mental welfare
commission for scotland

Policy Title: Records Management Policy	**Policy Number:** 039
Issue Number: 7	**Date of First Issue:** Feb 2005
Date of Last Review: December 2021	**Date of Next Review**: December 2023
Lead Person: Information Governance Manager	**Approved by:** Board

1. Introduction

1.1 The Mental Welfare Commission for Scotland ('the Commission') has duties under the Mental Health (Care and Treatment) (Scotland) Act 2003 and the Adults with Incapacity (Scotland) Act 2000, to ensure that care, treatment and support are lawful and respect the rights and promote the welfare of individuals with mental illness, learning disability and related conditions.

1.2 The National Confidential Forum, (the NCF) was established as a Committee of the Commission in 2014 under the Victims and Witnesses (Scotland) Act 201 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 MWC 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. The Commission remains the data controller of the records produced by the NCF

2. Purpose and scope

2.1 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.

2.2 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.

2.3 The NCF collected sensitive data as part of the conducting of hearings. During its lifespan, the majority of the data was stored in a specially commissioned database in an anonymous (redacted) format. When the Forum came in to an end, the redacted testimonies and corporate records were transferred to the National Records of Scotland for its permanent preservation.

2.3 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.

2.4 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 organisation; and protect the rights of users of mental health, learning disability and social care services, which includes their carers and

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

2.5 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 Mental Welfare 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 in order to define the procedures to be followed in managing the organisation's public records.

3. What is Records Management?

3.1 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.

3.2 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). By placing such controls around the lifecycle of a record, we can demonstrate that the key attributes of **authenticity**, **reliability**, **integrity** and **accessibility** are integral to our records management processes, both now and in the future.

3.3 Through the effective management of the organisation's records, the Commission can provide a comprehensive and accurate account of its activities and transactions. This may be achieved through the management of effective metadata[1] as well as the maintenance of comprehensive audit trail data.

3.4 We retain records that provide evidence of fulfilment of our statutory functions, assigned to the Commission under the Mental Health (Care and Treatment) (Scotland) Act 2003 and the Adults with Incapacity (Scotland) Act 2000.

---

[1] Metadata can be defined in very general terms as 'data about data' and is necessary in order to understand the context, purpose, extent and location of a record. Examples of metadata can include information relating to a record's creator, creation date, receipt date, editor, access history and disposal.

4. Why is Records Management Important?

4.1   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 also to ensure legislative compliance.

4.2 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 promote 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. Policy Statement and Commitment

5.1   The Commission is committed to the creation and maintenance of authentic, reliable and useable records which are capable of supporting business functions and activities for as long as they are required. This will be achieved through the consolidation and establishment of effective records management policies and procedures, including:

- The development of a business classification scheme to reflect the functions, activities and transactions of the Commission.
- The review and consolidation of the retention and disposal schedule to provide clear guidance for the management of Commission records.
- The review and consolidation of destruction arrangements to detail the correct procedures to follow when disposing of business information.
- The review and consolidation of information security policies and procedures in order to protect records and systems from unauthorised access, use, disclosure, disruption, modification, or destruction.
- The review and consolidation of the data protection policy in order to demonstrate the Commission's commitment to compliance with the General Data Protection Regulation (GDPR) and Data Protection Act 2018 and the safeguarding and fair processing of all personal data held.
- The establishment of a business continuity plan, encompassing strategies to ensure that vital records held by the Commission remain accessible over time and that there are processes in place to monitor the integrity and usability of records.
- The review of audit trail mechanisms, the potential of existing systems, and the gap which exists between current provision and best practice, in order to produce a clear strategy for improving the capture and management of key events in a record's lifecycle (e.g. creation, access, editing, destruction or preservation).
- The identification of records management as a distinct stream within the organisation's training portfolio, with dedicated training provided to all staff.
- The completion of a self-assessment review following implementation of the records management plan, in order to ensure that our records management practices remain fit for purpose.

6. Roles and Responsibilities

6.1   The Commission has assigned roles and responsibilities to individual staff to ensure that the Commission's obligation to manage its records effectively is carried out.

