Comhairle Ceantair an Iúir, Mhúrn agus an Dúin
Newry, Mourne and Down District Council

Records Management Policy and Procedure

Ag freastal ar an Dún
agus Ard Mhacha Theas
Serving Down
and South Armagh

Comhairle Ceantair
an Iúir, Mhúrn agus an Dúin
Newry, Mourne and Down
District Council

Policy Control

Policy reference:	CS30
Title:	Records Management Policy
Version:	2.0
Directorate/Departmental ownership:	Corporate Services/Administration
Officer responsible:	Assistant Director Corporate Services
Corporate Management Team authorised on:	26 July 2023
Senior Management Team authorised on:	09 August 2023
Strategic, Policy and Resources Committee authorised on:	17 August 2023
Council authorised on:	04 September 2023
Review date:	10 September 2027
Location where document is held and referenced:	Responsible Department ☒

Version Control

Version	Date	Amendments made	Amended By
V0.1	30/08/19	Authorised by Corporate Management Team	Sally Andrée
V0.2	05/09/19	Authorised by Senior Management Team with amendment to Beach Clause	Sally Andrée
V0.3	13/09/19	Authorised by Strategy, Policy and Resources Committee with inclusion of guidance on Transferring Records (Procedures, Page 19)	Sally Andrée
V0.3	07/10/19	Authorised by Council	Sally Andrée
V1.0	15/10/21	Approved version published	Sally Andrée
V1.1	28/06/23	Added Control table, page 2 Amendment to legislation - UK GDPR, page 3	Sally Andrée

Version	Date	Amendments made	Amended By
		Updated record requirements adding Relevant and Timely, page 4 **Procedure:** Pages 6 – 8 Defining a Record - new Pages 9 – 12 E-Records Management - new Pages 13 – 16 E-Records Naming Convention – new and updated Page 17 Version Control – IT amendment re file titles and table added to provide clarification on version numbering Page 18 replacement of MS Windows with 'the product in use' Page 19 update to Record Creation Page 20 update to Record Maintenance and addition of link to ATIPP slides Page 22 amendment to update disposal process with Information Asset Owner Page 23 amendment to Lost and Missing Records Page 25 addition of link to ATIPP slides Page 26 Record formats new and amended Page 29 Roles and Responsibilities – addition of Head of Compliance and Records Management Team duties and amendment to IT Department responsibilities. Pages 30 – 31 Role of the Information Asset Owner Page 31 amendment to Monitoring Page 32 Appendix B – Data Classification, Protective Marking and Information Handling has now been incorporated into the main body of the Procedure and L&S Drives added to Page 36 Pages 36 and 40 One Drive replaced with Office 365 **Appendices updates and new additions** Appendix A – revised text Pages 39-44 Appendix B – updated Glossary Page 45 Appendix D – Archive Box Label Template Page 49 Appendix E – Disposal of Records Form Page 50 Appendix G – Guidance and Best Practice Page 52	
V1.1	30/06/23	Provided comments/amends	Edel Cosgrove
V1.2	03/07/23	Updated as per amends	Sally Andrée
V1.3	26/07/23	Authorised by Corporate Management Team with amendments to Roles and Responsibilities (Assistant Director, Head of Compliance, Records Manager & Records Officer)	Sally Andrée
V1.3	10/08/23	Procedure updated as per IT amendments pages 6, 14, 17, 18, 29, 36 and 40 as above.	Sally Andrée

Contents

Records Management Policy

Title

Newry, Mourne and Down District Council's (NMDDC) Records Management Policy

Statement

NMDDC endorses the Records Management Policy as a framework for the Council's compliance with the Public Records Act (NI) 1923, Disposal of Documents Order (No. 167) 1925, Section 46 of the Freedom of Information Act 2000 – Records Management Code of Practice, Data Protection Act 2018, UK General Data Protection Regulations (UK GDPR) Freedom of Information Act 2000, Environmental Information Regulations 2004, Re-Use of Public Sector Information Regulations 2015, the Local Government Act (Northern Ireland) 1972, the Local Government Act (Northern Ireland) 2014 and Section 75 of the Northern Ireland Act 1998.

Aim

The aim of the Records Management Policy is to ensure NMDDC's compliance with statutory and regulatory requirements affecting the use and retention of records. NMDDC's records are a vital corporate asset: they provide evidence of Council's actions and decisions. NMDDC is committed to creating, receiving and maintaining authentic, reliable and useable records, which are capable of supporting business functions and activities for as long as they are required and will provide sufficient resources and training to ensure the Council keeps the records it needs for business, regulatory, legal and accountability purposes.

Definition

Records Management is defined in BS ISO 15489-1:2016 Information and Documentation - Records Management, as the field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including the processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.

The Records Management Policy will ensure that all records are:

- **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 electronic records, changes and additions must be identifiable through audit trails.

- **Accurate**
  Records must accurately reflect the transactions that they document.

- **Accessible**
  Records must be readily available when needed.

- **Complete**
  Records must be captured in full.

- **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.

- **Relevant**
  Records need to meet current and potential users' needs.

- **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.

- **Timely**
  Information is recorded and available as soon after the event as possible.

Scope

NMDDC's corporate records are a unique and irreplaceable resource, and the proper management of this resource is necessary to satisfy Council's internal business processes and to comply with the law. A small percentage of NMDDC's records will be selected for permanent preservation because of their long term historical / research value and as an enduring record of the conduct and management of the Council.

The Records Management Policy applies to all Council staff, including temporary staff, and Elected Members who create, receive, use and maintain records in the course of Council business. It also applies to contractors, consultants, volunteers, third parties and contracted out services, that have access to, process or manage Council records.

The Records Management Policy applies to all records, regardless of the format or technology used to create and store them, that are created, received, maintained and held in the course of Council business and thereafter retained for a set period to provide evidence of its activities and transactions.

The Records Management Policy includes all records that are held or processed on all Council sites and/or shared with, or managed by, third parties and to business information systems used to create, store, maintain and archive or dispose of records.

Related Policies

NMDDC's Retention & Disposal Schedule
NMDDC's Information Security Policy
NMDDC's Access to Information Policy & Procedure
NMDDC's IT Policies & Procedure
NMDDC's Social Media & Acceptable Use Policy & Procedure
NMDDC's Privacy Notice
NMDDC's Publication Scheme
NMDDC's Customer Services Charter

Breach of this Policy

Any breach of this Policy and its associated procedures by staff will be investigated in accordance with Council's disciplinary procedure, any action taken will depend on the circumstances of each individual case. Any breach of this Policy and its associated procedure by non-staff will be investigated and steps taken in accordance with the law and any relevant contract.

The Records Management Procedure attached hereto and Best Practice and Guidance documents produced by the Records Management Team must be adhered to in the delivery of this Policy.

Equality Screening

This policy has been equality screened and the outcome is that it not be subject to an Equality Impact Assessment (with no mitigating measures required).

Rural Impact Assessment

Due regard to rural needs has been considered and a rural needs impact assessment has been completed.

Records Management Procedure

Introduction

Records Management is defined as the field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including the processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.

Newry, Mourne and Down District Council's (NMDDC) records are Council's corporate memory and, as such, it is vital that Council prioritise the management of every facet of a record from creation through to disposal in an appropriate manner.

Records are a valuable resource and records management is the process by which NMDDC manages all aspects of records and information, from creation through to eventual disposal (Records Life Cycle). The aim of the accompanying guidance documents is to ensure:

Accountability – records are adequate to account fully and transparently for all business actions and decisions in particular to protect legal and other rights of staff or those affected by those actions; facilitate audit or examination; and provide credible and authoritative evidence.

Accurate – records accurately reflect the transactions they document.

Accessibility – records can be located when needed and only those persons with a legitimate right can access the records. The information within them is displayed consistently and the current version is identified where multiple versions exist.

Storage – electronic and physical storage is utilised fully to ensure the correct and secure management of records.

Interpretation - the context of the record can be interpreted, i.e.

- Who – identification of staff who created or added to the record;
- When – during which business process; and
- How – the record is related to other records.

Quality – records can be trusted - are complete and accurate and reliably represent the information that was actually used in, or created by, the business process and a record's integrity and authenticity can be demonstrated.

Maintenance through time - that the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed despite changes of format and changes to the corporate structure.

Security – records are secure from unauthorised or inadvertent alteration or erasure, access and disclosure. They are properly controlled and there are audit trails to track all use and changes in order to ensure that records are held in a robust format which remains readable for as long as records are required.

Retention and disposal – records are retained and disposed of appropriately in accordance with NMDDC's Retention and Disposal Policy and Schedule (R&DS).

Staff are trained – that all staff are made aware of their responsibilities and use their time effectively regarding records management.

Legislation

In addition to being an efficient business tool for Council, an effective records management policy is required to allow NMDDC to manage all its records in accordance with legislative requirements.

The Public Records Act (NI) 1923 established the Public Record Office of Northern Ireland (PRONI) as the place of deposit for public records, created the roles of Keeper and Deputy Keeper of the records and defined the context of public records.

The Disposal of Documents Order (No. 167) 1925 sets out how public authorities should deal with the disposal of public records once their business need comes to an end, i.e. destruction of those records that have no long-term value or the preservation and transfer of records selected for permanent preservation to PRONI.

The Code of Practice under Section 46 of the Freedom of Information Act 2000 (FOIA) provides guidance to public authorities on the keeping, management and destruction of records.

The aims of the code are twofold, the first aim is to provide a suitable set of practices in relation to the creation, management and disposal of public records and the second deals with the arrangements for reviewing and transferring the records to a place of deposit once their administrative use has come to an end.

The FOIA and the Environmental Information Regulations 2004 (EIR) give the public the legal right of access to recorded information held by public authorities unless a relevant exemption applies.

The Data Protection Act 2018 (DPA) and UK General Data Protection Regulations (UK GDPR) give anyone the right to information held about them by a public authority and set out rules to ensure that information is handled properly unless a relevant exemption applies.

The Re-Use of Public Sector Information Act 2015 (RPSI) governs the use of public sector information for a purpose other than the initial public task it was produced for. RPSI is about permitting re-use of recorded information and how it is made available. In Northern Ireland the OpenDataNI Portal facilitates the re-use of public sector information through published datasets.

The roles and functions of councils, established in the Local Government Act (Northern Ireland) 1972, require a commitment to the development of an efficient and effective records management system. The Local Government Act (Northern Ireland) 2014 confers upon the Council the power of general competence and a duty to continuous performance improvement.

