Office of the Public Guardian

Records Retention and Disposition Schedule

## Introduction

1. This schedule applies to the records that are created and managed by staff employed in the Office of the Public Guardian (OPG). It has been agreed following consultation between the OPG 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. The Office of the Public Guardian’s work is governed by the Mental Capacity Act 2005 and amending legislation.

## More about this schedule

1. The records listed below are not selected for permanent preservation.
2. This schedule is split into two sections:
   1. Records unique to the Office of the Public Guardian
   2. Records held by various teams within the MoJ and its associated bodies and where a common retention and disposition policy is applied.
3. 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).
4. 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>.
5. 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 |
| --- | --- | --- |
| 1. Unique records held by the Office of the Public Guardian | | |
|  | **Lasting Powers of Attorney (LPA)**  **and**  **Enduring Powers of Attorney (EPA)**  Including, but not limited to:   * Case records management systems * Powers of Attorney (PoA) * Scanned copies of letters from third parties * Correspondence (including Local Authority) * Reports collection * OPG 100 search requests * Registration documents (LPA and EPA applications) * Payment receipt spreadsheets * Complaints – case related * Wills * Presumption of death orders | Unless covered by one of the exceptions below, **keep for seven years** from date of case closure and then destroy.  Exceptions:  a) The **Public Guardian Registers[[2]](#footnote-2)** for LPA and EPA (including instruments):  **Keep for 100 years** from vulnerable person’s date of birth and then destroy (unlessthe person is still living, in which case keep for seven years from case closure and then destroy)  b) Incomplete applications (all rejected and withdrawn cases):  **Keep for three months** and then destroy  c) Pending, imperfect, pre-application objection and passed validation cases:  **Keep for three months** from date of last action and then destroy |
|  | **Supervised Clients**  Including, but not limited to:   * Panel referral records * Panel deputy appointment records * Professional deputy information * Assurance visits records * Correspondence (including with local authorities) * Supervision case files * Administration records and reports * Reports on closed cases * Bonds * Orders (including presumption of death orders) | Unless covered by the exceptions below, **keep for seven years** from date of last entry and then destroy (including after case closed[[3]](#footnote-3)).  Exceptions  a) The **Public Guardian Registers** for Supervised Clients:  **Keep for 100 years** from vulnerable person’s date of birth and then destroy  (unlessthey are still living, in which case keep for seven years from case closed and then destroy)  b) Incomplete applications (all rejected and withdrawn cases):  **Keep for one year** from date of last action and then destroy |
|  | **Safeguarding**  Including, but not limited to:   * Responses (further information requests, * Whistle-blower signposting * Case acceptance documents * Cases accepted for investigation * Safeguarding vulnerable people (SVA) documents | Where there is OPG jurisdiction:  a) Documented referral concerns should be attached to main case record and kept for the same period.  b) Initial case information, including:   * Unaccepted case records * SAAR referrals * Social Services * Police liaison records   **Keep for seven years** after case closed[[4]](#footnote-4) and then destroy  Where there is no OPG jurisdiction, **keep for one year** from date of last action and then destroy (including non-supervised sub orders such as presumption of death) |
|  | **Court application related documents**  Including, but not limited to:   * Recovery and resolution * Court of Protection communications * Case databases * Record of legal issues relating to bonds and panel deputies | Unless covered by the exception below, **keep for seven years** from date case was closed[[5]](#footnote-5) and then destroy  Exception:  Record of Counsel opinions, personal injury matters and committee papers:  **Keep for five years** from date of last correspondence and then review:   * If still operationally relevant, keep for a further **three years** after correspondence ended and then destroy * If no longer required, destroyed immediately |
|  |  |  |
|  | **Visits** (including Visitors’ commissioning documents, visit reports and any associated documents) | Unless covered by the exceptions below, keep for **seven years** after date case closed[[6]](#footnote-6) and then destroy  Exceptions:   * Visitors’ employment and payment information (non-permanent staff), * Visitor administration records   Keep for **three years** from date of last action and then review:   * If still operationally relevant, keep for a further **three years** and then destroy * If no longer required, destroyed immediately |
|  | **Investigations** (including complaints about a specific investigation) | Keep for **seven years** after date case closed[[7]](#footnote-7) and then destroy |
|  | **Missing Person information** (including any supervised sub orders such as presumption of death) | Keep for **seven years[[8]](#footnote-8)** |
| 2. Records managed by a common retention and disposition policy | | |
|  | HR information (held by line managers) | Destroy in line with the *What to keep* [[9]](#footnote-9)guidance |
|  | Audio recordings of telephone calls | Keep for **three months and one day** after the telephone call and then destroy |
|  | a) Records and information held in open internet tools (e.g. YouTube videos, podcasts)[[10]](#footnote-10)  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 to:   1. Parliamentary Questions (PQs) 2. Correspondence (including Ministerial Correspondence (MCs)) 3. Information requests made under:  * Freedom of Information Act * Environmental Information Regulations * Reuse of Public Sector Information Regulations   **NB.** The answers to these requests are held by:  a) Ministers, Parliament, Strategy and Implementation (see row 37 of MoJ HQ schedule)  b) Ministerial Correspondence Unit (see row 4 of the Private Office schedule)  c) Disclosure (see row 40 of MoJ HQ schedule) | 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 | 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.[[11]](#footnote-11) |
|  | Litigation cases | Keep for **six years** from last action and then destroy. |
|  | Finance and risk management information | Store in folders by financial year which are closed annually.  Keep for **seven years** after closure and then destroy. |
|  | Submissions, briefings for ministers and policy team, other correspondence with Private Office, Chief Executives’ Offices, etc **including Ministerial responses to submissions and other documents** | Keep for **seven years** and then destroy. |
|  | Functional leadership (all aspects) | 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[[12]](#footnote-12) | Keep for **three years** and then destroy. |

Phillip Crowcroft

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

**Signed: 12 December 2019**

Date of Original Issue of RRDS: (with the Court of Protection) September 2009

Previously amended: November 2016

1. See rows 11 and 12 for maximum retention period [↑](#footnote-ref-1)
2. To request a search of the Registers, please see the guidance available at: <https://www.gov.uk/government/publications/requesting-a-search-of-the-public-guardian-registers-public-guardian-practice-note> [↑](#footnote-ref-2)
3. Case is closed on death of client, date of cancellation, withdrawal or revocation of court order [↑](#footnote-ref-3)
4. Case is closed on death of client, date of cancellation, withdrawal or revocation of PoA [↑](#footnote-ref-4)
5. Case is closed on death of client, date of cancellation, withdrawal or revocation of PoA [↑](#footnote-ref-5)
6. Case is closed on death of client, date of cancellation, withdrawal or revocation of PoA [↑](#footnote-ref-6)
7. Case is closed on death of client, date of cancellation, withdrawal or revocation of PoA [↑](#footnote-ref-7)
8. To be further reviewed in the next iteration of this schedule once OPG has fully developed this service [↑](#footnote-ref-8)
9. *What to keep* is available at: <https://www.gov.uk/government/publications/record-retention-and-disposition-schedules> [↑](#footnote-ref-9)
10. Staff should check the intranet for more detailed guidance: *Guidance for using Open Internet Tools* [↑](#footnote-ref-10)
11. Limitation Act 1980 s.5 sets the time limit for actions founded on simple contracts (signed under hand) at six years [↑](#footnote-ref-11)
12. If the business identifies record types which need a new retention period, they should contact the DRO’s team. [↑](#footnote-ref-12)