

CPS Retention and Disposal Schedule Policy

1. Description

1.1 The Retention and Disposal Schedule (R&DS) covers all information and records, irrespective of medium, and should be applied to all digital and paper copy information as well as databases and social media. The R&DS provides a management tool for identifying and determining the retention and disposal of information and records created by the Crown Prosecution Service (CPS) and contains the major categories of information and records it creates. It provides guidance to enable compliance with legal obligations.

1.2 For sensitive information, including that covered by the General Data Protection Regulation (UK GDPR) (EU) 2016/679 [UK GDPR overview](#), the Data Protection Act (DPA) 2018 [DPA 2018](#) and Law Enforcement Directive (LED) 2016 [LED 2016](#), we must be able to allow access to those who need to see this information while preventing others from gaining access. We also need to be able to identify personal and/or sensitive personal information, know who it is shared with, and dispose of information we are no longer entitled to hold.

1.3 This R&DS has been created to form part of the CPS Information Management and Governance, as required under section 46 code of practice of the Freedom of

Information (FOI) Code 2000 s46 FOI Code Records Management.

2. Introduction

2.1 Disposal scheduling is an important aspect of establishing and maintaining control of corporate information. It increases efficiency and cost-effectiveness by ensuring that information is disposed of when no longer needed. This enables more effective use of resources, for example physical and digital storage space, and saves staff time searching for information that may not be there. Efficiently disposing of information once it has reached a set retention date also ensures compliance with legislation such as the Public Records Act (PRA) 1958 & 1967 [PRA 1958](#), the UK GDPR, the DPA and the LED.

3. Purpose of the Retention and Disposal Schedule

3.1 The aim of this R&DS is to provide a consistent approach to the way the CPS handles its information, and to provide a clear set of guidelines to all staff and support the Information Management and Governance Policy. The R&DS will help the organisation to:

- Identify information which has historical significance, and which will be transferred to The National Archives (TNA)
- Retain personal data no longer than is necessary for the purpose you obtained it for

- Ensure personal data is disposed of when no longer needed, reducing the risk that it will become inaccurate, out of date or irrelevant
- Prevent premature destruction of information which needs to be retained for a specific period to satisfy legal, financial and other requirements
- Authorise the destruction of information once no longer required by the business.

4. Scope of the Retention and Disposal Schedule

4.1 The R&DS covers all the functional information and records of the CPS. This is a corporate document. As well as providing a guide for staff, it will be used externally as a reference tool by members of the public when they wish to search for information under legislation such as the Freedom of Information and Data Protection Acts.

4.2 The R&DS details the types of information and the length of time it should be retained before taking disposal or archive action. Many retention periods are determined by statute – such as information needed for income tax and audit purposes, or information on aspects of employment/health and safety. If we keep personal data to comply with a requirement like this, it will not be considered to have been kept “for longer than necessary”. Where available or appropriate the relevant legislation or statutory reason for keeping the information for a specific period has been included.

4.3 You can read about legislation that relates to, or affects archives, records management or public sector information on [The National Archives website](#).

5. Records and Information Management Policy

5.1 A record can be defined as information created, received and maintained as evidence and information by an organisation, in pursuance of legal obligations or in the transaction of business.

5.2 You can find more information about what comprises a record in TNA introductory guide [What is records management?](#)

5.3 Information created by staff on behalf of the CPS belongs to the department and must be reviewed and disposed of routinely and in accordance with line of business retention and disposal schedules.

5.4 Through effective information management, the Department will comply with the following obligations:

- the DPA
- the UK GDPR
- the PRA
- the Government's [Information Principles](#) (management of information from creation to destruction).
- the [Civil Service code](#) (states you must keep accurate official records and handle information as openly as possible within the legal framework).

5.5 All systems and records must have designated owners throughout their lifecycle, whether that is named individuals or nominated business areas. Records and information must

be stored and handled in accordance with the requirements of the [Government Security Classification System](#).

5.6 [Digital continuity](#) must be considered for the systems and formats that are used to store digital records. All records must be supported by metadata that documents their authority, status, structure and integrity to demonstrate their administrative context and relationship with other records.

5.7 All records must be traceable and retrievable. File movements and movements of data must be tracked, including for files migrated into or out of the department through [machinery of government changes](#).

5.8 Records must be stored in environmental conditions that protect them from deterioration. For more information refer to The National Archives guidance:

- [Requirements for an offsite store](#)
- [Implementation guides](#)

6. Retention requirements for personal data

6.1 The UK GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people. This also applies to work email addresses when they include a person's full name.

6.2 The UK GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data. Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the UK GDPR depending on how difficult it is to attribute the pseudonym to an individual.

6.3 UK GDPR Article 5(1)(e) about storage limitation specifies that personal data shall be kept 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 it 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) of UK GDPR

6.4 CPS' lawful basis for processing personal data is set out in our [Privacy Notice](#)

6.5 Personal data must be periodically reviewed in accordance with the CPS retention schedules and if it is no longer needed it should be deleted or anonymised as appropriate. Anonymised data is not subject to UK GDPR or the Data Protection Act 2018.

6.6 Any challenges to the retention of personal data must be considered in accordance with [UK GDPR Article 17 \(Right to erasure\)](#), or the equivalent sections in the [DPA 2018](#) if the processing is for law enforcement purposes. The right to erasure does not apply where we are legally obliged to

process personal data or where the processing is necessary for performing our functions.

