



# Service Operations

## Records Retention and Disposition Schedule

### Introduction

1. This schedule applies to the records that are created and managed by staff working in the Service Operations (SOPS). It has been agreed following consultation between the SOPS and the Departmental Records Officer's (DRO) team in the Ministry of Justice (MoJ).
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 (GDPR), the Data Protection Act 2018, Freedom of Information Act 2000 (FoIA) and amending legislation. The MoJ uses Records Retention and Disposition Schedules (RRDS) to manage its compliance with statutory obligations to identify what information and records we hold, how long we keep it and what should happen to these records at the end of that time.
3. Where SOPS's work is not subject to specific legislation (including GDPR or FoIA), it is governed by the Crown's common law powers, as limited by the restraints of public law and constitutional principle.

### More about this schedule

4. None of the records listed below are selected for permanent preservation and transfer to The National Archives (TNA).
5. This schedule is split into two sections:
  - a. Records unique to the Service Operations
  - b. Records held by various teams within the MoJ and its associated bodies and where a common retention and disposition policy is applied.
6. 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 relevant records for at least **three months** after the request is resolved.<sup>1</sup>

---

<sup>1</sup> See rows 6 and 7 for maximum retention period

7. While the Independent Inquiry into Child Sexual Abuse (IICSA) continues its investigations, the moratorium on the destruction of records of potential interest 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: <https://www.iicsa.org.uk/news/chair-of-the-inquiry-issues-guidance-on-destruction-of-documents>.
8. Records that might of interest to the forthcoming public inquiry into the Covid-19 pandemic should be retained until the Inquiry has published its terms of reference. Once the Inquiry’s terms of reference are published, these records should be reviewed against the criteria to identify any that no longer need to be kept.
9. As part of its commitment to transparency, this schedule will be published on the MoJ’s webpage: <https://www.gov.uk/government/publications/record-retention-and-disposition-schedules>.

## The schedule

No.	Record type	Retention and disposition
<b>A. Unique records held by Service Operations</b>		
<b>1.</b>	Records held on Service Now: a) Service management b) Operational services: Problem management	Keep for <b>five years</b> from date of last action and then destroy.
<b>2.</b>	Records held on Service Now: a) Operational Services: Incident Management b) Operational reports	Keep for <b>three years</b> from date of last action and then destroy.

No.	Record type	Retention and disposition
3.	Records on previous Legacy system Remedy.	Keep for <b>three years</b> from date of last action and then destroy.
<b>B. Records managed by a common retention and disposition policy</b>		
4.	a) Records and information held on mobile phones (e.g. text messages, WhatsApp) b) Instant Messages (Skype, Teams, etc)	Keep for <b>three months</b> and then transfer to the corporate memory or destroy
5.	HR information (held by line managers)	Destroy in line with the <i>What to keep</i> <sup>2</sup> guidance
6.	Responses to Subject Access Requests	Keep for <b>nine months</b> and then destroy.
7.	Background information (held by business) for responses to: a) Information requests made under the Freedom of Information Act <sup>3</sup>  <b>NB.</b> See footnotes showing where the answers to these requests are held	Keep for <b>one year</b> and then review: <ul style="list-style-type: none"> <li>Where operationally relevant, keep for <b>another year</b> and then repeat the process until the item is no longer needed.</li> </ul> Where no longer needed, destroy immediately.
8.	Data loss incident records (held by business)	Keep for <b>three years</b> from incident closure and then destroy
9.	Business continuity plans (held by business)	Updated annually. Keep previous versions for <b>three years</b> and then destroy.
10.	Contracts (value up to £10,000): including, but not limited to: signed contracts, records of performance, meetings, complaints, changes to requirements, variations and extensions (up to £10,000)	Keep for <b>six years</b> after contract ends and then destroy. <sup>4</sup>
11.	Finance and risk management information	Keep for <b>seven years</b> and then destroy.

<sup>2</sup> *What to keep* is available at: <https://www.gov.uk/government/publications/record-retention-and-disposition-schedules>

<sup>3</sup> The answers to these requests are held by Disclosure (see row 40 of the MoJ HQ schedule)

<sup>4</sup> Limitation Act 1980 s.5 sets the time limit for actions founded on simple contracts (signed under hand) at six years

No.	Record type	Retention and disposition
12.	Submissions, briefings for ministers, other correspondence with Private Office, Chief Executives' Offices, etc <b>including Ministerial responses to submissions and other documents</b>	Keep for <b>seven years</b> and then destroy.
13.	All other types of record not specified above, including copies of records which are owned by other business areas <sup>5</sup>	Keep for up to <b>three years</b> and then destroy.

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

**Signed:** 14 March 2022

Original Issue of RRDS: Operational Services Division, May 2008  
 This RRDS supersedes: Service Planning Division RRDS, July 2015

---

<sup>5</sup> If the business identifies record types which need a new retention period, they should contact the DRO's team.