contact HMPPS Information Management & Security team in the first instance with any queries at InformationmgmtSecurity@hmps.gsi.gov.uk.

2.13 This section defines the roles and responsibilities around the mandatory requirements and expected outcomes that all users of HMPPS information must comply with, inclusive of the key principles in record management, contracts and relevant legislation.

2.14 The following section details the general mandatory responsibilities and describe the expected requirements at each stage of the records' lifecycle.

MAINTAINING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY

2.15 Managers and employees, and all parties involved in operating records are expected to maintain confidentiality. If one employee breaches another's right to confidentiality, this may be treated as a disciplinary offence, depending on the circumstances.

2.16 **Confidentiality, Integrity and Availability** of information are a set of rules that limits access to information, integrity is the assurance that the information is trustworthy and accurate, and availability is a guarantee of reliable access to the information.

Managers and employees are expected to adhere to these rules and they are designed to prevent sensitive information from reaching the wrong people, while making sure the right people can in fact get it: access must be restricted to those authorised to view the data in question.

Integrity involves maintaining the consistency, accuracy and trustworthiness of data over its entire life cycle and availability is best ensured by rigorously maintaining all hardware and maintaining a correctly functioning operating system.

Statement of compliance

2.17 *In order to confirm that the requirements of this policy are being met by HMPPS, CRCs, third party contracted services, each Prison, NPS Division and HQ Directorate must complete and return an annual 'statement of compliance', by the end of each financial term* ***31 March*** *to* InformationmgmtSecurity@hmps.gsi.gov.uk.

2.18 Information provided in the statement of compliance may be used during subsequent audits.

3. Create

This section outlines procedures and requirements linked to stage 1 of the lifecycle of a record: **creating or receiving information.**

Named conventions

3.1 Naming conventions help identify records and folders using common terms and titles. They also enable users to ascertain between similar records to determine a specific record when searching the electronic or physical file system.

3.2 Naming conventions need not be overly prescriptive or formalised but must be:

- Clear and well defined;
- Convey an idea of the content that is understandable;
- Identifiable – specifying the type of document, e.g. minutes, contract; draft; final, will assist access;
- Concise - avoiding repeating information that can be gleaned from the name of the folder in which the file will be stored will assist access; and
- Consistent naming - enabling ease of reference.

3.3 Without naming conventions the context of the record becomes meaningless to anyone other than the creator, creating the unnecessary need to explore the contents of each individual record to avoid the risk of records being destroyed or lost.

Emails

3.4 There is a need for specific guidance on naming conventions for emails. An email's subject line is offered by Outlook and / or your current e mail service as a default filename which is rarely a good idea to accept as composition and accuracy can vary or have changed over the course of an exchange.

3.5 Email records which are judged to be records must be stored appropriately and protected from unauthorised deletion. Retention periods must be established in accordance with the guidance. Business e mails should not be stored in a personal folder but moved to a dedicated area of a shared drive that justifies retention.

3.6 Emails within your current Case Management System (CMS) should be saved using:

- **.msg** format, for the reason that this format preserves all metadata and attachments as part of a single saved file.

- a filename of **yyyymmdd – subject**
- **FW** or **RE** removed to reduce length

3.7 If leaving the organisation or moving to another area of work, staff must ensure that electronic records (including emails) are clearly described and accessible to colleagues and team members before their departure.

Records from external agencies

3.8 Any documents or files received from third party contracted partners, (e.g. Police authorities, Crown Prosecution Service etc.), which HMPPS has no requirement to retain, must be securely returned to the sender unless otherwise agreed in writing to securely dispose on site.

4. Use

This section outlines procedures and requirements linked to stage 2 of the lifecycle of a record: **use/handling in accordance with the Data Protection Act**.

4.1 All records must be initiated and, at the appropriate time, terminated/closed on the relevant case management system(s).