Compliance with the Records Management Policy and Procedure will be augmented by the creation and maintenance of departmental records management manuals that document departmental practices around record creation, storage, management and disposal in line with this procedure.

Related NMDDC Policies

NMDDC's Retention & Disposal Schedule
NMDDC's Information Security Policy
NMDDC's Access to Information Policy & Procedure
NMDDC's IT Policies & Procedure
NMDDC's Social Media & Acceptable Use Policy & Procedure
NMDDC's Privacy Notice
NMDDC's Publication Scheme
NMDDC's Customers Services Charter

Defining a record

A lot of information is generated as part of your day-to-day work, but most of it would not be classified as a record. It will help your workload if you understand how to recognise the difference between records and the kind of superfluous material which can be destroyed.

The definition of 'document' and 'record'

In records management it is important to be clear about the difference between a document and a record.

A document is any piece of written information in any form, produced or received by an organisation or person. It can include databases, website, email messages, word and excel files, letters, and memos. Some of these documents will be ephemeral or of very short-term value and should never end up in a records management system (such as invitations to lunch).

Some documents will need to be kept as evidence of business transactions, routine activities or as a result of legal obligations, such as policy documents. These should be placed into an official filing system and at this point, they become official records. In other words, all records start off as documents, but not all documents will ultimately become records.

Record means anything in which information is recorded, regardless of format, created or received, maintained and disposed of by any organisation in the transaction of business or the conduct of affairs which provide evidence of actions taken and decisions made.

In other words, records are the final products of your work, or the information that feeds into those final products. A record shows what happened or what was intended to happen and tracks decisions as well as the options that were available to inform those decisions.

Records may exist in contracts, memos, paper files, electronic files, reports, emails, CCTV footage, digital media, social media posts or business information systems.

How to recognise Council records

There are certain records that are vital to the running of the Council. The following list outlines some of the key types of Council records, but there will be others:

- customer records, for example, application forms, certificates, licences, receipts, etc.;
- staff records including contracts and attendance details;
- records relating to the governance of the Council including Council and Committee agendas, minutes. In addition, there may be emails or notes concerning the background to meetings which might also be considered records if they include decisions;
- records which relate to the legal and financial position of the Council, including contracts, financial records, accident reports and property deeds; and
- records which feed into the history of the Council, including records about the origin of the Council and its departments, community planning, strategic planning, etc.

How to recognise superfluous material

Some information has no significant operational, informational or evidential value and so should be destroyed as soon as its use has passed.

Under the UK GDPR and DPA, the Council is required to keep personal data only as long as is necessary. An individual can request access to all personal data, including emails and other correspondence, by making a subject access request under the DPA. It is advisable to delete or destroy any personal data once it has become superfluous. You can read more about the legislation in Council's Access to Information Policy and Procedure.

Other examples of superfluous material are meeting requests, notifications of acceptance or apologies, duplicate documents, marketing materials, forms, manuals, etc.

What should I file?

You should file any document that is important to you in your work for NMDDC, for example:

- the final version of a letter, presentation, report, spreadsheet, etc.;
- non-routine emails;
- minutes of meetings if you are the secretary; and
- documents you need to keep for legal reasons.

You should not file information that is of no continuing value to Council's work, for example:

- working drafts, duplicates, junk mail, newsletters, notices, trade literature;
- personal or local copies of records that are filed elsewhere, e.g. policies, reports; and
- routine emails such as invitations to meetings or acknowledgements.

There will be times when you need to exercise your judgement on whether or not you should file something. Ask yourself, *'would I or a colleague need this information in the future in order to understand properly the work to which it relates?'* If the answer is 'yes' then file it and if it is 'no', or if you are unsure check with your line manager or the Records Management team.

Business Classification of records

A Functional Business Classification Scheme is a system in which your business area decides the naming convention and organisational principles of your record keeping system.

Classification work commenced with Council's updated R&DS categorising records into functions, activities and transactions and these are being further developed into an organisational classification scheme for each department. This is a cooperative effort involving the Records Management team and business areas.

Checklist – What is a record?

This checklist has been designed to help you determine whether or not an item should be treated as a record.

If the answer to any of the questions is 'Yes' then the item is a record and it should be captured and filed in an official record keeping system.

Was it made or received in the course of official business?	YES/NO
Does it document a function of the organisation?	YES/NO
Does it document an action taken?	YES/NO
Does it document an action made?	YES/NO
Does it document the formulation of a policy?	YES/NO
Does it document a decision-making process?	YES/NO
Does it document a change to organisational policy or procedure?	YES/NO
Does it have financial implications?	YES/NO
Does it have legal implications?	YES/NO
Is it required for the operation or administration of normal business processes?	YES/NO
Does it need to be approved by another individual or body?	YES/NO
Does it need to be reported to another individual or body?	YES/NO
Does it set a precedent?	YES/NO
Is it governed by legislation?	YES/NO
Does it affect or protect the rights and entitlements of citizens?	YES/NO

- Any officer who creates a record is responsible for ensuring that it is captured in an official record keeping system.
- Any officer who receives a record from outside the Council is responsible for ensuring that it is captured in an official record keeping system.
- If you receive a record from another officer in the Council, you should not have to file it as it should already have been captured.

E-records Management

In March 2021, the Strategy, Policy and Resources Committee endorsed prioritising a digital first approach to Council records[1]. A digital record is defined as electronic information in any form created or received and maintained by an organisation or person in the transaction of Council business or the conduct of affairs and kept as evidence of such activity.

Electronic records should be arranged consistently and logically so that they can easily be found and used. They should be structured into folders and sub-folders with the other electronic records, including emails, that belong with that subject, case or project. The default space for storing electronic records is the Q Drive.

Each business area needs a sustainable system for managing electronic information and this takes time, however, when the system is running effectively it will save time for everyone. It will also support more effective information management and knowledge sharing, helping you meet your objectives and work more efficiently.

Creating and managing folders

A folder is a container within a file system used to store records (and other folders). It is the principal building block of a filing structure. Ideally, you will be able to identify and manage the contents of your folders without having to open and review the content of each individual file, document, or email. Defining a strong folder and file naming system creates good habits, reduces the time and effort required to manage your electronic records, and supports business continuity and compliance for the office.

The best folder structure is the one that mimics the way you work, e.g. if you plan important tasks quarterly or annually then a new folder for each quarter or year's work is a good starting point and if you work on projects then create a new folder for each project but with the same sub-folders for each.

Browsing through folders and finding files should be intuitive. If the method of organisation is tedious, it's going to be hard for the rest of the team to follow. For company projects, pick something that works well for everyone in the team, since everyone may not search for a file or folder in the same way you do. If you want to maintain your folder structure long-term, you'll want to make sure everyone understands (and hopefully likes!) the system.

Folder names should be unique, short and meaningful: this will facilitate more efficient sharing and retrieval of information. Folders should be named according to activity or transaction rather than directorate, department, business area and must NEVER be personal names. They should describe the work that is being done, not who is doing it.

New top-level folders on a shared drive should only be created with the agreement of the Information Asset Owner/Administrator. They must have an owner, who will agree the names of lower-level structures and access rights to all folders in the structure.

Lower-level folders should contain files in all formats (Word, Excel, PowerPoint etc.) You should not maintain separate folders for different file formats, such as a folder for Word files and another for Excel spreadsheets: records should be managed according to function, not format.

[1] Strategy, Policy and Resource Committee Minutes 11 March 2021

If for any reason the contents of the folders need to be protected or secure, **a service request should be made to the IT HelpDesk via Hornbill. You must advise the Records Manager that a hidden folder has been created.**

Folders should be closed and locked if there has been no activity for 12 months or if the number of items in the folder exceeds 100, since managing and searching for documents becomes difficult and slow.

Folders that are in continuous use should be closed annually. For example, for agendas, minutes and background papers for meetings; 'archives' should be created annually so that efficient information management and retrieval can be maintained.

A folder should also be closed if the work associated with it has ceased, for example a project is completed.

The business area must decide on whether it is important to divide folders and sub-folders by date, client, project, subject matter, usage, etc, to maximise the usability of the folder for retrieval and disposal.

Folder names should not be repeated in the hierarchy as redundant detail only increases the length of file names and paths. Instead of:

Q:/Compliance/Operations/Compliance Team Meetings/Meetings 2023 /May/10.05.2023Minutes.doc

Use:

Q:/Compliance/Operations/Team Meetings/2023/May/Minutes.doc

A strong folder structure:

- groups together records by function, such as putting all contracts or complaints in one location;
- groups together records by cut-off and retention period for easy deletion at the end of the deletion period – don't mix your 1 year and 6 year records;
- allows for easy identification of individual records without having to open each file to determine what it contains; and
- is straightforward and quick for everyday use – resist overcomplicating and don't add too many folders.

Deleting folders

All electronic folders must be managed according to retention schedules. A folder should contain documents which have the same retention period attached to them in order to facilitate easy management of the destruction of data at the appropriate time.

Very few documents should be retained on network drives permanently. Retention schedules provide rules for the retention and destruction of records. Other saved information should be held for up to 6 years after business use has ceased.

A folder should be deleted when:

- its contents have reached their destruction date or have been moved to an alternative archive folder for retention management. Folders should not be deleted along with their contents unless a review of use has been carried out;
- it contains duplicate information for individual or team reference and the business use has expired;
- it contains working documents, e.g. report updates (not official drafts) and other information on which a record has been based, where the business use has expired; and

- the folder contains duplicate information for individual or team reference and the business use has expired.

Staff must record all deletion of electronic records in accordance with the Record Disposal guidance below.

Creating documents

When you create a document, you need to make decisions about its purpose and content so that it can be effectively managed throughout its lifecycle.

You should use templates to create frequently used types of documents, such as reports, minutes, press releases and presentations. They provide a consistent and professional format with appropriate branding and document properties, and prevent information being overwritten. This is especially important for documents which are routinely released to the public.

Templates should be named according to the rules described in this guidance and be available for all to use on a shared drive within an appropriately named folder. A template can be identified by the file extension .dotx for Word documents, .xltx for Excel, or .potx for PowerPoint.

When creating new documents, spreadsheets, presentations, etc on the departmental Q Drive they must be saved within a relevant folder and not on the same level as folders as this will disrupt the filing structure. If it relates to a new project or new calendar year, etc. create a new folder first before saving the record within it.

