mental welfare commission for scotland

Respectful · People of integrity · Compassionate · Positive · Knowledgeable

Policy Title: Records Management Policy	**Policy Number: IG-POL-01**
Issue Number: 9	**Date of first issue: February 2005**
Date of last review:	**Date of next review: March 2028**
Lead person: Information Governance Manager	**Approved by: ELT**
	Date approved: 14 April 2026

General Note

The Mental Welfare Commission acknowledges and agrees with the importance of regular and timely review of policy statement and aims to review policies within the timescales set out.

New policies will be subject to a review date of no more than one year from the date of first issue.

Reviewed policies will have a review date set that is relevant to the content (advised by the author) but will be no longer than three years.

If a policy is past its review date, then the content will remain extant until such time as the policy review is complete and the new version published.

1. Policy Statement

The Commission collects and uses a variety of sensitive and personal information about people in order to fulfil its statutory functions and other operational duties. This information includes data on users of mental health, learning disability and social care services and their carers; current, past and prospective employees; suppliers; clients/customers; and others with whom it communicates.

The purpose of this policy is to demonstrate the importance which the Commission assigns to effective records management, to outline key aims and objectives for the Commission in relation to its recordkeeping, and to provide the structure through which its records management policies, procedures and initiatives are to be delivered.

2. Scope

This policy applies to all employees, whether permanent or temporary, including those who are mobile working, Board members, contractors, secondees, and any other persons who are given authorised access to data held by us.

This policy applies to all records created, received or maintained by the Mental Welfare Commission in the course of carrying out its functions.

3. Definitions

Records management - the process whereby an organisation manages its records, whether created internally or externally and in any format or media type, from their creation or receipt, through to their destruction or permanent preservation.

Records –specific recognised type of collated and organised information and data created, received, and maintained as evidence by an organisation for reference in the transaction of business or pursuance of legal obligations. This definition extends to the archive role, particularly in recording corporate memory.

4. Roles & responsibilities

4.1 Chief executive

The chief executive has overall independent responsibility for records management. As the accountable officer they are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. This overall responsibility is delegated to the senior information risk owner (SIRO).

4.2 Head of culture & corporate services

As the SIRO, this postholder has responsibility for ensuring information assets (records) are processed in a safe, fair, and lawful manner. This responsibility extends to all records held by the Commission, in whatever format and for whichever purpose. This extends to the promotion of sound recordkeeping principles and practices in order to support business efficiency and effectiveness.

4.3 Executive directors and managers

Executive directors and managers are the information asset owners of their business areas. It is their responsibility to understand the value of their information from a business and legal perspective, know what to keep and how long for.

The executive director (medical) is also the Commission's Caldicott guardian. A Caldicott guardian has responsibility for the use of patient identifiable information. They are responsible for ensuring use of patient identifiable information is legal, ethical, and appropriate, and that confidentiality is maintained.

The executive director (social work) has similar responsibility in relation to social work data relating to individuals.

4.4 Information governance manager

The information governance manager has the lead responsibility for the overall development and maintenance of records management within the Commission. They are responsible for embedding records management into day to day practice to support the delivery of services, compliance with legislation and efficient, safe,

appropriate, timely retrieval of records. They will also ensure that appropriate arrangements are in place for the disposal of records and will provide advice and guidance to colleagues on record management issues.

4.5 Data protection officer (DPO)

At the Commission, the DPO is the information governance manager.

The DPO holds a key advisory and monitoring role in relation to the use and management of personal data. Their role and responsibilities are defined under UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

4.6 Information asset owners (IAOs)

The IAOs are responsible for managing information risk associated with the information assets they are responsible for on behalf of the organisation and providing assurances to the SIRO. IAOs are senior individuals involved in running the relevant business. The Commission's IOAs are listed in Appendix 4 of this policy. Their role is to understand what information is held, what is added, what is removed, how information is moved, and who has access and why. As a result, they can understand and address risks to the information assets they 'own' and provide assurance to the SIRO on the security and use of the assets.

The IAO relies on line managers responsible for a business area.

4.7 Staff

All staff have responsibility to ensure that they create, manage and dispose of records in accordance with relevant policies and procedures.

All staff must follow this policy and associated procedures at decision making stages. Line managers should also ensure that policies are adhered to, and all staff have completed the relevant training.

5. Operational system

5.1 Introduction

The Commission's records are its corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations.

Records support business activity, policy formation and managerial decision-making; protect the interests of the Commission; and protect the rights of users of mental health, learning disability and social work/social care services, which includes their carers and relatives.

They support consistency, continuity, efficiency and productivity across the range of the Commission's activities.

The Commission is also responsible for the records created by the National Confidential Forum (NCF). The NCF was established as a Committee of the Commission in 2014 under the Victims and Witnesses (Scotland) Act 2014 and came

to an end on the 28 June 2021 under the terms of the Redress for Survivors (Historical Child Abuse in Care) (Scotland) Act 2021. During its lifespan, the NCF was a committee of the Commission and did not exist as a separate legal entity from the Commission.

