



Records Management Policy

April 2025

Version	Date	Author	Reason for Change
1.0	20/04/25	Hassim Ganiyu	N/A

1. Introduction

1.1. This Records Management Policy sets out the principles and framework for managing records throughout their lifecycle within the Dyfed-Powys Office of the Police and Crime Commissioner (OPCC).

1.2. It ensures compliance with relevant legislation, supports operational efficiency, accountability, and transparency, and protects the legal and financial interests of the organisation.

1.3. The policy has been developed with reference to the Code of Practice on Records Management issued by the Lord Chancellor under section 46 of the Freedom of Information Act 2000 (FOIA).

2. Aim

2.1 Records management is the structured approach by which Dyfed-Powys OPCC manages all records and information from creation to final disposal, commonly referred to as the Records Lifecycle. The aim of this policy is to ensure that:

- **Accountability** – Records provide a reliable and transparent account of the decisions and activities undertaken by the OPCC.
- **Accessibility and Security** – Records are readily accessible to those with legitimate authority while ensuring appropriate protections are in place. Information must remain consistent with its original context, and the most current version is clearly identifiable where multiple versions exist.
- **Quality** – Records are complete, accurate, and trustworthy, supporting confidence in the information held.
- **Maintenance** – The integrity and usability of records is preserved over time, even where updates or changes occur.
- **Retention and Disposal** – Records are retained for appropriate durations in line with legislation and business need. Records of long-term historical value are identified and preserved, with consideration given to transfer to an approved archive, such as the Dyfed Archives.
- **Staff Awareness** – All staff understand and uphold their responsibilities regarding the creation, use, and management of records in accordance with this policy.

3. Scope

3.1 This policy applies to:

- All records created, received, and maintained by OPCC employees and contractors.
- Records in all formats: paper, digital, email, photographs, audio/video, etc.
- Both corporate and personal information processed on behalf of the OPCC.

4. Other organisational policies (both specific to OPCC and adopted policies from Dyfed Powys police) that relate to Records Management.

- 4.1 Record Retention and Disposal Policy and Schedule
- 4.2 Freedom of Information Policy
- 4.3 Freedom of Information Publication Scheme
- 4.4 Data Protection Policy (Dyfed Powys Police)
- 4.5 Government Security Classification Policy (Dyfed Powys Police)

5. Records Lifecycle.

- 5.1 **Creation/Receipt:** Ensure appropriate naming, metadata, and secure capture.
- 5.2 **Use:** Accessed and referenced during business processes.
- 5.3 **Storage:** Stored securely in suitable systems, whether digital or physical.
- 5.4 **Retention:** Held in accordance with the Retention Schedule.
- 5.5 **Disposal/Archiving:** Securely destroyed or permanently archived depending on value.

6. Definitions

- 6.1 Record: Any document or data which evidences activities, decisions, or transactions, regardless of format.
- 6.2 Records Management: The systematic control of records throughout their lifecycle from creation to disposal.
- 6.3 Retention Schedule: A list that defines how long each record type should be retained and the method of disposal.

7. Responsibility for Records Management.

- 7.1 The Chief Executive of the Dyfed-Powys Office of the Police and Crime Commissioner (OPCC) is responsible for endorsing this policy, supporting its implementation, and ensuring appropriate resources are allocated to deliver effective records management.
- 7.2 The Head of Assurance is designated as the lead for records management and is accountable for ensuring the OPCC complies with all relevant legislation and regulatory requirements. Designated staff will support this function, and they will be provided with appropriate training to carry out their responsibilities effectively. All OPCC staff who create, receive, or use records share a responsibility for managing them in accordance with this policy.
- 7.3 The OPCC maintains structured file lists for managing both digital and physical records. Electronic records stored on the shared drive are periodically reviewed and updated by the Administration Team. Although the majority of records are now held electronically, any hard copy records are tracked using a spreadsheet that records their title and storage location. This list is reviewed and maintained by Business Support Officer.

7.4 Each functional area, as listed in the Records Retention and Disposal Schedule and the Information Asset Register, is assigned a designated 'Information Owner'. This individual is responsible for ensuring that records within their area are managed appropriately on a day-to-day basis in line with this Records Management Policy and the OPCC's Records Retention and Disposal Policy and Schedule.

8. Storage and Security.

8.1 Records must be stored securely, protecting confidentiality, integrity, and accessibility.

8.2 Physical records must be in locked cabinets or secured rooms.

8.3 Electronic records must be stored in access-controlled systems.

8.4 Backups and business continuity plans must be in place for critical data.

9. Accessibility.

9.1 The Head of Assurance, in consultation with the Chief Executive, will determine which records require access restrictions and will identify who is authorised to access them. Access to confidential records—including personnel files and sensitive documents—will be limited to the Chief Executive, and other named individuals whose roles necessitate access.

10. Disposal and Destruction

10.1 Records must be reviewed at the end of their retention period.

10.2 Disposal must follow the processes outlined in the Retention and Disposal Policy.

10.3 Disposal must be documented in a Destruction Log.

10.4 Sensitive materials must be securely destroyed (e.g., shredding, digital wiping).

11. Naming Electronic Records.

11.1 Naming conventions play a critical role in effective records management. To support consistency and improve information retrieval, Dyfed-Powys OPCC requires a standardised approach to naming electronic records across the organisation.