Saving documents

Outlook is a communication, not document management, system, and should not be used to store email messages, see Guide to Email Records Management for information on managing your mailbox.

When a document is ready to be saved, there should be one logical location for it, usually on the departmental Q Drive. You should not keep duplicate records. If required, links to a document can be stored in other folders for specific circumstances, such as when they provide background to the work files saved in that folder. To create a shortcut, right click on the document name and choose Create Shortcut.

Related information is sometimes held in both paper and electronic formats, for example, where a paper correspondence file contains incoming letters and the responses are held electronically. This is referred to as a 'hybrid' file and it must be cross-referenced. The paper folder name and location should be added to a document called Paper folder properties which should appear at the top of the electronic folder. The folder title should also note that it is hybrid. Similarly, the paper file should contain a reference to the location of the electronic folder.

PDFs

A PDF retains its original security features and recipients cannot edit the information unless the author allows editing, therefore:

- When sending a final document by email, save and send it as a PDF rather than the native file.
- When saving a corporate document to the R Drive or Intranet, save it as a PDF rather than a native file.

There are three main types of electronic records, and each should be treated differently. Documents should be named according to guidance on Naming Convention and Version Control.

Shared documents and records

These are documents and records that are shared among colleagues and constitute the bulk of the information most of us use every day. As soon as a document reaches a point where it is to be shared with or reviewed by colleagues, it should be stored on a drive accessible to that person or group. This prevents duplication of documents and reduces network traffic.

Attaching documents to emails means a document is duplicated to every recipient and causes congestion on the servers. More importantly, it will cause uncertainty as to which is the latest or authoritative version of a document. **If you are notifying colleagues via email that a document is available on the shared drive, provide a link to that document instead**, using the 'point and click' method. See Guide to Email Records Management on how to create a hyperlink.

Working documents containing incomplete information, which have not contributed to any final business decisions, should be deleted as soon as they are no longer of use, for example when the final version of the document has been approved.

Storing documents and records on a shared drive offers the following advantages:

- avoids duplication;
- allows for accurate version control; and
- improves access for information retrieval, both for business use and as necessary to respond to information requests.

These documents and records should be stored on a shared drive.

Confidential shared documents and records

Records should be open and accessible unless it can be shown that it is necessary to restrict access to them. Examples of confidential information include minutes and reports from closed sections of meetings, and documents containing personal information such as employee or customer data.

Access to folders can be restricted to particular individuals or groups. You must contact the IT Helpdesk via Hornbill to set up restricted access to shared folders.

Passwords should be used sparingly and preferably in circumstances where access is limited to one or a few people. You should also consider the risks involved when staff are away from the office, and access is needed to password-protected documents. Passwords should be removed when a document is ready to be shared.

These documents and records should be stored on a shared drive.

Personal documents

These documents contain information that is personal to its creator and not related to functions and duties performed for work but is linked to their work, e.g. Learning & Development Certificates; People, Perform Grow forms, etc.

These documents and records should be stored on the personal drive.

Deleting documents and records

Destroy electronic documents and records in the same way as physical ones: the content determines the nature of the file, i.e. document or record; use the R&DS to ensure compliance and complete the Disposal of Records Form for all Council electronic records.

E-records Naming Convention

Make finding electronic records easier

This document is intended to provide a common set of rules to apply to the naming of electronic records. The conventions are primarily intended for use with Windows based software and documents such as word-processed documents, spreadsheets, presentations, emails and project plans. 'File names' are the names that are listed in the file directory and that users give to new files when they save them for the first time.

The conventions assume that a logical directory structure or filing scheme is in place and that similar conventions are used for naming the levels and folders within the directory structure.

Why use naming conventions?

Naming records consistently, logically and in a predictable way will distinguish similar records from one another at a glance, and by doing so will facilitate the storage and retrieval of records, which will enable users to browse file names more effectively and efficiently. Naming records according to agreed conventions should also make file naming easier for colleagues because they will not have to 're-think' the process each time.

Multiple documents stored on shared drives can become unruly quickly. Without a naming convention it is difficult for users to determine the version status and whether the record has been acted upon. All records should be named consistently with a method for naming that is documented, shared, and agreed upon by the service area.

Naming folders and files

In addition to using a strong folder structure, appropriately naming your files and folders is an advantage to managing your records properly.

Metadata is data that describes the context, content and structure of a record and helps users to easily search for and find a record. Metadata will also allow users to manage a record throughout its life cycle. By ensuring the title of the record contains information such as the subject, date created, description, author, etc. users can search across a wide range of data to find both paper and electronic records efficiently.

Do:

1. Keep file names short, meaningful and specific.

2. Use keywords to reflect the purpose of the document and make the name meaningful to others to allow it to be easily located both now and in the future.

3. Use a structured approach placing emphasis on the strongest element at the front of the title sequence, e.g. a case reference number.

4. For readability, start all names with a capital letter. Start additional words within names with capital letters. Capitalize any acronyms in names.

5. Avoid initials, acronyms and abbreviations unless regularly in use, easily recognisable and will remain understandable during the retention period.

Business areas should create a "Read Me" file that contains a brief glossary of terms for the sake of future clarity.

6. Use capital letters to delimit words, **not** spaces, hyphens or underscores.

7. Keep file names brief – ensure file names **do not exceed** 50 characters in length (including spaces and file extension). Note that even if a file name is only 50 characters long, it might exceed the total recommended character length of the file path because of where it sits in the filing structure. Microsoft Windows does not support files whose entire file path exceeds **200 characters** and the IT Department is therefore **unable to support, back-up, or restore any such files or folders**.

8. When using a date in the file name always state the date in this format:

   YYYY or YYYY-MM or YYYY-MM-DD

   Using this format means that the chronological order of the records is maintained when files names are listed in the file directory which assists with file retrieval.

   To ensure that files are sorted in proper chronological order, the most significant date and time components should appear first followed by the least significant components. If all the other words in the file name are the same, this convention will allow us to sort by year, then month, then date.

9. When using a number in a file always give it two digits, i.e. 01-99.

10. Save digital photographs as '.jpg' files and must not exceed 2Mb in size. Exemptions must be approved by the IT Department.

11. When saving items such as digital photographs and scanned images, change the title from the system-generated number to something meaningful.

Don't

1. Repeat a name that is included in the folder name and avoid repetition and redundancy.

2. Use staff or team names within the file name as this may prevent others from locating the file, can be confusing and/or superfluous and may result in a data protection breach;

3. Use terms such as 'my', 'stuff', 'general' or 'miscellaneous' or generic terms such as 'Meeting, 'Presentation, 'Latest Version'.

4. Use non-alphanumeric characters, such as: ? ; : / \ < > * & $ £ + = and full-stops/dots. Hyphens may be used.

5. Use all capital letters in the naming of your document.

6. Identify electronic file format information, powerpoint presentation, email, excel, etc. as this is automatically captured in the metadata.

7. Use initials when referring to individuals always use the name in full, e.g. 20230112 MeetingWithJohnSmith and not 2023.0112 MeetingWithJS.

8. Use words describing the form or format of a document; words such as 'draft', 'letter', 'presentation', 'spreadsheet', should not be used at the start of file names.

9. Use names that lead to confusion, e.g. 'Final, Final Draft', 'Old' or 'Don't Use'. If a file is in draft form, then then version numbering will reflect this, if it is no longer in use, then archive or delete it as appropriate.

Naming Emails and Correspondence

The file names of emails and correspondence should include:

- the name of the correspondent;
- an indication of the subject;
- the date of the correspondence; and
- whether it is incoming or outgoing.

You don't need to include an indication of the subject, as it's given in the folder name.

If you are saving an email with attachments use '**att**' in the file name along with the number of attachments contained within it, e.g. **.../Complaints/.../JSmithS2I1 20230630att3.msg** (ordered alphanumerically) represents the first incoming correspondence of a Stage 2 complaint on 30/06/2023 from J Smith with 3 attachments.

Remove FW' and 'RE' from the titles of emails saved to folders.

To ensure that files are sorted in proper chronological order, the most significant date and time components should appear first followed by the least significant components. If all the other words in the file name are the same, this convention will allow us to sort by year, then month, then date.

Remember, MS Office cannot guess what you mean and so you need to be accurate and maintain that accuracy with all associated files for a particular topic or service.

Naming elements

The name of the document is made up of elements that when brought together will form the filename. The filename should also appear in the footer information. Using naming elements is beneficial because once you become familiar with the agreed upon naming convention its use efficiently relays a lot of information. Key elements include:

- transaction, project or account number;
- subject or activity (required);
- document form;
- date (required if not using Version); and
- version (required if not using date).

Document Form

Use one of the abbreviations below to identify the document form. If you require a new abbreviation, please email the Records Management Team and we will add it to the template.

Table of Abbreviations

ACK	Acknowledgement	LTR	Letter
ACT	Action Request	MEM	Memo (internal)
AGD	Agenda	MIN	Minutes
AGR	Agreement	MNL	Manual
ANN	Announcement	MTG	Meeting
APP	Appendix	NSL	Newsletter
ART	Article	PLN	Plan
BIO	Biography	PMT	Permit
BRC	Brochure	POL	Policy
BRN	Briefing Note	PPR	Paper
CHT	Chart	PRC	Procedure
CON	Contract	PRF	Profile
COM	Customer Complaint	PRO	Proposal
COV	Cover Page	PRS	Presentation
DFT	Discussion Draft	PRL	Press Release
DRT	Directory	REQ	Request
DWG	Drawing	RES	Response
EXA	Example	RPT	Report
FCT	Fact Sheet	RVW	Review
FRM	Form	SCH	Schedule
GRA	Grant	SPE	Speech
GUI	Guidelines	SRY	Survey
INT	Interview	SUM	Summary
INV	Invoice	SUP	Supplement
INX	Index	TML	Timeline
LGL	Legal Document	TOR	Terms of Reference

Version Control

Version control is the process by which different drafts and versions of a document or record are managed. It is a tool which tracks a series of draft documents, culminating in a final version. It is important that the system is applied systematically and consistently, particularly when a document is updated by different people and at different times. Version control is beneficial for documents such as policies, procedures or regulations.

Using a system of version control means that:

- there is an 'audit trail' of how a document developed during the drafting process;
- you can be confident that you have the most up to date version of a document;
- you can prove which documents were 'in force' at a particular date – this might be crucial for appeals processes, for example; and
- you can confidently delete draft or redundant versions of documents.