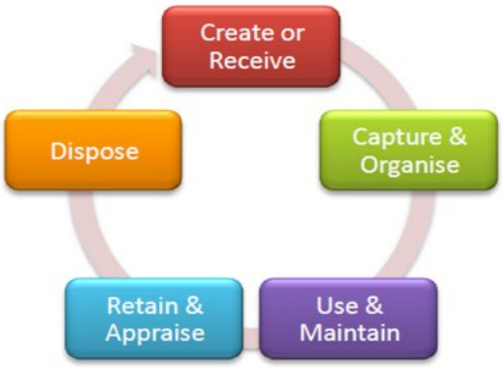
The NCF's core function was to receive and listen to testimony from those who were in institutional care as children.

During its lifespan, the majority of the data was stored in a specially commissioned database in an anonymous (redacted) format. When the NCF came to an end, the redacted testimonies and corporate records were transferred to the National Records of Scotland for permanent preservation. The Commission remains the data controller of the records produced by the NCF.

The Public Records (Scotland) Act 2011 places an obligation on named authorities to produce a records management plan, the purpose of which is to provide for effective management of all records in each of the organisations identified. The Commission is a named authority as defined in the Act. The creation of a records management policy statement is a mandatory element of the plan and is necessary to define the procedures to be followed in managing the organisation's public records.

5.2 What is records management?

Records management can be defined as the process whereby an organisation manages its records, whether created internally or externally and in any format or media type, from their creation or receipt, through to their destruction or permanent preservation.



Records management is about placing controls around each stage of a record's lifecycle, from the point of creation (through the application of metadata, version control and naming conventions); during the maintenance and use phase (through the management of security and access classifications, facilities for access and

tracking of records); at the point of review (through the application of retention and disposal criteria); and, ultimately, disposal (whether this is in the form of recycling, confidential destruction or transfer to the archive branch of NRS for permanent preservation).

Fundamentally, records management is concerned with knowing what information you hold, where it is and how long you are required to retain it, either in relation to business or regulatory/legislative requirements.

5.3 Why is records management important?

Information and records are a valuable corporate asset without which we would be unable to carry out our functions, activities and transactions, or meet the needs of our stakeholders. They are also necessary to ensure legislative compliance.

The benefits of implementing records management systems and processes include:

- Staff, including those who participate in mobile working, have quick and easy access to the right information at the right time in an appropriate format;
- They provide the structure which enables the Commission to ensure that care, treatment and support are lawful and respect the rights and promotes the welfare of individuals with mental illness, learning disability and related conditions;
- There is a common and consistent approach to records management across the organisation;
- Improved business efficiency through reduced time spent searching for information;
- Demonstration of transparency and accountability for all actions;
- The maintenance of the corporate memory;
- Effective risk management processes, in terms of ensuring and demonstrating compliance with all legal, regulatory and statutory obligations;
- Help to meet stakeholder expectations, through the provision of good quality services.

5.4 Commission's records management plan

Section 1 of the Public Records (Scotland) Act 2011 (PRSA) requires every public authority to prepare a 'records management plan' (RMP) setting out proper arrangements for the management of their public records throughout its lifecycle.

The RMP provides public authorities with a framework to set out how their records are being managed. It is separated into 15 elements and each public authority is required to report on their status for each element to the 'Keeper of the Records of Scotland' and provide evidence to demonstrate this. The elements are as follows:

1. Senior Management Responsibility
2. Records Manager Responsibility
3. Records Management Statement
4. Business Classification
5. Retention Schedule
6. Destruction Arrangements
7. Archiving and Transfer Arrangements

8. Information Security
9. Data Protection
10. Business Continuity and Vital Records
11. Audit Trail
12. Competency Framework for Records Management Staff
13. Review and Assessment
14. Shared Information
15. Public records created or held by third parties (not applicable)

The Plan sets the arrangements for the public authority's management of their public records throughout its lifecycle.

Authorities must submit evidence of each of the elements. Authorities can voluntarily submit a Progress Update Review (PUR) one year after the date of agreement of its RMP and every year thereafter. This document provides an opportunity for authorities to report on progress against improvements and comment on any new initiatives, highlight innovations, or record changes to existing arrangements under those elements that had attracted an initial 'Green' score in their original RMP submission. The evaluation of a PUR submission will be undertaken by the National Records of Scotland Assessment Team rather than by the Keeper.

The progress update review is a public document available on the National Records of Scotland website - link here.

5.5 The principles of good records management

The Commission is committed to following the principles of good management as defined by the National Records of Scotland:

AUTHENTIC
It must be possible to prove that records are what they purport to be and who created them, by keeping a record of their management through time. Where information is later added to an existing document within a record, the added information must be signed and dated. With digital records, changes and additions must be identifiable through audit trails.

ACCURATE
Records must accurately reflect the activities and transactions that they document.

COMPLETE
Records must be sufficient in content, context, and structure to reconstruct the relevant activities and transactions that they document.

COMPREHENSIVE
Records must document the complete range of an organisation's business.

COMPLIANT
Records must comply with any record keeping requirements resulting from legislation, audit rules and other relevant regulations.