6.7 Where the CPS would be required to erase personal data, but the personal data must be maintained as evidence for legal purposes or for reasons of important public interest, CPS must (instead of erasing the personal data) restrict its processing.

7. Sensitive personal data

7.1 The UK GDPR refers to sensitive personal data as “special categories of personal data”. The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

For example, information about an individual’s:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation

8. Revision of the Retention and Disposal Schedule

8.1 The Security Information and Assurance Division (SIAD) will undertake a full review of the R&DS no less than every

five years. The revised R&DS will be submitted to the Policy Review Board (PRB) for approval prior to its implementation. Minor changes / updates will be incorporated into the R&DS as and when required.

8.2 If anything is not covered by this R&DS, the Records Management Team (RMT) must be contacted to discuss amendment of the R&DS. Do not destroy this type of information. Unauthorised destruction of information goes against s46 FOIA 2000 & 2009.

9. Roles and Responsibilities

9.1 The [Departmental Records Officer \(DRO\)](#) is a mandatory role who reports to the Head of SIAD /Data Protection Officer (DPO). The DRO is accountable for maintaining effective and efficient record keeping procedures in the CPS.

9.2 The CPS is responsible for transferring records selected for permanent preservation to TNA and other places of deposit. Areas/Directorates are accountable for the management and disposal of all other records that they create. Our Procurement and Commercial Services supports the business by managing CPS' outsourced paper records centers. Corporate Communications are responsible for CPS' internet and intranet governance.

Day-to-day responsibilities for information and records management will be delegated by Chief Crown Prosecutors/Heads of Directorates appointed as Information Asset Owners (IAO) to information specialists within each Area/Directorate.

9.3 Public requests for CPS information must be actioned by Areas/Directorates in accordance with relevant legislation.

9.4 In accordance with this policy, all staff are responsible for managing, storing appropriately and disposing of the information they create and receive as part of their normal daily business activities.

9.5 All CPS staff as well as contractors, must take responsibility for ensuring that information and records are created with appropriate retention periods, and these are adhered to.

9.6 Staff must also be aware of the need to dispose of information on a routine basis, in line with the R&DS. Records that fall under the Long-Term Interest (LTI) criteria must be sent to the RMT as soon as they have been concluded.

10. Definitions of Disposal Action Terms Used

A - Archive or Permanent Retention - This information has historical value. Public records and information may be offered to TNA (or Place of Deposit) for permanent preservation and be made available to the public. Non-public records and information may need to be permanently retained by the CPS for administrative purposes

D - Destroy - This information is of a routine business nature and can be destroyed when the business need for retaining the information has expired.

R - Review - This information may have long term business value, or could potentially be of historical interest. A more thorough review therefore will be undertaken to determine its ongoing value before a destruction decision is made.

11. Lines of Business and Appraisal reports

11.1 Areas/Directorates will identify, appraise and offer records identified as having historic value through the RMT, and if applicable transfer to TNA at 20 years + 1 or earlier. Historic records can be transferred earlier by agreement of all parties affected by the decision. Records with historic value, retained beyond the 20 year +1 will be with Secretary of State for Digital, Culture, Media and Sport (previously Lord Chancellor) via the Advisory Council for authorisation.

11.2 Areas/Directorates must develop and maintain their own Appraisal Reports to identify groups or series of key departmental records which are required for ongoing administrative, legal or fiscal purposes. The report will act as the basis for appraising records that have short, medium- and long-term value and for developing detailed line of business retention and disposal schedules already in place. It will enable Areas/Directorates to identify records to be transferred to TNA for permanent preservation. TNA has developed an appraisal template and guidance on completing the appraisal report template for these purposes which is presently under review (2020).

11.3 The CPS has in place an LTI criteria that gives guidance on the types of cases and policy development areas that should be sent to the RMT.

11.4 Staff should refer to the CPS key events list to help identify appropriate records for permanent preservation. TNA [Records Collection Policy](#) sets out an overview of the types of records which are and are not collected from public bodies.

12. Audit and compliance

12.1 CPS Areas/Directorates are accountable for developing their own assurance compliance to ensure that the core principles in this policy and related activities are being complied with.

12.2 CPS Areas/Directorates must audit and monitor the secure disposal of their own records as well as those of any third parties that share or produce records on their behalf. And are responsible for maintaining an audit trail of their review, destruction and disposal decisions.

12.3 It should be noted that as a result of the Independent Inquiry into Child Sexual Abuse (IICSA) (aka Goddard), which was established by the Home Secretary on 12 March 2015, a moratorium on the disposal of all information throughout the CPS was put in place. The automatic destruction of case files on CMS was disabled on 12 May 2015 and the disposal of archived boxes held in off-site storage at Iron Mountain since March 2015. This is currently in force and will remain so until further notice.

12.4 In addition, there are two other national Inquiries that the Department is involved - these are the Undercover Policing Inquiry (UCPI) (aka Pitchford) (May 2014) and Infected Blood Inquiry (IBI) (July 2017).

13. Previous versions of the Retention and Disposal Schedule

13.1 This R&DS replaces other versions last published in 2008.

Issue	Date	Review	Author/Reviewer/Authorised
1.0	June 20	Submitted to PRB	DRO/NK
2.0	July 20	Approved by PRB	PRB
	July 23	Next review date or sooner if required	