4.2 Accurate and up-to-date records must be maintained at all times whilst active.

4.3 Any information that is judged to be part of the offender record must be recorded in the appropriate case management systems. This applies to all users of HMPPS information that is classed as offender / service user's records.

- Hard copies of relevant Prisons documents must be placed in the paper record (F2050).
- Hard and electronic copies of relevant Community Offender documents must be uploaded to nDelius.

4.4 Mandatory instructions for CRCs on the management of offender / service user's records at the end of engagement can be found under supporting guidance at section 2.1 CRC Management of offender service records at the end of engagement.

4.5 Medical confidential information must be stored in line with the NHS guidelines. Further information can be found on www.nhs.uk.

4.6 Sharing of records must be considered in conjunction with AI 12/2016, PSI 16/2016, PI 15/2016 Information Sharing Policy.

4.7 All offender / service user records must be terminated / closed on the appropriate CMS once each element of the sentence, including custody, periods of licence and/or post-sentence supervision has been completed.

4.8 All offender / service user records are subject to the Data Protection Act 2018 and General Data Protection Regulation; the Freedom of Information Act 2000 (FOIA); the Public Records (Transfer to the Public Record Office) (Transitional and Savings Provisions) Order 2014; the Public Records Act 1958 (PRA); and must therefore be processed in such a way to facilitate access in an accurate and timely manner.

4.9 Consideration should be given to identifying vital records in the local business continuity plan. Vital records are records which are essential for the continuation of the business following a disaster (including both paper and electronic records), for e.g. fire or flooding.

Vital records must be recorded on the Information Asset register in accordance with AI 18/2014, PSI 24/2014, PI 18/2014 Information Assurance.

5. Retention

This section outlines procedures and requirements linked to stage 3 of the lifecycle of a record: **Maintaining closed records in line with retention schedules.**

5.1 Records that are no longer live (i.e. not in active use) are sometimes referred to as **archive records.**

5.2 Retention periods apply to records in whatever format they are created/held. Retention and destruction of electronic records must be managed as well as those held on paper and follow the same rules.

5.3 Retention periods are based on the requirements of the Data Protection Act 2018 and General Data Protection Regulation and the Public Records Acts 1958 and 1968. Any retention period should be treated as a benchmark as there might be situations where the data should be held for a minimum or longer periods than those recommended in the Record Retention Disposition Schedule (RRDS) any deviation should be documented fully. These periods may also be altered by subsequent legislation or organisational instructions.

5.4 Records must be stored in appropriate conditions. In particular, the LIM's must ensure that:

- Records are protectively marked and securely stored in accordance with AI 18/2014, PSI 24/2014, PI 18/2014 Information Assurance.
- Records are clearly labelled and organised and can be retrieved quickly when required.
- For paper records, they must be stored in conditions which are free from damp or damage by vermin and with restricted & controlled access.

Retention Periods for Personal Data

5.5 The DPA states (principle 5) that organisations must not process (which includes "retain") personal data for any longer than is required to fulfil business' needs.

5.6 In accordance with the provisions of the appropriate RRDS, personal records on staff must be reviewed regularly and destroyed when no longer required.

5.7 In the event of a Subject Access Request (SAR) being made, we must search for, copy and provide all personal data held even if it is no longer in use.

Side note: There are cost implications from unnecessary storage of records.

Retention Periods for Non-Personal Information

5.8 Freedom of Information Act 2000 (FOIA) compliance relies on the ability of the business to identify and locate the information sought in an accurate and timely way.

5.9 The correct use of registered files will assist in meeting this requirement of the act. A regular critical examination of information held is essential to avoid holding data longer than is required.

5.10 Retention period is dependent on record type and is classified in 3 ways:

A.Corporate Record	B. Offender Record	C. Victim/Other/3rd Party Record
•Based on type and nature of the record. • 3-5 years for auditable records (dependant on audit cycle) •6 years after leaving service for employee records •7 Years (6+1) for majority of primary finance records. •100 years from date of birth or 5 years after date of last action for any records which have a bearing on pensions	•Based on Sentence length of the the Offender. •Usually 6 years from termination or release for determinate sentences. •99 years from date of birth for lifers.	•Based on date of last contact. •Usually 6 years to cover limitation period.