Version control is achieved by adding a number at the end of a file title. Each successive draft of a document is numbered sequentially from 0-1, 0-2, 0-3… until a finalised version is complete. This would be titled version 1-0. If version 1-0 is to be revised, drafts would be numbered as 1-1, 1-2, etc. until version 2-0 is complete.

NOTE: the version number added to the **file title** must be written with a hyphen **'-'** and not a full stop/dot **'.'** in accordance with the guidance set out in Naming folders and files.

Version Details

Draft Versions	
0-1	Initial draft of a new document sent for review
0-2	Second draft sent for review
3-1	Initial draft of previously approved document, e.g. updating the 3rd version of a policy

Final Versions	
1-0	Final version of the first issue of a document
4-0	Final version of the fourth issue of a document

In addition to adding the version number to the end of the file title, it should also be displayed within the document where it may be written as 1.0, 2.1, etc. The version number should appear on any document title page and also in the header or footer of each page. To ensure against the accidental loss of final versions of records, a read-only tag can also be applied. Should any changes to this document be made, the user will be prompted to save the file with a new title.

Version Control Tables

Some documents will require a version control table, which should be inserted at the beginning or end of the document. This approach may be necessary for documents where there are legal or regulatory reasons for having a clear audit trail of changes. It is also good practice for all policy documents. The version control table (see example below) must be updated each time a change is made to the document. It details:

- the new version number;
- the date of the change;
- the person making the change; and
- the purpose of the change or the change itself.

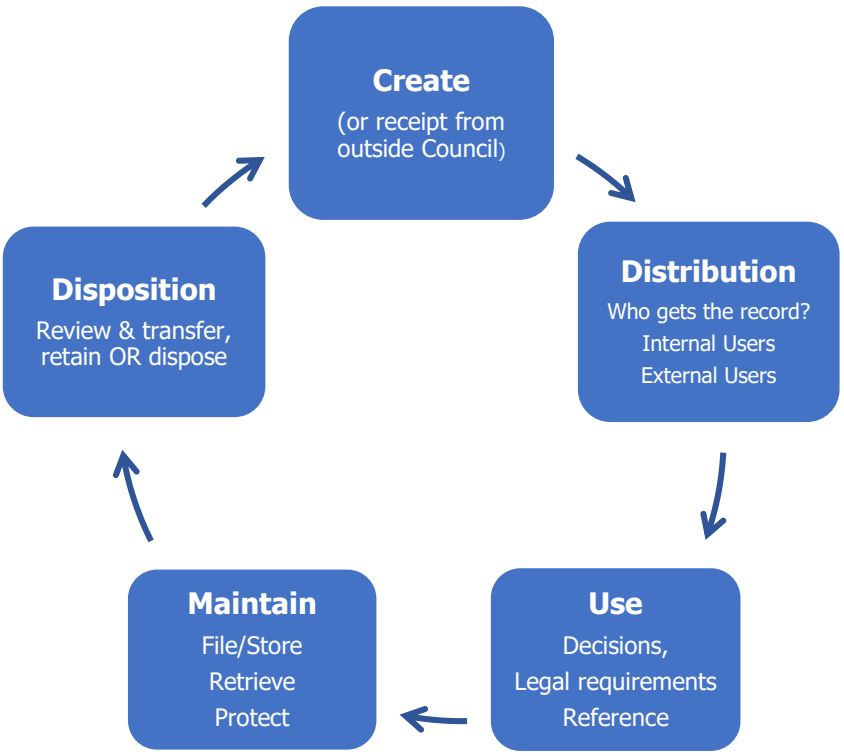
Versimon	Date	Changes	Author
0.1	21/03/2018	Initial Draft to Working Group	J Smith
0.2	02/04/2018	Suggested amendments added by track changes	J Smith
1.0	06/06/2018	Final version approved by SMT	J Smith
1.1	08/09/2018	Draft revision of Section 2.3 to clarify procedure	E Brown
2.0	10/09/2018	Revision approved by SMT	J Smith
3.0	03/05/2019	Update to contact details	M White

Keeping Drafts and Final Versions of Documents

Once a document is finalised, a decision should be made on whether the drafts should be kept or whether they can be deleted. In the majority of cases it is possible to delete drafts once the final version of a document has been agreed. This will reduce confusion caused by the duplication of documents and means that there is less danger of earlier versions being accidentally made available or having to be provided under the FOIA. Drafts must be kept if it is necessary to preserve a record of the process of developing the document. This may be, for example to maintain a record of why particular changes were made or to help when the document is redeveloped at some future date.

'DRAFT' or 'FINAL' watermarks must be added to documents, spreadsheets and powerpoint presentations, to make their status clear to all users. Use MS Office Help to advise on adding watermarks as the steps will vary dependent on the version of the product in use.

Record Lifecycle



The record life cycle describes the different stages records follow in their lifespan from creation or receipt to use and maintenance and finally disposal which is either the destruction or permanent preservation of the record.

A records management system captures, manages and provides access to records from creation through to disposal. NMDDC has three types of manual record systems, these are:
Physical paper record systems;
Unstructured electronic record systems, e.g. network drives and electronic mailboxes; and
Structured electronic record systems, e.g. databases and IT business information systems.

Record Creation

All records should be created in accordance with the Corporate File Plan, Appendix A, which provides a framework for a consistent approach to classifying records across Council regardless of format or physical location, or in accordance with the departmental file plan which relates directly to each department's core function. The references for departmental files and records originate with the business information system, e.g. Tascomi; or the funding body of a project, e.g. Interreg V; etc., specifically created for or aligned to that department. These file plans are used to identify and retrieve records and practical steps should be taken to ensure that duplicate records are not created.

All files, electronic and paper, should include the minimum data set: reference number, file name and date created.

Officers should always ensure that they do not have more personal data than needed to achieve the purpose for which the data is being processed.

If a new file series is being created in response to a new data processing system, technology, project, etc., which requires the collection, receipt and processing of personal data and is considered "high risk", an assessment is required to identify if there is a need to undertake a Data Protection Impact Assessment (DPIA) to minimise the data protection risks created by the processing. The DPIA will provide information that will allow for secure processing and retention of personal and sensitive personal data which will guide how the associated records are created and stored. The DPIA template is saved in R:\Policies and Procedures. Queries can be directed to the Data Protection Officer.

Newly created information must be assessed to identify if it falls within the scope of NMDDC's Publication Scheme and the Records Manager informed of the specific class of information, its description, relevant publication and availability including any charges if applicable.

Record Maintenance

Electronic files must be saved and stored in line with this procedure and updating and cleansing folders must be carried out routinely, refer to Data Cleanse Guidance for Electronic Files for guidance. Files must be moved to retention/archive folders at the appropriate time and in accordance with the R&DS.

Storage accommodation for paper records must be safe from unauthorised access, clean and tidy, prevent damage to the records and provide a safe working environment for staff.

All paper files should be kept in good condition. If a file becomes too big then the file should be split, and new folders created to hold the information. The new folders should be marked clearly with the same details and clearly indicating which section it refers to; Part 1, Part 2, etc. Inform Records Management when new parts have been created so the filing system can be updated to reflect any changes.

Records containing personal data (whether active or archived, paper or electronic) must be weeded periodically to reduce the risks of inaccuracies and excessive retention and to ensure compliance with the UK GDPR Data Minimisation principle.

Records that have been superseded must be updated or replaced within the file structure, the Publication Scheme and the corporate website.

Record Access

It is important that records are protected from unauthorised access, however they must be stored in a manner that ensures the efficient delivery of Council services and accurate naming and storing of files is essential to achieve this.

Individuals have a right to access NMDDC's records under legislation such as the DPA, GDPR, FOIA and EIR. Effective and compliant records management allows Council to meet these statutory obligations and the Access to Information Policy and Procedure saved in R:\Policies and Procedures provides information on managing requests for recorded information held by Council.

Record Disclosure

There are a range of statutory provisions that limit, prohibit or set conditions in respect of the disclosure of records to third parties, and similarly, a range of provisions that require or permit disclosure. Refer to Council's Access to Information Policy and Procedure or the Access to Information Training Slides for further information on managing the disclosure of Council records and/or contact the Compliance Team.

Record Security

Information security is "the practice of preventing unauthorised access, use, disclosure, disruption, modification, inspection, recording or destruction" of sensitive records. NMDDC is committed to ensuring the confidentiality, integrity and availability of Council's records and the Data Classification, Protective Marking and Information Handling section provides detailed guidance on Council's procedures for security.

Line Managers should ensure that before a member of staff leaves, any records held by that employee which only they can access, e.g. P Drive, Outlook, should be transferred to team/departmental folders and obsolete information deleted. **The** IT Leavers Procedure **should be completed for leavers, movers and long-term absence.**

At the point at which an Elected Member's term of office comes to an end, all information (including emails) held on Council equipment will be retained and/or disposed of in accordance with Council's R&DS. All Elected Members are responsible for adhering to this policy and procedure. Should any non-Council information be held on any item of IT equipment Elected Member's should remove prior to return, otherwise it will be deleted. The Democratic Services Manager should ensure completion of this task.

Refer to the IT Procedures for more information on leavers, internet use, etc.

Record Closure

When a record is closed it must be documented and stored to ensure that it remains accessible throughout its retention period and can be reviewed prior to either destruction or selected for permanent preservation. When a file is closed no new papers should be added to it.

NMDDC's R&DS provides retention timescales to ensure files are not kept longer than necessary.

Electronic media, such as CDs, should not be attached to or stored with paper records to ensure preservation of these materials. These should be filed separately with the location noted on the original record and filing system.

Review and sort files before closing them to remove unnecessary material that is not relevant to the record.

Closing Electronic Records

Electronic folders should be archived if there has been no activity for 12 months in an archive folder created for this purpose. Sub-folders will hold the retained the data and Line Managers will retain access to carry out six monthly reviews of the contents and, where applicable, implement the disposal of relevant records and folders in accordance with Council's R&DS.

Folders that are in continuous use should be closed annually. For example, for agendas, minutes and background papers for meetings, 'archives' should be created annually so that efficient information management and retrieval can be maintained.

Closing Paper Records

Each hard copy file must have a Certificate of File Closure attached to the inside cover of the file. If a large number of files are being boxed together for archiving, a list of the contents should be attached to the top and sides of the box, see Appendix D – Archive Box Label Template.

- Department name;
- File reference;
- File name;
- Date file closed;
- Proposed disposal date; and
- Box # of # (if applicable)

For further information on closing files and associated forms refer to Council's R&DS.

