Ministry of Justice

HM Prison & Probation Service

Operational and System Assurance Group (HM Prison & Probation Service)

Records Retention and Disposition Schedule

Introduction

1. This schedule has been drawn up following consultation between Operational and System Assurance Group (OSAG) of HM Prison & Probation Service (HMPPS) and staff working for the Departmental Records Officer (DRO) in the Ministry of Justice.

2. As a public body, the MoJ takes its responsibilities for managing information seriously. These responsibilities include compliance with the Public Records Act 1958, General Data Protection Regulation, the Data Protection Act 2018, Freedom of Information Act 2000 and amending legislation. The MoJ uses Records Retention and Disposition Schedules (RRDSs) to manage its compliance with its statutory obligation to identify what we hold, how long we keep it and what should happen to these records at the end of that time.

3. OSAG's work is governed by the Crown's common law powers, as limited by the restraints of public law and constitutional principles. OSAG records are not selected for permanent preservation.

4. This schedule is split into two:

    a. Records unique to the Operational and System Assurance Group
    b. Records held by various teams within the MoJ and its associated bodies and where a common retention and disposition policy is applied.

5. This is a new RRDS which has been developed due to the unique records held by OSAG and which are not covered by the HMPPS RRDS (also known as Prison Service Instruction 04/2018).

6. For the purposes of clarification, records are checked annually at the start of each financial year (i.e. in April) and, where appropriate, destroyed.

7. If a Freedom of Information Act 2000 request or a subject access request under the General Data Protection Regulation and Data Protection Act 2018 is received, **a hold must be put on the destruction of relevant records until 20 working days after the request is resolved**.

8. While the Independent Inquiry into Child Sexual Abuse (IICSA) continues its investigations, the moratorium on the destruction of records of potential interest to IICSA remains in place. All government departments and their associated bodies (in common with other public sector bodies) are required to comply with the moratorium. All business areas should apply the moratorium to any records covered by the following criteria:

    a. documents which contain or may contain content pertaining directly or indirectly to the sexual abuse of children or to child protection and care
    b. the document types include, but are not limited to, correspondence, notes, emails, and case files, regardless of the format in which they are stored (digital, paper, CDs, etc)
    c. for the purposes of this instruction, the word "children" relates to any person under the age of 18
    d. further information about the moratorium is available on IICSA's website at: www.iicsa.org.uk/news/chair-of-the-inquiry-issues-guidance-on-destruction-of-documents.

9. As part of its commitment to transparency, this schedule will be published on the MoJ's webpage: www.gov.uk/government/publications/record-retention-and-disposition-schedules.

The schedule

No.	Record type	Retention and disposition
1. Unique records held by Operational and System Assurance Group		
1.	Audit reports, supporting working papers, recommendations, Quarterly Assurance reports and intelligence reports	Where the audit has included the examination of long-term contracts, **destroy when there has been no activity for six years**. For all other audits, **keep for three years from either the date of the last document** or the closure of all recommendations and then destroy.
2.	Action plans in response to reports or inspections by external scrutiny agencies including, but not limited to, HM Inspectorates of Prisons and Probation, National Audit Office, Prisons and Probation Ombudsman	Keep for **10 years** and then review: • Where operationally relevant, keep for another 10 years and then repeat the process until the item is no longer needed. • Where no longer needed, destroy immediately.
3.	Summary analysis sheets for external scrutiny agencies	**Keep for 10 years** and then review:

No.	Record type	Retention and disposition
		• Where operationally relevant, keep for another 10 years and then repeat the process until the item is no longer needed. • Where no longer needed, destroy immediately.
4.	a) Managing the Quality of Prisoners' Life (MQPL) survey results and reports b) Custodial operational assurance audits (all reports, documents and data)	**Keep for 10 years** and then review: • Where operationally relevant, keep for another 10 years and then repeat the process until the item is no longer needed. • Where no longer needed, destroy immediately.
5.	Submissions and responses to Independent Monitoring Board	Keep for **seven years** and then destroy.
6.	OSAG programmes, plans and strategies	Store in folders by financial/calendar year which are closed annually: **Keep for one year after closure** and then review. Destroy documents which have been superseded, and **keep the remaining documents for one further year**.
7.	Audit Committee and Standards Audit Steering Group minutes and associated papers.	Store in folders by financial/calendar year which are closed annually. Keep for **three years** after closure and then destroy.
8.	Audit manuals and guides, audit products and audit outputs and audit datasets	Store in folders by financial/calendar year which are closed annually. Keep for **three years from last update** and then review. Destroy documents which have been superseded, and **keep the remaining documents for one further year.**
2. Records managed by a common retention and disposition policy		

No.	Record type	Retention and disposition
9.	Briefings and submissions Includes briefing of ministers and of HMPPS / MoJ senior officials. Records include, but are not limited to, cover sheets, summary analysis sheets and briefings produced by OSAG on individual establishments.	Keep for **three years** from last update and then destroy.
10.	HR information (held by line managers and recruiting managers)	Destroy in line with the *What to keep*[1] guidance
11.	Ministerial Cases (MCs)	Keep for **five years** from date of last correspondence and then destroy.
12.	Treat Official (TOs)	Keep for **two years** from date of last correspondence and then destroy.
13.	Freedom of Information Act and Data Protection Act responses	Folders are closed annually. • ICO investigations should be kept for **four years** from the date of the last correspondence and then destroyed. • All other responses should be kept for **three years** after the date of the last correspondence and then destroyed.
14.	Parliamentary Questions (including background research)	Folders are closed annually. **Keep for one year** after closure and then destroy.
15.	Finance and risk management	Store in folders by financial year which are closed annually. Keep for **seven years** after closure and then destroy.
16.	Business continuity plans	Updated annually. Keep previous versions for **three years** and then destroy.

[1] *What to keep* is available at: www.gov.uk/government/publications/record-retention-and-disposition-schedules

No.	Record type	Retention and disposition
17.	Records and data sets which are used by the business on a regular basis, but which are not required for permanent preservation	Keep for **10 years** and then review: • Where operationally relevant, keep for another 10 years and then repeat the process until the item is no longer needed. • Where no longer needed, destroy immediately.
18.	All other types of record not specified above, including copies of records which are owned by other business areas[2]	Keep for **three years** and then destroy.

Philip Dawkins

Departmental Records Officer
Ministry of Justice
102 Petty France
London SW1H 9AJ

Signed: 08 August 2019

Date of original issue of RRDS: N/A
Last amended: N/A

[2] If the business identifies record types which need a new retention period, they should contact the DRO's team.