Records Retention and Disposal Schedules (RRDS)

5.11 Record Retention and Disposal schedules are the means by which the Ministry of Justice manages its compliance with the Public Records Act. The different RRDS for the types of record held by HMPPS can be found in the accompanying guidance documents and must be followed:

- **Corporate Records RRDS** and guidance can be found in supporting guidance under:
  3.2 Corporate Records RRDS
  3.3 Corporate Records Guidance
  3.4 Investigations
  3.5 Projects

- **Offender Records RRDS** and guidance can be found in supporting guidance under:
  3.6 Offender Records RRDS
  3.7 Custodial Records Flow Diagram
  3.8 Community Records Weeding List

- **Victim Records RRDS** and guidance can be found in supporting guidance under:
  3.9 Victims RRDS
  3.10 Visitors

5.12 The retention periods in these schedules must be followed, unless there is clear justification to deviate in which case guidance below must be followed. **See 5.13.**

5.13 For shared drives and other electronic repositories, including local systems, retention periods must be established following above RRDS guides.

Exceptions to retention periods

5.14 If records from a previous receipt into custody have not yet been destroyed, these "back records" (including any electronic records where available) must be requested by the receiving establishment as soon as the offender has re-entered custody. The back records must be retained with the records for the current receipt into custody.

5.15 In some cases, it is acceptable and a legal requirement to retain the records for longer than the established retention period. Examples include:

- If a record is due for destruction but is known to be the subject of a request for information, destruction should be delayed until disclosure has taken place, or if the authority has decided not to disclose the information, destruction should be delayed until the complaint and appeal provisions have been exhausted.
- If records relate to an event or incident which is subject to an ongoing investigation, complaint or appeals process (and may be required as evidence)
- **If an offender is unlawfully at large, no part of the offenders file may be destroyed until the offender has been returned to custody, irrespective of the sentence expiry date up to a maximum of retention period of 99 years from date of birth.**

5.16 Retention of records beyond the prescribed or established retention period must be justified and documented by an Information Asset Owner, where possible on the file or record itself.

6. Review

This section outlines procedures and requirements linked to stage 4 of the lifecycle of a record: **determining whether records are worthy of permanent archival preservation.**

6.1 The review of records is the appraisal process which establishes what action should be applied to that record, for example whether all or part of the record needs to be further retained and if so for how long, whether it can be destroyed or whether it should be transferred to another repository for permanent preservation e.g. the National Archives. Practical guidance on how to carry out a review is included in supporting guidance, section 4.2 Key Disposal Considerations.

Appraisal for Historical Records (written by the National Archives)

6.2 Under the Public Records Acts 1958 and 1967 (see www.nationalarchives.gov.uk), HMPPS is required to identify records of historical value with a view to permanent preservation and making them available to the public. There is also a wider duty to retain historical objects, such as those items formerly held by the Prison Service Museum. Only a small proportion of records (usually less than 5%) will fall into this category. For example, if the notoriety of the offender or an offence merits the permanent preservation of the record for historical reasons.

6.3 The IAO or LIM should conduct a preliminary assessment to establish whether the records are of possible historical significance and should be considered for preservation at the National Archives or other approved repository. There is a **statutory requirement** for this work to be done under the supervision of the National Archives, so in the first instance the IAO or LIM should provide a list of the records to the HMPPS Information Management & Security Team who can discuss the selection criteria with the National Archives.

6.4 Further guidance on the selection and arrangements for the transfer of permanent records can be found under supporting guidance, section 4.1: TNA Permanent Records Guidance (see www.nationalarchives.gov.uk).