Record Disposal

It is important that records are not kept for longer than is needed. A record can only be retained for longer than the minimum period if it is required for an existing request for information or legal proceedings.

The length of the retention period depends upon the type of record and is based upon the business needs of NMDDC in addition to the regulatory environment within which the Council operates.

Records must be retained, closed and disposed of in accordance with this procedure, Council's Retention and Disposal Schedule and any relevant privacy notice.

The retention period is calculated from the point the file is closed and destruction will take place following a review and authorisation by the Information Asset Owner and in accordance with the Retention and Disposal Schedule.

All final action decisions must be agreed with the Records Manager and the Assistant Director Corporate Services and recorded on the Disposal of Records Form.

Destruction will be conducted by a confidential waste paper disposal contractor or as the Council deems appropriate.

Where the action is permanent preservation by Council, the records will be referred to PRONI at the end of the retention period for a decision as to the disposition of the contents.

Where the action is PRONI permanent preservation appropriate arrangements will be put in place to ensure timely transfer.

Non-records should be disposed of as soon as possible after their primary usefulness has expired. Unlike Council records, non-records do not require approval prior to their disposal. Non-Records may still be valuable to departmental business processes and they may still be expected to be kept locally within a department for future business processes. For example, some units may want to have ready access to reference copies of contracts for use when drafting new contracts for similar goods and services. For this reason, departments may intentionally retain these copies for specified periods of time, but they should plan to dispose of the materials as soon as their primary usefulness has expired.

Vital Records Management

Vital records are essential to NMDDC's core business and must be processed and stored accordingly. Historical records that are not essential to the operation of Council but are of value are recorded in the Retention and Disposal Schedule and should be included in any business continuity plan.

Electronic vital records must be stored on central servers so that they are protected by appropriate back-up and disaster recovery. They must not be stored on portable hardware or on a laptop hard

drive or personal hard drive. A readable format such as PDF/PDFA or plain text or rich text format should be used for vital records that are assigned a lengthy retention period.

Vital Records which are only available in paper format should be duplicated, in the same or original format depending on requirements, and the originals and copies stored in separate locations if possible. If duplication is impracticable or legally unacceptable, fire protection safes must be used to protect the documents.

Lost / Missing Records

It is important that records can be retrieved at any time whether active, inactive or closed for administration and/or legal purposes. A lost/missing record is a record either that cannot be found following a search in the office environment or is unavailable. **The loss of records constitutes a reportable incident and should be reported in accordance with Council's** Breach Management Plan**.**

The missing record must be marked as missing in either the electronic or manual tracking system in use. A temporary file should be created, clearly marked as a temporary file, populated with all relevant information available for that record and the electronic or manual filing system updated to note that a temporary file has been created.

When the record is found record the following:

- the date it was found on the electronic or manual filing system;
- name of the person who found the record;
- the location where it was found;
- the reason why it was lost and returned, if known; and
- document lessons learned in the process to prevent future misplacement of files.

When a file containing personal data or sensitive personal data has been recovered, notify Council's Data Protection Officer immediately. Refer to Council's Access to Information Policy and Procedure for further information on Council's breach management plan.

When a file containing sensitive commercial data has been recovered, notify the Information Asset Owner immediately providing details of the recovery.

Review the temporary and original files and merge together and notify the details of the incident on the electronic filing system and/or on the inside front cover of the hard copy file.

If, after six months, the record is still missing, inform the Data Protection Officer that the record is permanently missing. Document the missing record and actions taken to recover it and update the temporary file accordingly. Implement lessons learnt to prevent future loss of files.

Tracking Records

Recording and knowledge of the whereabouts of all records is essential if the information they contain is to be located quickly and efficiently. One of the main reasons why records get misplaced or lost is because their next destination is not recorded.

A departmental tracking system for all records should be in place to ensure that all information can be found quickly and easily.

A manual tracking system may consist of an index card or tracking schedule to record movement of information. An electronic tracking system could be on a spreadsheet using an On Loan column or on a database using the Notes section to record file movements.

To ensure that information is correct and applicable, all departments must ensure that their tracking system is routinely checked and updated.

Tracking systems should record the following minimum information:

- the reference number of the record;
- any other applicable identifier i.e. department, building, etc.;
- person or department who is taking the file out on loan;
- person, department and place to where it is being sent; and
- date of loan / transfer; and
- date of return, if system applicable.

See Appendix F – File Tracking Schedule

Transferring Records

When a file is requested by another department and/or location choose one of the following options for both the delivery and return of the file or folder:

- collected/returned in person, details and receipt to be confirmed by email; or
- sent securely via Council courier or internal post – request email confirmation of receipt.

Both options require the sender, or borrower if applicable, to complete the File Tracking Schedule.

Files must be named and have a reference number before they can be transferred, this includes drafts and working documents, codes can be used to protect the contents if they contain OFFICIAL-SENSITIVE material. Ensure that files are collected by staff members appropriate to the classification of the file and that files are protectively marked and securely packaged.

In the event that a colleague collects or returns the file on behalf of the record owner/requester this must be agreed in advance and an email confirmation of receipt sent.

Where possible, requesters should indicate how long they may require the file and return it as soon as possible once the file is no longer required.

File owners should regularly audit their filing system and confirm the status of any files out on loan to departmental colleagues or other departments/locations.

Should a staff member loan a file to a colleague whilst it is signed out in their name they will remain responsible for its security and will be held accountable in the event that it is mislaid.

Taking files home is discouraged but, if it is essential for a staff member to take a file home, they have personal responsibility to ensure the information is kept secure and confidential. This means that other members of their family and/or their friends/colleagues must not be able to see the content or have any access to the information. It is particularly important that official-sensitive information in any form is not left unattended where possible. Officers and Elected Members should refer to the Access to Information Policy and Procedure for further security guidance and Council's Access to Information Training Slides.

It is the responsibility of the staff member to note on the File Tracker Schedule that the file is being removed from its storage location and ensure that they return it as soon as practicably possible. The file must not remain out its storage location indefinitely. If the file in question has been borrowed from a colleague or other department, it is the responsibility of the staff member to email the file owner of the date they are removing the file and the date they have returned it to the office.

Record Formats

Email and Messaging Channels

Electronic Records which invoke the definition of 'document' and 'record' which includes any Emails, Texts, WhatsApp messages, Photographic Images, Social Media messages and MS Teams correspondence must adhere to the guidelines set out within this procedure.

Officers/Elected Members should refer to the Access to Information Policy and Procedure for further security guidance and Council's Access to Information Training Slides.

Officers/Elected Members leaving Council or moving to another department must transfer any business-related emails, texts, WhatsApp messages, social media messages, photographic images and Teams correspondence to the IAO or a designated colleague to ensure the data is retained for Council use.

Paper Diaries

NMDDC issues paper diaries for staff use on official Council business. These diaries remain the property of NMDDC at all times as they form a record of Council business activities and staff are responsible for the safe keeping and secure storage of them.

NMDDC is the owner of all Council information which is recorded and stored in diaries, irrespective of whether the diary is Council issued or acquired externally but used for Council business.

All Council staff and Elected Members have a personal responsibility for ensuring any personal identifiable data, confidential or sensitive information is held securely and therefore no personal data is to be held within these paper diaries.

Names and domestic addresses of customers or other activity locations should be recorded but must not be written together. If a printed record with personal data is required to facilitate a domestic site or other visit it must be kept securely and disposed of upon return.

Information noted in paper diaries whilst on site or other visits must be transferred to the appropriate document, business information system on return to the office. File notes of conversations that form a record must be filed in accordance with this procedure.

Staff leaving Council must return their paper diary to their line manager and Elected Members to Democratic Services. Paper diaries will be held securely in the departmental office for one year following completion and then transferred to archive storage in accordance with NMDDC's R&DS.

In the event of the loss or theft of a paper diary the staff member or Elected Member must immediately notify Council's Data Protection Officer of the incident to minimise the risk of a data breach.

Roles and Responsibilities

The Council is responsible for adopting this Records Management Policy & Procedure, considering and approving changes to it, and reviewing reports on records management matters.

The Chief Executive Officer and Directors have overall responsibility for ensuring that the Council complies with the requirements of legislation affecting the management of records with any supporting codes and regulations.

The Corporate Services Assistant Director's role is to lead and champion the Council's key commitments as identified in the Corporate, Community, Directorate and Service Business Plans by providing leadership and focus within the service, specifically Corporate Compliance.

The Head of Compliance is responsible for Information Governance and the management of risk associated with this area. This includes overseeing the creation, monitoring and updating of the Records Management Strategy, Policies and Procedures and providing strategic advice and guidance as required.

The Records Manager is responsible for the effective and appropriate management of Council's records from their creation, right through to their eventual preservation or disposal to ensure the Council meets its statutory obligations in accordance with the relevant legislation and best practice. He/she will assist in the promotion of the strategic and operational importance of Information Governance and Corporate Records Management to the organisation and take responsibility Council wide for working with staff and mangers at all levels of the organisation in order to provide a high quality and efficient records management function.

The Records Officer supports the Information and Records Management function to implement high standards of records management and maintain effective systems for electronic and paper records management to ensure the Council meets its statutory obligations in accordance with relevant legislation and best practice. He/she will champion a culture of high-quality information management across Council, acting as a centre of excellence for advice and a hub for departmental Business Support Managers.

Council's Information Asset Owners are responsible for ensuring that all information and records management systems within their control comply with the Records Management Policy and Procedure and to take the necessary remedial action when they do not.

The IT Department is responsible for supporting Records Management by providing guidance and codes of conduct on the use of IT systems. IT is also responsible for the security of data held electronically on Council supported systems and ensuring that it is backed up in accordance with Council policy.

All Council Staff have records management responsibilities and should be aware of the value of the records they create, process and maintain and are responsible for.

Individual Elected Members should be aware that records created within the conduct of their role are the property of Council and therefore must be processed and maintained in accordance with the Records Management Policy and Guidance and the Retention and Disposal Schedule and associated legislation.

Responsibilities of Third Parties

Third Parties, e.g. contractors, consultants, etc., must adhere to this procedure and have their own administrative practices documented and assessed in similar ways to Council business units as part of the tendering and contract monitoring processes. To do this, they must allow access by relevant Council staff to any Council records they create, receive or manage, including any record keeping system within which they are held.

