mental welfare commission for scotland

Policy Title: Records Management Policy	**Policy Number:** IG-POL-01
Issue Number: 8	**Date of first issue:** February 2005
Date of last review: January 2024	**Date of next review:** January 2026
Lead person (title)**:** Information Governance Manager	**Approved by: Board**
	Date approved: 27 02 2024

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 their 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.

4.2 Head of Culture & Corporate Services

As the Senior Information Risk Owner (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 Caldicott Guardian (Executive Director - Medical)

The 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.

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 practices 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 (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 Information Assets Owners are listed in Appendix 4 of this policy. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result, they are able to 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. The National Confidential Forum, (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 Forum came into 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 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.

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.

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.

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

- No. 5. IT Security Policy
- No.29. Data Protection Policy
- No.57. I.T Information Risk Management Policy
- No.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 2023– final draft - supersedes the NHS CODE OF PRACTICE 2012 and 2020.

Appendix 1: Top ten tips for better records 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 added to this policy as Appendix 3.

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 available in Appendix 3 of this policy (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 Commission's Information Governance Manager.

Appendix 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 (Appendix 3).

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.

Appendix 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 instead of 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:

- Draft documents - V0-1; V0-2; V0-3 …
- Approved document – V1-0

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

- Documents under review: V1-1; V1-2; V1-3 …
- 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)

Examples:

Incorrect	Correct
The records and files management new group (folder)	RecordsManagementGroup(folder)
Request received on 11 March 2024.docx	20240311Request
Sharing agreement between the Commission and HIS final last version 2024.docx	MWC-HIS-SharingAgreement2024Final-v.1
Updated Suggested framework for decision (to be handout)-Sep 12.docx	201209FrameworkForDecisionHandout-v1.1.docx

For meetings/minutes and documents saved in the same folder when date is relevant 12 March 2023 meeting 30 February 2023 meeting Meeting 12 Aug 2022 Last meeting 11 03 2024	For meetings/minutes and documents saved in the same folder when date is relevant Reverse data YYYYMMDD will show the documents in order: 20220812.docx 20230230.docx 20230312.docx 20240311.docx In some cases, an additional brief description can be useful if the document needs to be accessed out of its folder (the folder name is also part of the name and can contain relevant information about the records content)

Appendix 4: Information Assets Owners list

Business area	***Information Asset Owner***	***IAO Operatives***
Corporate information	Julie O'Neill	Katrina Thomson
Complaints	Paloma Alvarez	
Information Governance	Paloma Alvarez	
Finance and Payroll	Elizabeth Halliday	
HR	Katherine Meikle	
IT systems and information security	Elizabeth Halliday	Robert Osborne
Systems Imps	Elizabeth Halliday	Patricia Lambelet
Information Management system (IMS)	Suzanne McGuinness	Gail Devaney
Communications	Mary Mowat	Terry Rogers
Advice line – information on (IMPS plus policies and procedures)	Julie O'Neil	
Enquiries emails	Mark Manders	Michael Banks
Engagement and participation activity- Influencing and good practice	Suzanne McGuinness	Hazell Ness
Visits: **Local visits** **Themed visits** **Monitoring visits -AWI**	Claire Lamza	Neil Parson Margo Fyfe Lesley Paterson
Investigations & inquiries	Suzanne McGuinness	Mark Manders Paula John
Casework Administration	Julie O'Neill	Michael Banks
Statistic and Research	Julie O'Neill	Elaine Robertson
LD & Autism Review	Closed Project	Paloma Alvarez
Preservation Library	Paloma Alvarez	
Intranet site (under review)	Fiona Hamilton	
Neurosurgery and consent. DMP	Arun Chopra	Dichelle Wong

Last updated 12 03 2024