Review of Records

6.5 All records must be reviewed before a decision is taken about their destruction. A check must be made using the appropriate records management system in order to establish the status of the individual prior to destruction. The procedures below must be followed in order to decide what action should be taken with the file at the end of its retention period. Further guidance on key retention/disposal considerations can be found under 4.2 Key Disposal Considerations under supporting guidance.

6.6 If an offender is unlawfully at large (UAL), the file must be retained in its entirety, irrespective of sentence expiry date. This includes offenders who are unlawfully at large following recall after initial release. UAL records should be subject to regular review with a maximum retention period of 99 years from date of birth. If the individual has been returned to custody the records must be transferred to the establishment where the offender is being held.

6.7 If an offender / service user has returned to custody or community supervision for any reason e.g. recall or new offence, the records must be transferred to the establishment where the offender is being held or appropriate provider of probation service and any previous records requested (either under community archive retrieval or back records request).

6.8 If the offender / service user's sentence (or period of suspension if a suspended sentence), has not yet expired **records relating to the sentence and licence* must be retained until the sentence expiry date** when a further review must be carried out.
Other offender related records may be destroyed if there is no business justification for retaining them until the sentence expiry date.

***Records relating to the sentence and licence** shall include but are not limited to:

- Warrants (remand warrants and orders of imprisonment)
- Orders (Appeal, Recall etc.)
- Calculation sheets
- Court record sheets
- Indictments
- Copy of the release licence(s)
- Evidence of added days awarded on adjudication

Back records

6.9 When an offender re-enters custody or on a community order, there may be older records that have not yet reached its destruction date, these older records must be weeded when they reach their destruction date and only information that is pertinent should be retained and added to the newest record. Reason for retaining information must be recorded in the retained record.

7. Disposal

7.1 This section outlines procedures and requirements linked to stage 5 of the lifecycle of a record: **disposal, ensuring record of destruction is kept.** Further details about the moratorium can be found in the guidance at 4.3.

Destruction of records

7.2 Destruction of all records must be carried out in accordance with the instructions with Information Assurance and IT Security Policies, with reference to protective marking and data handling. In particular, staff responsible for the destruction of records must note the following:

- Under no circumstances must paper documents containing personal data or confidential information be simply deposited in an insecure waste bin. To do so could result in unauthorised disclosure of such information to third parties and render HMPPS / data controllers liable to prosecution or other enforcement action by the Information Commissioner. These records must be securely shredded.

- All instances of the records in multiple manual and electronic filing systems (including any records handled by a local external service provider) must be destroyed or deleted.

- Appropriate local arrangements must be put in place with any local service provider for them to either return their records to HMPPS for destruction, or for the service provider to provide HMPPS with an approved destruction log confirming that they have destroyed the records in their possession in accordance with our destruction instructions.

- Destruction of records should be recorded on the destruction log and if necessary indicate that it was a partial destruction of the file. A template Destruction Log can be found under supporting guidance, section 5.1 Destruction Log.

7.3 The destruction log must contain sufficient information from the records to identify positively, which records have been destroyed. In the case of core offender files, this must include (see guidance template log at the last page):

- Type of record destroyed;

- Destruction date;

- Method of destruction;

- Authorisation of Destruction

7.4 The destruction log must be retained for 99 years from the date of the first entry on the log and then destroyed.

7.5 The destruction log must be stored securely and must be produced when required by audit or other regulatory body.

7.6 The destruction log can be held on paper or electronically regardless of format; the LIM must ensure that the destruction log and procedures for its management follow the standards set out in the following bullet points:

- The appropriate access controls are put in place.
- Access and editing procedures ensure the integrity of the log is maintained and unauthorised alteration is prevented.
- Reasonable controls are in place to protect the destruction log from accidental deletion. It is acceptable to hold more than one destruction log within a working area. The LIM must know how many logs there are and be able to access each destruction log when required.
- Destruction of electronic records must be recorded on the destruction log.