Ombwdsmon
Ombudsman
Cymru · Wales

Records Management Policy

Mae'r ddogfen hon hefyd ar gael yn y Gymraeg.

This document is also available in Welsh.

Contents

_Toc89878884

1 Purpose

1.1 The Public Services Ombudsman for Wales (PSOW) understands the importance of effective records management in demonstrating actions and decision-making. The PSOW also recognises the need to manage records in accordance with legal and regulatory requirements and best practice.

1.2 The PSOW is committed to adopting the principles set out in its publication Good Records Management Matters, which includes a commitment to ensure effective systems to enable effective records management.

1.3 The Records Management Policy sits within the PSOW's information governance framework and outlines the organisation's approach to records management. This policy sets out the scope, benefits and outcomes, records management standards, roles and responsibilities, and obligations placed on PSOW in respect of its records.

1.4 The retention of different record types is defined within the Record Retention Schedule which accompanies this policy. Record types are grouped according to business function. These record types or information assets are recorded within the Information Asset Register and regularly reviewed. This approach ensures that the PSOW understands what information it holds, and the risks associated with each record type or information asset in order to protect it and to be able to exploit its potential"[1].

[1] Information Asset Register factsheet, The National Archives, February 2017.

2 Scope

2.1 A record is defined as:

"information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations of in the transaction of business".[2]

This policy applies to all records. It includes "not only paper files series and digital records management systems but also business and information systems (for example case management, finance, and geographical information systems) and the contents of websites".[1]

2.2 For the purpose of this policy, records can be about anything that is created, received or maintained in connection with any aspect of PSOW business. They can therefore hold personal or non-personal data and be held in a range of media including, paper, electronic, visual, audio or any other format.

2.3 This policy applies to the lifecycle of a record, from creation or receipt, through storage and use, to disposal or permanent preservation as archival records.

2.4 Good records management includes:

- The creation of appropriate records.
- The capture of records (received or created) in record keeping systems.
- Appropriate maintenance and management of records.
- Ensuring records are accessible when needed.
- Sharing information with other teams and organisations in a controlled manner and in accordance with the Data Protection Act.
- Regularly reviewing the records.
- Disposing of records securely at the appropriate time.

[2] Freedom of Information Act 2000, Section 46 Code of Practice (Section 1, Part V – Importance of Records Management)

2.5 This policy applies to all PSOW staff (including permanent staff, contract staff, temporary staff, and individuals or organisations contracted directly by PSOW). The policy is not intended to cover material generated by a member of staff in their personal capacity. Staff must adhere to the requirements of the Staff Standards of Conduct regarding their personal use of PSOW systems.

3 Benefits & Outcomes

3.1 The Code of Practice issued under the Freedom of Information Act 2000 (FOI Act) states the following:

> "Records and information are the lifeblood of any organisation. They are the basis on which decisions are made, services provided and policies developed and communicated".[3]

3.2 The PSOW considers that good records management benefits an organisation in the following ways:

- It supports the effective discharge of statutory function.
- It supports compliance with other legal requirements.
- It improves corporate memory and access to information which can be used for better decision-making.
- It improves accountability.
- It encourages more efficient working and better use of resources.
- It encourages consistency in working practices.
- It strengthens information security.[4]

3.3 The PSOW is committed to maintaining a well-managed, structured and appropriate set of records in which material will be kept secure and available to those who need it, but not kept for longer than necessary.

[3] Section 46 Code of Practice (Section 1, Part V – Importance of records management)

[4] Ibid.; The National Archives – Guide 4: Keeping records to meet corporate requirements.

3.4 This policy (and associated material) should also assist the PSOW to understand:

- What records are kept.
- Where records are kept.
- Who has access to the records?
- Who is responsible for the records?
- When the records are due to be destroyed?
- How records should be destroyed?
- Any applicable process for the handling of PSOW information by third parties acting under contract or instruction.

4 Legal Requirements, PSOW policies, etc

4.1 The PSOW will comply with all applicable legal requirements relating to the management of records. In particular, the PSOW must comply with the following:

- Public Services Ombudsman (Wales) Act 2019.
- Local Government Act 2000.
- Public Services Ombudsman for Wales (Standards Investigations) Order 2006 (SI2006/949).
- Human Rights Act 1998.
- UK General Data Protection Regulation (UK GDPR).
- Data Protection Act 2018.
- Freedom of Information Act 2000 (and the Code of Practice on the management of records issued under section 46).
- Environmental Information Regulations 2004.
- Common law duty of confidentiality.