EFFECTIVE

Records must be maintained for specific purposes and the information contained in them must meet those purposes. Records will be identified and linked to the business process to which they are related.

SECURE
Records must be securely maintained to prevent unauthorised access, alteration, damage or removal. They must be stored in a secure environment, the degree of security reflecting the sensitivity and importance of the contents. Where records are migrated across changes in technology, the evidence preserved must remain authentic and accurate.

5.6 Records and data protection

When creating and/or collating personal identifiable data in the formation of records, organisations must ensure that the collection of this data is necessary, justified, and proportionate, in support of data protection principles and therefore supporting compliance with Element 9 – Data Protection of the RMP.

Record of processing activities (ROPA)

The UK General Data Protection Regulation (UK GDPR) requires organisations to maintain a record of processing activities (ROPA) under its responsibility. This also fulfils part of the requirements under Element 9 – Data Protection of the organisation's RMP. The ROPA can be linked to or detailed within an Information Asset Register providing it contains details of the information processed by the organisation (digital or otherwise), the sensitivity and classification, the information risk, groups of users and who the information is shared with. Information Asset Registers should contain details of the correspondent function within the Business Classification Scheme which the asset relates to.

At the Commission, the business classification scheme, retention schedules and ROPA have been merged into the same document.

5.7 Identifying records

5.7.1 Naming convention (Appendix 3)

The Commission has guidance for naming conventions of digital records (files and folders); this helps identify records using common terms and titles.

They also enable users to distinguish between similar records to determine a specific record when searching the file system. Naming conventions need not be overly prescriptive or formalised, but they must be clear and well defined. Without naming conventions there is a significant risk of records being destroyed or lost within the file system.

The Commission's naming convention follows the National Records of Scotland guidance. Managing digital records without an electronic records management system

5.7.2 Metadata

Metadata is structured information that enables us to describe, locate, control, and

manage other information throughout its lifecycle.

5.7.3 Version control

Organisations should include details of the current and previous versions of the record in the metadata and/or using naming conventions for such purpose (see Appendix 3).

Appropriate version control arrangements that support the management of multiple revisions to the same document should be in place, to ensure that the most up to date versions are being referred to by staff or to ensure that the record which was in place at a certain point in time is easy to identify. To assist with version control for an organisation's controlled documents e.g. policies, guidelines, procedures, it is recommended that document control forms are also in place, which detail the version history and changes applied.

5.8 Storing Records

Records created by organisations should be arranged in a record management system that will enable the organisation to obtain the maximum benefit from the quick and easy retrieval of records whilst also having regard to security frameworks.

Records should be structured within an organisation-wide corporate "file plan" or business classification scheme which reflects the functions and activities of the organisation and facilitates the appropriate sharing and effective retrieval of records. This supports the organisation's requirements under Element 4 of the RMP.

5.9 Securing records

Records must be stored in a secure environment to prevent unauthorised access, alteration, damage, or removal. The level of security should reflect the sensitivity and importance of the information.

The Commission has processes, procedures, and technical controls in place to support the business continuity of records to ensure they are readily available when needed.

5.10 Destruction of records

The Commission has processes, procedures, and technical controls in place to ensure records are securely destroyed. This are explained in the element 6 of Commission's Records Management Plan and further updates (PURs).

6. Risk Management

This policy and the arrangements in place will ensure that the Commission will manage its records as prescribed in the Public Records (Scotland) Act 2011 (PRSA), data protection and related legislation.

A report will be submitted to the Audit, Performance and Risk Committee twice a year with a summary of the actions taken and any significant incidents.

7. Appendices

Appendix 1: Top ten tips for better records management
Appendix 2. Records management Fact Sheet RM, Good Housekeeping
Appendix 3: Naming electronic records and version control
Appendix 4: Information Assets Owners list

8. References

8.1 Legislative framework

- Public Records (Scotland) Act 2011
- The Environmental Information (Scotland) Regulations 2004
- Freedom of Information (Scotland) Act 2002
- Management of Health and Safety at Work Regulations 1999
- Human Rights Act 1998
- UK General Data Protection Regulation (EU) 2016/679 (GDPR)
- Data Protection Act 2018
- Inquiries Act 2005.
- Common law duty of confidentiality. All staff also have a duty to maintain professional ethical standards of confidentiality; this duty continues after leaving the organisation. Obligations around confidentiality remain even after the death of a patient/service user.

8.2 Relationship to other Commission's policies and guidance

- IT-POL-1. IT Security Policy
- IG-POL-03 Data Protection Policy
- IG-POL-2. Information Risk Management and IT code of conduct Handbook for staff o.65. Secure handling use storage retention and disclosure of disclosure information.
- Business Continuity Management Policy
- Records Management Plan
- Data and Information strategy
- Business classification Scheme (BCS) and Retention schedules
    - BCS business support
    - BCS statutory activities
    - Summary retention business support records
    - Summary retention policies statutory activities

External reference documents

New Records management Code of Practice for Health and Social Care, v 2024– final draft - supersedes the NHS CODE OF PRACTICE 2012 and 2020.
Records Management Code of Practice for Health and Social Care - Digital Healthcare Scotland (digihealthcare.scot)