Council Staff, Elected Members and Third Parties must not intentionally delete, destroy or alter official records. Records are only to be disposed of in accordance with Council's Retention and Disposal Schedule.

Role of the Information Asset Owner

The Council holds a wealth of information. This information can be in different formats and held in a variety of locations and systems. It is essential that the Council understands the information it holds so that if can adequately manage and protect it. Article 30 of the UK GDPR requires organisations to maintain a record of the personal data it processes, and Council has extended the use of the Retention and Disposal Schedule to incorporate these requirements.

An information asset owner (IAO) is a senior individual who holds relevant responsibilities in relation to a particular business area. Their role is to understand what information their staff hold (physical and digital records), what is added, what is removed, how information is transferred and who has access to it and why. As a result they will be able to understand and mitigate risks and provide assurance to the Director of Corporate Services in relation to the security and accuracy of their information assets.

IAOs should be in position to have a good knowledge of their asset and how and why it is processed to give them an understanding of the risks and opportunities associated with it. They also need to be aware of the consequences and impacts of those risks materialising.

IAOs must ensure that regular data quality reviews of records containing personal data are conducted to make sure they are accurate, adequate and not excessive and ensure lessons learnt are recorded and acted upon to prevent recurrence.

IAOs manage information risk from a business not a technical perspective. It is important to remember that information management responsibilities extend further than digital data, but also include building security, personnel (training and development) and paper records too. IAOs are empowered to take some risk decisions within their own portfolio and within their risk tolerance.

The IAO has five main responsibilities:

- lead and foster a culture that values, protects and uses information correctly;
- provide assurance for the security and use of their asset annually to the Director of Corporate Services;
- be responsible for approving, monitoring and minimising data transfers or sharing;
- ensure the asset is fully used for its intended purpose or for the individual it relates to, including responding to access requests; and
- approve data protection impact assessments (DPIA) for any new systems or projects that involve the processing of their information asset.

Information risks to manage

IAOs are responsible for managing risk associated with information assets; information assets face the following serious risks:

- Inappropriate access to, or disclosure of, protectively marked or personal data by staff, contractors, volunteers and the public, whether accidental or deliberate;
- Inappropriate data sharing – too much or irrelevant data is shared internally, i.e. a full list with all personal data is provided where only numbers of a specific category have been requested;
- Internal threat - staff, acting in error or deliberately, or external parties accessing your information illegally and exposing it/acting maliciously to defraud you or your customers;
- Information loss - particularly during transfer or movement of information, or as a result of business change, e.g. local government or internal restructure;
- Loss of access to information;
- Records management – that information assets are not retained for longer than required. They should only be retained for long periods either by law or for business need, as outlined in the corporate R&DS;
- Business continuity/disaster recovery – that the relevant personnel are aware of the agreed continuity and recovery for their services;
- Loss of digital continuity - i.e. losing the ability to use your information in the way required when needed. By use we mean being able to find, open, work with, understand and trust your information. The lifecycle of a piece of information - how long you need to use and keep it - is often different to the lifecycle of the IT system used to access and support it;
- Poor quality of information and poor quality assurance, for example, of data sets;
- Poor change management - business needs change, systems change, your information risk appetite may change, so you need to keep your policies and processes in step accordingly; and
- Not maximising the public benefit from information, leading to a waste of public money and poor service delivery.

IAOs and Information Leads should contact the Data Protection Officer for guidance on identifying and managing information risk.

Training

All staff and Elected Members will be provided with mandatory Records Management training which will be required to be undertaken every three years, subject to legislative amendments. Refresher guidance will be provided annually.

Records Management training will form part of the Council's induction for new employees. A copy of this policy and procedure will be provided to all employees and Elected Members.

Monitoring and Review

To ensure this Procedure complies with the regulatory and statutory legislation and meets the needs of Council it will be reviewed every four years. If there is a change in legislation and/or internal processes review may complete sooner.

The Records Manager, in conjunction with the Assistant Director Corporate Services, is responsible for the monitoring, revision and updating of this document.

Data Classification, Protective Marking and Information Handling

Introduction

The effective security of all information NMDDC creates, collects, processes, stores and shares to conduct business and deliver services is a key priority for Council. It is vital for public confidence and the efficient, effective and safe conduct of NMDDC's business. In the normal course of carrying out its duties, Council processes, manages and shares a broad range of information from, but not limited to, the public, businesses and local and central government departments.

Some of NMDDC's services directly involve the creation, collection, management and handling of personal data, sensitive personal data and sensitive commercial data and this information must be managed appropriately and securely.

Data Classifications indicate the sensitivity of data (digital and paper), in terms of the likely impact resulting from compromise, misuse or loss. This scheme sets out the protocol for the appropriate handling of information in accordance with the intrinsic needs and values of Council and relevant compliance requirements.

It is the responsibility of all Council, Elected Members and third parties to safeguard any information or data that they access, irrespective of whether it is protectively marked or not.

This scheme applies to all information assets created or held by Council in whatever format and however it is stored.

Inappropriate disclosure of OFFICIAL and OFFICIAL-SENSITIVE information, its accidental loss or deliberate theft could lead to the Council being levied with a fine in accordance with the terms of the GDPR, as well as experiencing a loss of reputation.

Data Classification

Government Security Classifications introduced in 2014 provide for a baseline set of controls that offer an appropriate level of protection to the data held, Official, Secret and Top Secret.

OFFICIAL is the relevant data classification for ALL routine public sector business, operations and services. NMDDC will operate exclusively at this level including the subset categories of **OFFICIAL-SENSITIVE**, **OFFICIAL-SENSITIVE: PERSONAL** and **OFFICIAL-SENSITIVE: COMMERCIAL**.

It is unlikely that NMDDC will work with Secret or Top-Secret information, however in the event that the Secret classification is required this will reflect that the information requires protection in proportion to the classification.

OFFICIAL-SENSITIVE and its PERSONAL and COMMERCIAL descriptors are not separate classifications but rather identify OFFICIAL information that could have damaging consequences to a third party or the Council, if lost or disclosed without consent and needs to be treated with particular care.

These classifications place greater emphasis on individuals taking personal responsibility for data they create and hold.

Protective Marking

Protective marking indicates to others the data classification category and level of protection needed in handling, transferring / sharing and storing information.

Once the data classification has been determined, this is communicated to others by displaying the classification category thus protectively marking the document or file.

There is no requirement to explicitly mark routine information as all unmarked documents will be assumed to be OFFICIAL. All documents created, processed and shared by NMDDC are a Council asset and have value and must be handled in accordance with Council's policies and procedures.

A limited subset of OFFICIAL information could have more damaging consequences if it were accessed by individuals by accident or on purpose, lost, stolen or published in the media. This subset of information should still be managed within the OFFICIAL classification tier but should have additional measures applied in the form of OFFICIAL-SENSITIVE.

This marking is necessary for person-identifiable information and commercially sensitive information and is applicable to paper and electronic documents/records.

In addition to the marking of OFFICIAL-SENSITIVE, further detail is required regarding the content of the document or record as follows:

OFFICIAL–SENSITIVE: COMMERCIAL
Commercial information, including that subject to statutory or regulatory obligations, which may be harmful to NMDDC or a commercial partner if improperly accessed.

OFFICIAL–SENSITIVE: PERSONAL
Personal information relating to an identifiable individual where inappropriate access could have damaging consequences.

In certain circumstances OFFICIAL–SENSITIVE information may contain both Personal and Commercial data, in such cases use of OFFICIAL-SENSITIVE will suffice.

Documents/records should be marked OFFICIAL, OFFICIAL-SENSITIVE, OFFICIAL- SENSITIVE: COMMERICAL or OFFICIAL-SENSITIVE: PERSONAL and should be marked in uppercase as follows:

MS Office	the heading of each page
Hard Copy Files and Folders	on the spine or front cover of the folder
Emails	in the subject heading
Databases	where possible, protectively mark information produced or created from bespoke and in-house databases

All Council staff, Elected Members and third parties have a responsibility for protectively marking documents and files to ensure the safeguarding of information assets owned by Council.

Data Classification Table

Classification Category	Impact if the information is lost or disclosed to unauthorised people:	Examples to consider:
OFFICIAL	Almost all the routine information processed on a daily basis related to Council business will be OFFICIAL information. OFFICIAL information includes: • personal data that is already in the public domain which, if disclosed without consent, would not cause harm or distress to any individual and staff's personal data relating to their role in Council, e.g. name and job title; • commercial, contractual information and intellectual property; and • public safety, criminal justice and law enforcement.	routine reports; published annual reports; out-turn data for key performance indicators; information that is freely available, e.g. planning applications or information on the website; commercial/contractual information already in the public domain; information the Council is required by law or regulation to publish; names and job titles of Heads of Service and above; and information that is neither commercially nor personally sensitive.
OFFICIAL-SENSITIVE	This is information that could have damaging consequences if lost or disclosed and needs to be treated with particular care. OFFICIAL-SENSITIVE data can: • cause harm or distress to individuals; • cause financial loss or loss of earning potential, or facilitate improper gain; • lead to unfair advantage for individuals or companies; • breach statutory restrictions on the disclosure of information; • would lead to a breach of confidence to third parties (where information is not in the public domain); • disadvantage the Council in commercial or policy negotiations with others; • cause substantial harm or distress to individuals or groups; • prejudice the investigation, or facilitate the commission, of crime; and • impede the effective development or operation of Council policies or services.	customer or staff information for which we have a duty of care, e.g. names, addresses, bank account or credit card details, salary and medical records; combinations of data, some or all of which may be in the public domain, but when put together could cause harm or embarrassment to the staff, customers or business partners concerned; IT authentication details; financial or contractual information relating to procurement / tender process; the information is (or may become) the subject of, or concerned in, a legal action or investigation; exempt committee papers e.g. "in closed session"; information relating to internal or criminal investigations/complaints/appeals; supplier information provided in confidence; and commercial / sensitive information due, but not yet finalised e.g. "draft", for publication.

Information Handling

Everyone has a responsibility to handle OFFICIAL information with care by:

- applying a clear desk policy;
- information sharing with the right people both internally and externally;
- locking PC screens when not in use;
- taking extra care when sharing information with external partners;
- only print where absolutely necessary;
- only use recognised couriers if sending hard copy and tamper proof envelopes;
- ensuring the security of files when transferring between sites; and
- using discretion when discussing information both in and out of the office.