4.2 This policy should be read in conjunction with the following PSOW documentation:

- Information Security Policy (and associated procedures).
- Information Asset Register.
- Business Continuity Plan.
- Principles of Good Administration.
- Good Records Management Matters.

- Agreed Set of Principles between the Information Commissioner's Office and the PSOW.
- Staff Standards of Conduct.
- Any other policies, procedures and guidance documents relating to the handling of PSOW records.

4.3 It is imperative that PSOW complies with data protection legislation. Personal data must not be retained unless there is a continuing operational need (or lawful basis) for it. The PSOW Records Retention Schedule sets out the guidelines for record retention periods (both electronic and hard copy), storage locations and disposal arrangements.

5 Standards

5.1 In line with best practice,[5] the PSOW will adopt the follow standards in respect of its records:

Standards		**Supporting documentation**
1.	Records should be held in appropriate locations, and, where necessary, held securely.	Information Security Policy. Information Asset Register.
2.	IT systems should support the management of records through the lifecycle, from creation to deletion.	Information Security Policy. Internal procedures.
3.	Records should be available for legitimate operational use.	Records Management Policy.
4.	Where possible, records should not be duplicated and should follow clear file structures and naming conventions.	Records Management Policy. Internal procedures.
5.	Information Asset Owners should monitor the records falling within their area of responsibility.	Information Asset Register.
6.	Records should be reviewed regularly for relevance and retention	Retention schedule

[5] In line with guidance issued by The National Archives (Managing digital records without an EDRMS)

7.	Records should be destroyed securely and in line with retention schedules	Retention schedule Information Asset Register
8.	All staff should ensure good information handling practice	All PSOW policies, processes and guidance. Staff Job Descriptions.
9.	All records containing personal information should be handled in accordance with Data Protection laws	All policies, procedures

6 Roles and Responsibilities

6.1 **All staff**

All members of staff are responsible for ensuring PSOW records are handled appropriately. In particular, staff should ensure that the records used as part of their day-to-day work are handled in accordance with PSOW policies, procedures and guidance.

6.2 Staff will receive training appropriate to their records management responsibilities.

6.3 **Management Team**

Oversees compliance with this policy and information governance and security standards. Management Team is responsible for approving our Information Governance Strategic Framework and annual records management action plan.

6.4 **Information Asset Owners (IAOs)**

The PSOW's Information Asset Register sets out the organisation's IAOs, together with their areas of responsibility.

The IAOs have responsibility for ensuring that the records and information in their specific area are regularly reviewed, either by themselves or their staff. In doing so, they should have regard for the purpose for which the record was created, the ongoing requirement to keep the record and any applicable retention periods.

6.5 **Senior Information Risk Owner (SIRO)**

The SIRO is responsible for overseeing PSOW's information risk management and advocating good information handling practices. This position is held by the Chief Legal Advisor.

6.6 **Chief Information Security Officer (CISO)**

The CISO is responsible for the security of the PSOW information, including cybersecurity and resilience of PSOW networks. Working with others the CISO advises on how best to manage risk whilst exploiting technology to deliver the organisation's strategic objectives. The position is held by the Chief Operating Officer.

6.7 **Information Governance Manager (IGM)**

The IGM is responsible monitoring internal compliance with the Data Protection Act 2018 and the UK General Data Protection Regulations in respect of any personal data processed by the PSOW.

6.8 **Records Management Group (RMG)**

The group assists in the development of the records management policy, guidance and training as required. Membership of the group changes according to the activities identified within the annual records management action plan and meets as frequently as required.

6.9 **Casework Support**

A member of Casework Support provides day to day records management support. For example, working with IT to ensure that paper and electronic case records are archived and disposed of in line with the requirements of the Record Retention Schedule.

7 Creation and maintenance

7.1 All records created will be accurate, complete and up to date to support operational requirements and decision-making processes.