6.2   The lead responsible officer for records management in the Commission is the Head of Corporate Services, who is fully supported by the Information Governance Manager

6.3   *Head of Corporate Services* – has overall responsibility for ensuring records management principles are implemented and adopted by all staff, Board members, contractors, secondees, and any other persons who are given authorised access to data held by us. This responsibility extends to all records held by the Commission, in whatever format and for whichever purpose. The Head of Corporate Services is also responsible for the oversight of a corporate approach to the management of records as defined within this policy. This extends to the promotion of sound recordkeeping principles and practices in order to support business efficiency and effectiveness.

6.4 Information Governance Manager – is responsible for the development, updating and communication of this policy and for creating, maintaining and implementing records management standards, procedures and guidance. The Information Governance Manager is also responsible for ensuring that the Commission's record keeping systems adhere to agreed records keeping principles and are managed and maintained in accordance with this policy and associated guidance. The post holder 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.

6.5   Line managers – will ensure that all records created within their area of responsibility are maintained in a way that enables them to be easily retrieved, and provide advice and guidance to their staff on records management issues. Line Managers will ensure that their staff have completed the record management training (see paragraph 9).

6.6   Our staff – have a responsibility to ensure that they create, manage and dispose of records in accordance with relevant policies and procedures. All Commission employees must follow this policy and associated procedures at decision making stages.

7. Legislative framework

The management of the Commission's records will be carried out within the following legislative, statutory and regulatory 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
- General Data Protection Regulation (EU) 2016/679 (GDPR)
- Data Protection Act 2018
-

8. Relationship to other Commission policies and guidance

- No. 5. IT Security Policy
- No.29. Data Protection Policy
- No.57. I.T Information Risk Management Policy
- No.42. Agile Working Policy
- No.65. Secure handling use storage retention and disclosure of Disclosure information
- Business Continuity Management Policy
- MWC naming conventions
- Retention schedules

9. Training

9.1   Training will be provided to all new staff on data protection, freedom of information and records management, to ensure that they are aware of their responsibilities in each of these overlapping areas and to establish effective records management procedures across the organisation.

9.2   The Commission has a specific module on Record Management in the LearnPro e-learning platform. It is mandatory for all staff to undertake this module every two years.

9.3 Line managers will assure that the training has been completed and this is monitored through the performance framework.

10. Monitoring and review

10.1   The Information Governance Manager will provide updates to the Executive Leadership Team meeting as required. Where non-compliance with this policy is discovered, appropriate action will be taken to put a solution in place and the matter reported to the ELT.

10.2   This policy will be reviewed biennially by the Commission's Board.

ADDENDA 1
Top ten tips for better record management

The documents we create and the records we keep are vital for every aspect of Commission working. The right information must be available to the right person at the right time to conduct business efficiently, make fully informed decisions, collaborate effectively with the Commission's partners and deliver first-class services.

All Commission staff are responsible for the proper management of the information they work with. This fact sheet provides some common sense tips to achieve this and points to others that provide more detailed guidance to help improve the management of records across the Commission.

These rules apply to all documents and records regardless of format or location.

1. Capture and create adequate records to meet the Commission's needs
When documenting work, ensure you capture and create quality records to support current and future working and provide sufficient evidence for internal and external audits and inspection. Quality records are ones that can be trusted as full, reliable, consistent, accurate, secure and accessible.

2. Name your electronic documents and folders consistently
Follow the naming conventions approved and available on the Intranet.

3. Do not store records on your "C" drive
No records should be saved to C: drives – information on the C: drive of your laptop is only available to you and is not automatically backed up so there is a greater risk of loss due to equipment failure.

4. Manage your emails by content, not format
Significant emails and attachments should be filed with related records on the shared drive or IMP. All others should be deleted once actioned. Where appropriate, save the full email conversation (incoming and sent emails) and ensure it has an appropriate title.

5. Store information in the correct system and filing area
Make sure that you store your files in the correct information system – shared drive or IMP – and filing area.

6. Share information appropriately

Where possible collaboration should be undertaken on a network folder to which all parties have access. Email hyperlinks to shared network drives, rather than emailing a copy of the actual document as an attachment. Attaching the document leads to file duplication and version conflict.

7. Keep personal and confidential information securely

Personal sensitive information must be saved on Imp. Restrict access to folders containing personal and confidential records only to those staff who need to access them. Do not leave computers unattended when logged-on, change your passwords at regular intervals, and use encryption where appropriate. Store confidential paper records in locked cabinets or drawers when not in use.

