Governance and Assurance

(HM Courts & Tribunals Service)

Records Retention and Disposition Schedule

## Introduction

1. This schedule applies to the records that are created and managed by staff employed in HM Courts and Tribunals Headquarters (HMCTS). It has been agreed following consultation between HMCTS and the Departmental Records Officer’s (DRO) team 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 (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 HMCTS’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

1. None of the records listed below are selected for permanent preservation and transfer to The National Archives (TNA).
2. This schedule covers both the records held by the Governance and Assurance Division in HMCTS and the records held in courts, tribunals, at regional level and HQ Directorates.
3. This schedule is split into two sections:
   1. Unique governance and assurance records held by HMCTS
   2. Records managed by a common retention and disposition policy

1. 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.[[1]](#footnote-1)
2. 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:
   1. documents which contain or may contain content pertaining directly or indirectly to the sexual abuse of children or to child protection and care
   2. 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)
   3. for the purposes of this instruction, the word “children” relates to any person under the age of 18
   4. 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>.
3. 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 |
| --- | --- | --- |
| A. Unique governance and assurance records held by HMCTS | | |
|  | HMCTS Ops reporting tool:  a) Key Control Check Sheets (KCCS) and all previous equivalents  b) Logging Sheets / Check and Test Documents  c) Evidence records for Standard Operating Controls (SOC) – self-assessment report | a-b) Keep for **seven years** and then destroy  c) Keep for **one year**:   * Where all issues are resolved, destroy * Where there are ongoing issues, keep for another year and review. Repeat until all issues are resolved but for **no longer** then seven years. |
|  | a) SOC self-assessment reporting tool  b) SOC database content  c) Risk and Assurance Management Tool (RAMT) | Keep for **seven years** and then destroy |
|  | Audit reports and recommendations | Keep for **three years** after closure of final recommendations and then destroy |
|  | **Risk Registers and governance statements**  a) Corporate  b) Regional  c) Directorate  d) Regions and central directorates (quarterly statements) | a) Keep for **seven years** and then review:   * Where operationally relevant, keep for a further seven years and then review again. Repeat until no longer required. * Where no longer required, destroy immediately.   **NB**. Copies of these records held in HQ should also be destroyed after **three years** |
|  | a) Health checks in courts and business units including:   * reports and related papers * correspondence * management information * evidence of recommendations met   b) Deep dives in HQ Divisions and Operations | Records are held by Assurance Business Partners and Assurance Business  Officers  Keep for **three years** from date that all issues and/or recommendations are completely resolvedand then destroy.  **NB**. Copies of these records held in HQ or other teams should also be destroyed after **three years** |
|  |  |  |
|  | a) Anti money laundering logs | Keep for **two years**:   * Where investigation has led to prosecution, keep for **seven years** from date case ended and then destroy * Otherwise destroy |
|  | a) Serious National Crime Agency (NCA) referrals  b) other related correspondence | Keep for **three years**:   * Where investigation has led to prosecution, keep for **seven years** from date case ended and then destroy * Otherwise destroy |
|  | a) Case and Asset Tracking System (CATS) database content | For criminal cases, keep for **seven years** from date case ended and then destroy (or for length of sentence plus one year) whichever is the longer  For suspicious activity reports; keep for **six months**  For all other cases, keep for **three years** from date case ended and then destroy |
|  | Integrated Fraud System (IFS) database content | Keep for **seven years** from case endand then destroy |
|  | HMCTS Counter-Fraud and Investigations team:  a) Investigation reports and case documents or reports  b) Other corporate reports | Keep for **five years** from report date and then destroy |
|  | Corporate publications:  a) HMCTS contributions to MoJ Single Departmental Plan  b) HMCTS Annual Reports and Accounts - Governance Statement and supporting documentation  c) HMCTS Annual Trust Statement - Governance Statement and supporting documentation  d) Annual report, business plans and all other corporate publications | a) Keep for **three years** and then review:   * Where operationally relevant, keep for a further three years and then review. Repeat until no longer required. * Where no longer required, destroy immediately.   b-d) Keep for **six years** from date of report and then destroy |
|  | HMCTS-specific policies including, but not limited to:  a) Risk management  b) Fraud guidance  c) Information assurance | Keep for **three years** from date superseded and then destroy |
|  | Minutes from formally constituted groups including, but not limited to:   * SOC Steering Group * Senior Management Team | Keep for **three years** and then destroy  (Agendas, room bookings, etc keep for no more than **one year** and then destroy) |
|  | Internal Audit reports and supporting papers | Where the audit has examined long-term contracts, keep for **six years** from report date and then destroy.  All other reports should be kept for **three years** and then destroyed. |
|  | HMCTS management information | Keep for **10 years** and then review:   * Where operationally relevant, keep for another 10 years and repeat the process until the data is no longer needed. * Where no longer needed, destroy. |
|  | Reports to the ARAC (Audit, Risk Assurance Committee) and committees | Keep for **seven years** and then destroy |
| B. Records managed by a common retention and disposition policy | | |
|  | HR information (held by line managers) | Destroy in line with the *What to keep*[[2]](#footnote-2)guidance |
|  | Customer bank details | Keep for **no longer 14 days** and then destroy |
|  | a) Records and information held in open internet tools (e.g. YouTube videos, podcasts)[[3]](#footnote-3)  b) Records and information held on mobile phones (e.g. text messages, WhatsApp)  c) Instant Messages (Skype, Teams, etc) | Keep for **three months** and then transfer to the corporate memory or destroy |
|  | Responses to Subject Access Requests | Keep for **nine months** and then destroy. |
|  | Background information (held by business) for responses information requests made under:   * Freedom of Information Act[[4]](#footnote-4) * Environmental Information Regulations   **NB.** See footnotes showing where the answers to these requests are held | Keep for **one year** and then review:   * Where operationally relevant, keep for **another** **year** and then repeat the process until the item is no longer needed.   Where no longer needed, destroy immediately. |
|  | Data loss incident records (held by business) | Keep for **three years** from incident closure and then destroy |
|  | Business continuity plans (held by business) | Updated annually. Keep previous versions for **three years** and then destroy. |
|  | 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 **six years** after contract ends and then destroy.[[5]](#footnote-5) |
|  | Litigation cases | Keep for **six years** from last action and then destroy |
|  | Finance and risk management information | Keep for **seven years** and then destroy. |
|  | All other types of record not specified above, including copies of records which are owned by other business areas[[6]](#footnote-6) | Keep for **three years** and then destroy. |

Phillip Crowcroft

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

**Signed: 27 July 2020**

1. See rows 19 and 20 for maximum retention period [↑](#footnote-ref-1)
2. *What to keep* is available at: <https://www.gov.uk/government/publications/record-retention-and-disposition-schedules> [↑](#footnote-ref-2)
3. Staff should check the intranet for more detailed guidance: *Guidance for using Open Internet Tools* [↑](#footnote-ref-3)
4. The answers to these requests are held by Disclosure (see row 40 of the MoJ HQ schedule) [↑](#footnote-ref-4)
5. Limitation Act 1980 s.5 sets the time limit for actions founded on simple contracts (signed under hand) at six years [↑](#footnote-ref-5)
6. If the business identifies record types which need a new retention period, they should contact the DRO’s team. [↑](#footnote-ref-6)