11.2 When creating a file or document name, it is important to clearly reflect its content. The elements used to construct a file name will depend on the nature of the document, but the subject should always be distinct enough to differentiate it from other records. Common components to consider when naming files include:

- **Date**
- **Subject or Title**
- **Version Number** (where applicable)

11.3 Staff must avoid naming files or folders using their own names unless the content is biographical in nature (e.g., relating to personnel matters about that individual). The goal is to ensure clarity, relevance, and ease of access across the team.

12. Email Management.

12.1 The OPCC email system is designed for communication, not long-term storage. Any email that constitutes a formal record of business activity must be saved to an appropriate folder on the shared network drive in a timely and structured manner.

12.2 Staff must not save all emails indiscriminately to the shared drive. Doing so can create excessive storage demands and hinder efficient information retrieval, increasing the risk of non-compliance with the Freedom of Information Act (FOIA) and Data Protection legislation.

12.3 In line with current policy, any emails not saved to the shared drive will be automatically deleted after 12 months. Staff are responsible for ensuring that key records are preserved appropriately before this timeframe lapses.

12.4 Attachments or documents within an email that require retention must be saved as separate records on the shared drive, rather than being retained solely within the email. This ensures wider accessibility for authorised staff.

12.5 Unless an email is sent via a secure platform, its content—including any attachments—should be regarded as potentially accessible to the public. Sensitive or confidential information must not be transmitted or stored on personal devices or unsecured platforms.

12.6 Material classified as 'Official-Sensitive' or higher must not be sent to personal or unsecured email addresses. Exceptions are only permitted with the express approval of the Chief Executive (e.g., Joint Audit Committee agendas).

12.7 Staff must not use personal email accounts for conducting OPCC business unless there is a valid reason to do so. In such cases, all relevant communications and records must be saved promptly to the shared drive. Under no circumstances should personal accounts be used to store work-related information.

12.8 Other forms of digital communication—such as Microsoft Teams or Skype messages—are also considered records when used for business purposes. These must be saved to the shared drive if they constitute a business record. Otherwise, they should be deleted by the user in accordance with this policy.

13. Inactive Records.

13.1 Responsibility for managing inactive records—whether digital or in hard copy—lies with the designated folder owner, as specified in the Records Retention and Disposal Schedule and the Information Asset Register.

13.2 Any physical records stored in personal workspaces, such as desks, drawers, or lockers, remain the responsibility of the individual who created or holds them.

13.3 Inactive records must be regularly reviewed by their owners. A decision should be made as to whether they are to be disposed of securely or retained. If retention is necessary, consideration should be given to whether they are suitable for archiving.

13.4 The Head of Assurance should be notified of any records—electronic or hard copy—identified as suitable for archiving. Following a review, and subject to the Chief Executive’s approval, appropriate records may be archived internally (e.g., via SharePoint).

13.5 Records identified as having historical significance may be transferred to Dyfed Archives, in accordance with the OPCC’s Retention and Disposal Schedule and Archiving Procedure. A comprehensive review of all records will also take place upon the appointment of a new Police and Crime Commissioner (PCC).

14. Website Management.

14.1 The Head of Communications and Engagement, with input from other OPCC staff as required, is responsible for overseeing the OPCC’s website. This includes regular reviews to ensure information remains accurate, relevant, and compliant with statutory publication and transparency obligations.

15. Partnership Working and Commissioned Services

15.1 When records arise from partnership working, a clear agreement must be in place identifying whether the OPCC or a partner organisation is responsible for the creation, management, retention, and disposal of those records.

15.2 If Dyfed-Powys OPCC is the lead partner, its records management policies and procedures must apply unless an alternative arrangement is formally agreed.

15.3 Where another organisation assumes the lead partner role, their records management procedures will apply. However, Dyfed-Powys OPCC should retain and manage any records that relate to its specific role in the partnership, in accordance with its own Records Management Policy.

15.4 In cases where no lead partner has been designated, Dyfed-Powys OPCC will ensure that a nominated partner organisation takes responsibility for records management duties within the partnership agreement.

16. Government Security Classification System

16.1 Dyfed-Powys OPCC adopts the **Government Security Classification System (GSCS)**, which is also used by Dyfed-Powys Police. All documents should be classified under one of the following categories:

- **Official**

- **Official – Sensitive**
- **Secret**
- **Top Secret**

This system ensures appropriate protection and handling of information based on its sensitivity and associated risks.

16.2 It is the responsibility of the originator of a document or record to apply the correct classification and to restrict initial circulation to individuals with a legitimate 'need to know'.

16.3 All records marked as sensitive must be disposed of using appropriate, approved methods.

- **Official and Official – Sensitive** documents must be disposed of via locked confidential waste bins clearly labelled for sensitive waste.
- **Secret** material must be shredded using a cross-cut shredder or destroyed via a secure, approved method.

Staff should refer to Dyfed-Powys OPCC's Disposal and Information Security procedures for further guidance.

17. Training and Awareness

17.1 All staff will receive training on records management responsibilities.

17.2 Refresher training will be provided periodically or when policies are updated.

18. Compliance and Review

18.1 Dyfed-Powys OPCC is committed to regularly auditing its records management arrangements to ensure continued compliance with relevant legislation, policy, and best practice.

18.2 Periodic spot checks will be conducted by the Head of Assurance, supported by the Governance Officer, to monitor staff compliance with records management procedures. Findings from these checks will be reported to the Chief Executive.

18.3 This Records Management Policy will be reviewed by the Head of Assurance at appropriate intervals, and no less frequently than once every four years, or sooner if prompted by legislative or operational change.