8. Regularly clear out files of unnecessary documents

Take time to regularly weed files (both paper and electronic) and destroy/delete unwanted working copies, trivial emails and out-of-date reference material.
This will save time looking for the information you need and reduce storage space.

9. Folders structure.

The Information Asset Owner (IAO) should think about the structure of the folder at the start of each project and create consistent subfolders and naming convention (so each themed visit/ investigations follow the same/similar structure)

It is also good practice to close down electronic folders at appropriate intervals to keep them at a manageable size. e.g. end of calendar or financial year, project close, completed application process, completed service user case.

This will make it easier to apply Commission retention periods and keep folders at a manageable size for searching and browsing.

10. Make sure you know how long to keep your major categories of records

Consult the Commission's Retention Schedule to work out how long records should be kept for and dispose of (or delete) records accordingly and in the appropriate manner.

If you require any further information, please contact the IGM.

ADDENDA 2

RECORDS MANAGEMENT FACT SHEET RM GOOD HOUSEKEEPING

All Commission staff have responsibility for managing the records they create, receive and use in the course of their work. The guidance supports you in meeting this responsibility. It is good practice to carry out what we can call housekeeping tasks, enabling you to self-monitor and ensure that you are managing these records in the best way to support your own working, that of your colleagues and fulfil the Commission's information governance requirements.

1. Clearing out personal drives

It is clearly bad practice to save Commission records on personal drives as these are inaccessible to others and are not backed up. Impacts of this include wasted time searching for inaccessible information, file duplication, compromised decision making due to incomplete information, compromising of compliance with data protection and freedom of information.

Check your personal directories regularly to ensure they only contain your own personnel files.

2. Tidying up your email
While email is a very effective communication and distribution tool, poor email working practices can also impact adversely on your productivity and lead to stockpiles of temporary information that very quickly becomes obsolete, scattered with isolated valuable business records. Applying the following good housekeeping rules to your email inbox and sent items will help your email work for you rather than against you.

- Use your inbox only to store those emails that have still to be actioned.
- Save any emails and attachments that are business records/service user records to the appropriate location on the shared drive or IMP. Remember your sent items too as this will also contain records that will need to be accessed for information and evidence in the future.
- Regularly clear out emails in in-boxes, sent items, draft, delete item and other private folders.
- Avoid using the "auto archive" function as this creates yet more silos of information which will be lost not just to others but to you too.

3. Tidying up shared server drives

Many of the electronic and paper documents saved on shared drives are ephemeral and would only need to be retained for a short period of time, they can be destroyed as soon as they are no longer of business use.

When carrying out a clear out, either on your own or as a team exercise, use the following list to identify items that can be routinely destroyed after immediate business use:

- files kept "just in case"
- convenience copies of policies, procedures, guidance, memos etc.
- files that have been downloaded from Intranet or internet
- files which have been created for temporary use and for one-off exercises to do calculations, data manipulations, labels, signs, posters, etc.
- information collected for a specific project long completed and for which you were not the lead officer or where specific issues have been resolved
- files of a personal nature, shouldn't be saved on a shared drive

4.   Misfiling and misnaming

When we are in a rush it is easy to misfile information or name files in a way that, at a later date, makes no sense to ourselves or others. Also, when we can't work out which folder to save a file to, it is tempting to create a new one e.g. miscellaneous or general. These are all sure fire ways to lose information and to waste time trying to find and potentially recreate the information. When you come across paper and electronic files that have been misfiled, take the time to move them to the correct place. If you come across files that need to be opened in order to find out what they are about then clearly the file name could be more meaningful. Again take the time to rename the file to aid future retrieval, following the Commission's file naming convention guidance.

Folder Owners/IAO should monitor the use of folders and file naming conventions and organise staff training and clear-up sessions to ensure that the effective and efficient file creation, filing and naming becomes part of normal working practice.