All OFFICIAL-SENSITIVE material including documents, media and other material should be physically secured to prevent unauthorised access. As a minimum, when not in use, OFFICIAL-SENSITIVE: COMMERCIAL and OFFICIAL-SENSITIVE: PERSONAL material should be stored securely in a secure encrypted device such as a secure departmental drive; encrypted pen drive or USB stick; password protected disk; lockable filing unit; drawer or room.

OFFICIAL-SENSITIVE data must be managed as follows:

- it should only be shared with those who have a legitimate need to access it;
- it should be locked away in a lockable cabinet, drawer or room when not in use;
- it should be saved securely in the correct drive;
- it should not be saved in a personal drive; and
- if lost or stolen it must be reported to the Head of Service and Compliance department immediately.

Information Handling Procedures

Type of Information	OFFICIAL	OFFICIAL-SENSITIVE
Paper Records	Secured in lockable cabinets, drawers, rooms when office is unattended. If off-site working, files, diaries, etc. are not to be left unattended or in a car. When posting, ensure correspondence is correctly addressed and mark Private & Confidential. Apply a clear desk policy and follow the guidelines above.	Secured in lockable cabinets, drawers, rooms when not in use. Follow guidelines re clear desk above and not to be left out when away from desk. Use tracked mail only when posting, N.B. recorded email is not tracked until the information has been received by the recipient. It is recommended to 'double envelope'. Create a label advising: *"This letter is intended for [insert data subjects name]. If you have received this letter in error, please do not open and return to the Data Protection Officer in NMDDC"*. Place the Official-Sensitive contents into the envelope and seal with the label. Place all into a second sealed and properly addressed envelope.

Type of Information	OFFICIAL	OFFICIAL-SENSITIVE
Q Drive	It is a requirement to use the shared departmental Q Drive for Council business. Non-Council work is not to be saved on the Q Drive. If required, request a restricted folder for the shared drive from the IT Service Desk to store sensitive documents or password protect documents as appropriate.	
P Drive	The P Drive is for personal work-related files only. See guidance below. Personal media is NOT to be stored on the P Drive.	
R Drive	The R Drive is a repository for information accessible to all Council staff, e.g. policies and procedures, forms, etc. The R Drive can also be used to share essential information between departments. This must be approved by the IAO and time limited to ensure good records management. Contact the IT Helpdesk to set up a folder if required.	Secure folders for sharing sensitive information between departments can be set up on the R Drive. This must be approved by the relevant IAO and time limited. Contact the IT Service Desk to set up a secure folder if required. See also R Drive guidance below.
L Drive and S Drive	Respectively, Libraries and Projects, these Drives are repositories for specific folders created with authorisation by Heads of Service and IT and are not for general use. Authorised users must adhere to the guidelines set out within this procedure.	
W Drive and Z Drive	The W and Z Drives are **not** to be used for creating or storing new documents of ANY nature. The information contained within these drives is for reference only and essential information should be transferred to the Q Drive only after prior notification to the IT Department. The remainder should be disposed of in accordance with Council's R&DS.	
OFFICE 365	Data may be stored on Office 365, however all staff and Elected Members using Office 365 have a responsibility to ensure the information stored is secure and to take extra care when sharing data internally and externally. Office 365 comprises numerous tools including OneDrive, MS Teams, Sharepoint.	
Email – between @nmandd.org accounts	Check email trail to ensure your recipient is authorised to access the information.	Use the Outlook Permission Settings (see below) and mark OFFICIAL-SENSITIVE: COMMERCIAL or OFFICIAL-SENSITIVE: PERSONAL in the Subject field.

Type of Information	OFFICIAL	OFFICIAL-SENSITIVE
	Verify recipient's address before you click send. Avoid putting a data subject's name in the Subject field where possible. Auto-forwarding to personal email accounts is not permitted.	Check email trail to ensure your recipient is authorised to access the information. Verify recipient's address before you click send. Password protect email attachments. Avoid putting a data subject's name in the Subject field where possible. Auto-forwarding to personal email accounts is not permitted.
Email – From @nmandd.org to external accounts	As above and: Redact information from email messages and attachments if not relevant to all recipients.	As above and: Check with the Data Protection Officer whether there is a data sharing agreement in place to understand any security controls for sharing personal data. Redact information from email messages and attachments if not relevant to all recipients.
Email – between two external email accounts for work purposes	Not permitted.	
Council Mobile Devices – e.g. laptops, tablets, smartphones, USB, CDs,	Information must be password protected. Where access to the shared drive is not possible save temporarily to the desktop and transfer immediately to the shared drive when access becomes available. The desktop copy must be deleted immediately. Council devices are for work use only.	

Information Rights Management for Email

Information Rights Management (IRM) allows users to specify access permissions to email messages which helps prevent official sensitive information from being read, printed, forwarded or copied by unauthorised people. Once permission for a message is restricted using IRM, the access and usage restrictions ae enforced regardless of where the message goes.

Council's default setting for email messages is Unrestricted Access. To set permissions to restrict access go to New Email and click Options. On the Options toolbar click Permission and choose the option relevant to the content and nature of your email. The recipient will see a no-entry sign and the restriction status in the information bar of their inbox and the message will read as follows:

- Do Not Forward – Recipients can read this message, but cannot forward, print or copy content. The conversation owner has full permission to their message and all replies.
- Confidential \ All employees – Confidential data that requires protection, which allows all employees full permissions. Data owners can track and revoke content.
- Highly Confidential \ All employees – Highly confidential data that allows all employees view, edit and reply permissions to this content. Data owners can track and revoke content.

The majority of MS Word, Excel and PowerPoint documents that are attached to a rights-managed message will be automatically restricted also. Note that PDF attachments are not automatically restricted.

In addition, users can add delivery and expiry dates to a message to prevent the content being delivered before a certain date/time and also from being seen after a period of time. To set delivery and expiry dates go to New Email and click Options. On the Options toolbar go to Delivery Options and click More Options then tick 'Do not deliver before' and/or 'Expires after' and set the appropriate date and time.

To ensure that all OFFICIAL-SENSITIVE data is secure when emailed, all Council staff and Elected Members must follow the above instructions to apply the appropriate access.

Appendices

Appendix A – Corporate File Plan

A file plan provides a framework for a consistent approach to classifying records across an organisation regardless of format or physical location. Well-structured corporate and departmental file plans allow for efficient retention and disposal of records.

NMDDC uses a number of differently named network drives to allow staff to fulfil their duties. Not all drives are accessible to all staff and the main drives in use are outlined below.

Q Drive

NMDDC currently uses a shared drive system for creating and storing electronic documents and records. Most business areas have a folder on the departmental Q Drive which is accessible to all members of the team. **ALL** departmental work **MUST** be created and stored on the Q Drive. It is not permitted to create new folders in any other network drive with the exception of the R Drive where it is permitted for specific time-limited reasons and in accordance with the process set out below.

All departments should create sub-folders in accordance with the Creating and managing folders guidance.

In addition, third party business information systems create references for certain departmental records, e.g. within Building Control, the Te-Build database automatically creates a reference for each new application submitted to Council regardless of location and the same reference is used for both database and paper files. Should there be a requirement to open a sub-folder on the Q Drive relating to this file the same reference is used for efficiency and to facilitate compliance with the GDPR, DPA, EIR and FOIA.

R Drive

The R Drive has two purposes, it is used primarily for Council business related information that is relevant to all staff, e.g. Policies and Procedures and secondly to allow designated staff across different departments to **securely** access a folder with information that is required by both teams, e.g. an ERT Officer providing data in response to a Freedom of Information request from the Compliance team.

When adding a new/revised policy, procedure or form you must save it as a PDF so it cannot be amended and, if you are sharing a template to the R Drive it must be saved as a PDF or Word Template to prevent users inadvertently saving their own information to the R Drive.

In order to create a **secure** folder on the R Drive, a Line Manager or Head of Service must send a service request via Hornbill to the IT Department, identifying the need for a folder, the folder name, who is to have access and what access is required to that folder. Once the shared and time-limited project or piece of work has been completed then the data must be transferred to the correct departmental folder and maintained in accordance with Council's R&DS.

Sharing a folder securely in this manner minimises the risk of data being accessed accidentally or deliberately by unauthorised users and also ensures that all involved are working on the correct version of a document.

The R Drive is NOT a repository for documents and folders that do not fit in with the existing departmental file plan or for sharing with other staff. **All staff** are not authorised to access/read R

Drive folder content unless they are provided authorisation by the IAO of said content, as described above. Security queries should be directed to Councils Data Protection Officer.

The Records Manager will conduct quarterly screening checks of **top-level R Drive folder names** and liaise with IAOs on ambiguities with their departmental file plan.

P Drive

The P Drive is for creating and storing work related personal files such as learning and development application forms, HR and Payroll queries. The P Drive may be used for creating first drafts of documents that require design or layout work before saving in the departmental Q Drive. No records may be stored on the P Drive as this prohibits sharing of work and retrieval of records in the event of a staff member's absence.

L & S Drives

Respectively, Libraries and Projects, these Drives are repositories for specific folders created with authorisation by Heads of Service and IT.

The L Drive holds libraries of documents or images used by Council departments and have restricted access for designated users only.

The S Drive is for major Council projects that require input from a number of departments and allows designated staff to share information and manage version control. A Head of Service must submit a Hornbill request to the IT Department advising the nature and size of the project and providing the name of the lead folder.

W & Z Drives

The W & Z Drives are the legacy Down District Council and Newry and Mourne District Council Drives and must NOT be used to create, update or store files. These Drives will be phased out in accordance with the IT transformation strategy.

Refer to Data Cleanse Guidance for Electronic Files for information on managing data in legacy drives.

Office 365

Elected Members use Office 365 for all Council related business and have no access to any other Network Drives. Office 365 is used to create and store records and may also be used for sharing documents with agreed and approved internal third parties only.

Office 365 comprises numerous tools including OneDrive, MS Teams, Sharepoint.

Paper Files

Corporate file references have been created to manage paper records and these must be used when creating new files. The root of the reference may not be amended but is added to in order to identify the specific work area. The date of creation is essential to ensure compliance with the R&DS. As with automated departmental file references being replicated across all formats, these corporate file references must be replicated on the departmental Q Drive when creating electronic folders to store records relating to that specific work area.

The main purpose of the file plan for both electronic and paper files is to ensure that records are created and stored in the same way across Council, the subject is easily recognised and understood, they are accessible to the appropriate staff and can be easily retrieved for both use and disposal.