7.2 The PSOW will ensure that appropriate arrangements are in place for ensuring the continuity and availability of information when staff leave, or during major organisational or technological changes.

7.3 All staff are expected to:

- Undertake training as appropriate.
- Create, keep and manage records which document the PSOW's activities.
- Ensure records are authentic, reliable, have integrity and remain usable and that teams are mindful of information quality assurance.
- Store records within shared repositories as appropriate (e.g. WorkPro, team directories held on The Hub) as opposed to personal filing systems, to ensure that information is managed in a systematic and accountable way and easily located when it is required.
- Adhere to file name conventions as required.
- Adhere to the tracking and monitoring processes in relation to any hard copy records so that they can be easily retrieved.

8 Storage

8.1 All records must be adequately protected and stored securely. Appropriate access controls should be in place and records easily located and retrieved.

8.2 Records will remain accessible and usable for as long as they are required.

8.3 Those commissioning external services will ensure that appropriate contractual arrangements are in place where information is stored, managed or hosted elsewhere on behalf of the PSOW.

8.4 All staff are expected to:

- Ensure that records or information are held securely and accessed on a need to know basis, including information held on removable devices such as DVDs and any information held inside or outside of the office.
- Avoid storing duplicated documents unless this is necessary for ease of working (for instance, the electronic complaint case record is the primary record, and this record must be kept up to date and complete. However, some information may be copied and held on a paper file during an investigation as it may be easier to read on paper than on screen. Once the

investigation is concluded the paper file should be returned to Casework Support to be securely disposed of).

9 Use

9.1 Records must be protected against unauthorised alterations, and authorised alterations should be traceable.

9.2 All records are subject to appropriate security measures in accordance with the Information Security Policy.

9.3 Information is published where it is in the public interest.

9.4 All staff are expected to:

- Adhere to version control requirements as appropriate.
- Protect the personal data and special categories of personal data held in the records.
- Responsibly share information in compliance with relevant legislation.
- Report any issues regarding data quality or risks of data loss to the IGM and/or Head of IT Services.

10 Retention and disposal

10.1 All records must be disposed of securely and at the right time. The Record Retention Schedule details how long records should be kept and why, in line with statutory, operational and best practice requirements. The Record Retention Schedule applies to records held electronically or in hard copy formats.

10.2 A summary Record Retention Schedule will be published to the website alongside this policy.

10.3 Secure facilities are in place to enable the storage of historic paper records. Associated electronic media, which may be kept separately from the paper record, is also destroyed securely.

10.4 There is a clear, documented process in place for the secure destruction of redundant records or the archival of those records held permanently.

10.5 All staff are expected to:

- Adhere to the Record Retention Schedule.
- Reply promptly to records management related queries .
- Dispose of confidential or sensitive information securely using the confidential waste bins provided.
- Ensure that records are not knowingly destroyed if they are subject to current information requests or access may be required by an Inquiry (e.g. The Covid-19 Inquiry) .

11 Records Retention Schedule

11.1 The PSOW's Record Retention Schedule (RRS) is designed as a guide to the retention of different types of records we hold and accompanies our Records Management Policy. The RRS provides guidance to help the PSOW decide what to keep (and for how long) and what to dispose.

11.2 The RRS groups different types of records under relevant business functions. It is important that there are clear processes in place to help implement and maintain the RRS requirements. Any required changes need to be agreed by those administering the relevant processes and then approved by the Information Asset Owner.

11.3 Further guidance is available from the IGM.

12 Monitoring & Compliance

12.1 In accordance with the tasks set out under the UK GDPR, the IGM, in conjunction with the ISG and the RMG will monitor progress with the implementation of

actions identified in the records management action plan. Progress with the implementation of agreed actions is reported to Management Team and ARAC on a quarterly basis.

12.2 The IGM, in conjunction with the SIRO and CISO, is responsible for monitoring the processing of personal data contained within PSOW records.

12.3 Any breaches of this policy should be reported to the IGM or the IT Manager, who will review in accordance with the Breach Notification Process set out in the Information Security Policy.

13 Review

13.1 This policy will be reviewed every three years or following changes in internal processes or external requirements.

13.2 The Information Asset Register and Record Retention Schedule will remain under review according to ongoing business needs.