ADDENDA 3
NAMING ELECTRONIC RECORDS AND VERSION CONTROL

Why do we need naming conventions?
Using standard terms and following consistent rules for how we name files and folders has a number of benefits for everyone:

- groups related records and documents together and in a logical order
- saves time naming files and searching and browsing for the information we need
- helps identify the most current version of a document
- helps identify obsolete, superseded and out-of-date documents

Naming files – basic rules
The file name should provide a quick signpost to what is contained within a file and help to distinguish between documents on the same topic. When naming a document, think about whether someone in 5 years will be able to work out what it is about just from looking at the title as they may be using it in an entirely different context from the one you created it for. The following rules will help you achieve these goals.

1. Provide short, meaningful titles
The title should be short and meaningful and contain, at a minimum, the following elements:
- Subject – what the document is about e.g. the "subject" of this fact sheet is "naming conventions"
- Document type – e.g. minute, report, invoice or, in this case "fact sheet"

Depending on the content and context of the document, you should include additional information
e.g. for correspondence:
- Date – the date sent or received
- Outgoing correspondence – "to" and recipient name
- Incoming correspondence – "from" and sender name

e.g. for documents going through a review and approval process e.g. policies, reports, meeting minutes
- Status – e.g. draft, copy, final
- Version number – e.g. V0-1, V2-1

2. Avoid unnecessary information
People often include information in the file title that is unnecessary or automatically captured elsewhere:

- avoid words that add no value to the title meaning e.g. "a", "the", "of"
- do not include document type in file names in IMP as you will supply this in a separate indexing field
- so long as the file remains in its current parent folder, do not repeat information already sign posted in the folder name.
- do not include creation or modified date as this information is automatically captured in the properties of the file.
- do not include the file type as this indicated in the file extension and icon

3. Use capital letters or underscores to separate words, not spaces.
There are a number of reasons for this rule:
- When a file name is converted to a hyperlink, spaces are converted into %20%
- Some applications do not support spaces

File names should be written in lowercase, starting with a Capital, which is used to separate each word.
e.g.   FileNamingConvention.doc or file_naming_convention.doc

4. Avoid the use of non-alpha numeric characters

File names cannot include any of the following characters as they may not be recognised in file names by other document management systems. Even if the Commission's systems allow you to save the file, if you send it to someone outside the Commission, they may not be able to open it:

/ | \ : > ; , < ? * ",.
Hyphens and underscores can be used.
Dots/full stops should only be used to separate the file name from the file extension and not used within the title. Including dots within the title can cause problems when migrating the file into certain information management systems

5. Agree standard terms for consistency
Standard terms (including abbreviations and acronyms) should be agreed to ensure consistent terminology is used for the names of committees, organisations, activities and subjects.

6. Use of dates
If dates are used in folder or file names, order them in the format YYYYMMDD so they will be listed chronologically.

7. Use of numbers
When using numbers in titles, work out the highest number that will be required and use the following format so they are listed numerically –
Up to 10 – 01,02,03 …10
Up to 100 – 001, 002, 003, …033, 034, ..099, 100 etc..

8. Personal names
When it is appropriate to include a personal name in the file title (e.g. correspondence, appraisals) it should be given as surname first followed by initials as it is most likely that the record will be retrieved according to the surname of the individual.

Surname	- Enter prefixes such as O' (without the apostrophe), Von, Van as part of the surname. - Enter Mc or Mac as they are spelt. - Enter surnames with hyphens as whole units, e.g Smithers-Brown becomes SmithersBrown
Forename(s)	Enter only initials, unless the combination Surname+Initial already exists. In this case, enter the full forename.

9. Naming Folders
The names given to folders should enable the viewer to instantly identify the contents within the folder. Avoid dashes, commas, abbreviations or jargon when naming folders.

10. Use a standard protocol for version control

Some records go through a number of versions, starting out as working drafts and then moving on to a review and approval process prior to release as a finalised record. It is important to be able to differentiate between these various drafts, using a consistent version numbering protocol at the end of the file name.

The following simple protocol for version control should be used:

- o Draft documents - V0-1; V0-2; V0-3 …

- o Approved document – V1-0

When an approved document then moves into a new review phase e.g. annual review of a policy,

- o Documents under review: V1-1; V1-2; V1-3 …
- o Approved updated document: V2-0

The document control history of more formal review processes should also be documented within the content of the document, ideally using a formatted document template (see – *Creating and Capturing Records* for more information on templates)