Where possible and practicable, creating and maintaining electronic rather than paper files in accordance with this procedure, will be more efficient and effective in managing Council business.

Information Audit

A Council wide information audit is ongoing to review compliance with the UK GDPR and to record processing activities across all departments. The audit results will inform change and provide the basis for implementation of new records management and filing systems plans and procedures.

Regular departmental information audits will be carried out to ensure Council maintains a robust records management system.

IAOs must advise the Records Management Team of any new/updated information assets added to their file plan and ensure that the asset information held is accurate, up to date and noted for future R&DS preparation.

Functional Business Classification Scheme

NMDDC has commenced work on a functional business classification scheme (FBCS) with the revised R&DS currently awaiting approval by the Minister for Department for Communities and the NI Assembly. The FBCS will be an integral feature of any future Council corporate file plan. The existing bespoke business information systems, paper records and shared drives have no single unified system as the basis for classifying, storing, accessing, and disposing of information. The introduction of a classification scheme and file plan that will be used across all departments will provide a common and consistent framework for handling information. The FBCS will support all areas of Council's business, including programme and project-based working and the effective retention and disposal of Council records. The information audit will provide a functional analysis of Council on which to base the framework with the following purpose and benefits:

- to create a clear classification that represents the business purpose and functions of the organisation;
- to provide clear links between records that are generated from the same functions and activities;
- to deliver systematic and economical storage of records determining where records should be placed and creating order and unity across Council;
- to prevent needless duplication of records and information;
- to assist users in readily finding records and information;
- to ensure compliance with the R&DS; and
- to ensure access rights are clear and information security maintained.

A FBCS is be organised into a three-level classification as follows:

- Function - used as a top-level term to represent the major responsibilities that are managed by Council to fulfil its goals.

- Activity - used to describe the major tasks performed by Council to accomplish each of its functions. Several activities may be associated with each function.

- Process/Transaction - used to describe the tasks, which take place on a regular basis to perform each activity.

Two further levels will hold specific transactional folders and files/records respectively.

Defining the FBCS and corporate file plan is an ongoing part of the Electronic Data Records Management System work. It will enhance NMDDC's capacity to share, communicate and use information more effectively and efficiently. Adherence to the records management procedures

presented above will ensure that all staff, Elected Members and relevant third parties are prepared for change.

NMDDC is currently restructuring and so the corporate file plan shown below reflects the main business activities only as, whilst there are changes to directorate names and reporting lines, the delivery of Council services remains as do the basic activities and transactions that are used to administer these.

This file plan was created for use in conjunction with the electronic shared drive filing system and paper filing. As discussed above, the references provided are predominantly for use in paper filing but also form the basis of any linked electronic files.

Active paper files, both legacy and newly created, are stored in the central filing and departmental filing rooms. Please note that it is essential to close paper files in accordance with the procedure above and ensure that they are not held beyond the retention date.

Business Activity	**File Plan Reference**
Chief Executive's Office	CEO
Administration	CEO/AD
Senior Management Team	CEO/SMT
Local Government Chief Executive's Group	CEO/LGCEG
Elected Members Support	DS/MS
Elections	DS/EL
Council Constitution	DS/CC
Performance	CPL
Community Planning	CPL/CP
Local Development Programme	CPL/LDP
Strategic Programmes	CPL/SP
Transformation, Innovation & Performance	TIP/TIP
Enterprise, Employment & Regeneration	EER/
Regeneration & Business Development	EER/RBD
Programmes	EER/
Tourism Product Development	TCE/PD
Culture, Arts & Heritage	TCE/CA
Events	TCE/EV
Museums	TCE/MU
Development Management	PL/DM
Planning Enforcement	PL/ENF
Local Development Plan	PL/DP
Building Regulations	BCR/BR
Licensing	BCR/LIC
Postal Numbering	BCR/PN

Business Activity	File Plan Reference
Enforcement	BCR/ENF
Health & Wellbeing	HW/
Environmental Health	HW/EH
Sustainability	HW/SUS
Indoor Leisure	LS/LR
Parks & Open Spaces	LS/POS
Sports Development	LS/SD
Engagement	CEN/CE
Community Services, Facilities & Events	CEN/CS
Waste Processing & Enforcement	WM/WM
Refuse & Cleansing	WM/WD
Fleet Management	WM/FM
Facilities Management	FMM/FAC
Cemeteries	FMM/CEM
Council Markets	FMM/MKT
Grounds Maintenance	FMM/GM
Buildings Maintenance	FMM/BM
General Administration	AD/GA
Compliance	AD/FOI/EIR/SAR
Legal Administration	AD/LEG
Customer Services	AD/CS
General HR	HR/GEN
Recruitment & Selection	HR/SA
Learning & Development	HR/TR
Safeguarding	HR/SF
Finance	FIN/
Financial Management	FIN/FMA
Audit & Risk Governance	FIN/ARG
Pay & Pensions	FIN/SA
Procurement	FIN/PPS
Information Technology	IT/
Systems & Infrastructure	IT/
ICT Support	IT/
Security	IT/
Corporate Policy	CPP/PO
Corporate Plan	CPP/CPL

Business Activity	File Plan Reference
Equality, Disability & Irish Language	CPP/EDIL
Projects	CPP/PROJ
Marketing	CPP/MK
Internal Communications	CPP/IC
PR & Media	CPP/PRM
Capital Projects	EPM/CPP
Property Asset Management	EPM/PM
Corporate Health & Safety & Emergency Planning	EPM/CHS

Appendix B – Glossary of Terms

Active Record

Active records are those records which are frequently used for current business and therefore should be maintained in their place of origin.

Archived Records

Archived records are records which have been created or received by NMDDC in the course of its activities and functions and selected for permanent preservation for their historical or evidential value by PRONI.

In addition, closed electronic records are saved in archive folders until such time as they are reviewed for either permanent retention or disposal.

Closed Records

Records are closed when the current business activity has ended. Closure begins the mandatory retention period for the records. Retention schedules require records to be closed either:

- at the end of a defined time period (e.g., the end of the fiscal or calendar year), or
- when a certain event relating to the record has occurred (e.g., the denial of a permit or receipt of final payment).

No new documents or records may be added to a closed file, but they must be kept accessible for the duration of its retention period in the event it is required in accordance with Council's Access to Information Policy and Procedure and for formal review prior to destruction or permanent preservation in accordance with Council's Retention and Disposal Schedule.

Data Protection Impact Assessment (DPIA)

A DPIA is a process designed to systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of NMDDC's accountability obligations under the GDPR, will help assess and demonstrate how compliance with all Council's data protection obligations. It is an essential requirement at the outset of a new project or implementation of a new or revised data processing system to identify if a DPIA is required and to set up records management procedures in line with the requirements defined by the DPIA.

Data Minimisation

Processing of personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum.

Information Asset

An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles. An example of an information asset is all the files associated with a specific project. This might include spreadsheets, documents, images, emails to and from project staff and any other form of records. All individual items can be gathered together and treated the same as they have similar definable content, and the same value, business risk and lifecycle.

Information Asset Owner

Information asset owners (IAOs) are senior staff involved in running the relevant department(s). 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 and ensure that information is fully used within the law for the public good and provide input on the security and use of their asset.

Inactive Records

Inactive records are related to closed, completed or concluded activities but must be retained for administrative, historical and/or legal purposes. As inactive records are no longer routinely referenced, they are generally stored in a secure filing room or archive storage centre remaining accessible for purposes of business processing only with restrictions on alteration.

Metadata

Metadata, usually defined as 'data about data', is information that describes characteristics of a document or record to aid in the identification, discovery, assessment and management of documents and records. Metadata can include a record's date, location, or creator; the device on which a record was created; the duration of phone calls or web browsing; and much more.

Metadata allows users to manage and work with records and facilitates accessibility, and identification of resources.

Non-Records

Any document, device or item, regardless of physical form or characteristic, created or received, that does not serve to document NMDDC's functions, policies, decisions, procedures, operations or other activities. Non-records may include duplicates of official records, reference documents, documents relating to an individual's own, personal affairs.

Preservation

Processes and operations used in ensuring the technical and intellectual survival of authentic records over time.

Privacy Notices

The GDPR requires that data controllers provide certain information to people whose information (personal data) they hold and use. A privacy notice is one way of providing this information. A privacy notice should identify who the data controller is, with contact details for its Data Protection Officer. It should also explain the purposes for which personal data are collected and used, how the data are used and disclosed, how long it is kept, and the controller's legal basis for processing.

NMDDC publishes privacy notices that apply to the collection, sharing and retention of data. Records must be retained in accordance with the relevant privacy notice in addition to this procedure and Council's Retention and Disposal Schedule. Personal data can only be lawfully utilised by Council for the purposes set out to the data subject in the privacy notice.

Publication Scheme

Under the Freedom of Information Act 2000, every public authority must publish and maintain a Publication Scheme which sets out the information they routinely make available to the public.

The scheme includes seven broad classes of information that cover:

- who Council is and its constitutional and legal governance;
- financial information;
- strategy and performance information;
- decision making;
- policies and procedures;
- lists and registers; and
- the services Council offers.

Council staff, Elected Members and third parties must be aware of what is freely available to members of the public through the Publication Scheme and advise the Records Manager if information requires updated, replaced or altered.

Records

Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business. Records include, but are not limited to, paper files, emails, CCTV recordings, electronic files, databases and photographs.

Records Management

The efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.

Records Management Manual

A records management manual is a document that details how records are created, maintained and disposed of within a department, service area, project or working group.

Retention and Disposal Schedule

The purpose of a Retention and Disposal Schedule is to ensure that records are retained only for as long as required by statute or for as long as they are needed for business purposes and, when no longer required, disposed of in a documented, timely and appropriate manner.

Vital Records

Vital records are classified as being essential to the continuation of Council business in the event of a major event, e.g. a disaster. Vital records include those records which are required to recreate Council's legal and financial status, to preserve its rights, and to ensure that it can continue to fulfil its obligations to its stakeholders in the event of a disaster. Vital records may be in any format such as paper, electronic, etc. and examples are records which give evidence of the legal status of NMDDC and its holdings, minutes and papers of committee meetings particularly where major policy decisions are taken, current accounts payable and receivable, contingency plans, key staff contact details, staff records, and next of kin details, etc.

Appendix C – Certificate of File Closure

Certificate of File Closure - to be completed by the Information Asset Owner

File Reference:	
Title of File:	
Department:	
Brief Description of Information held on File / Records:	
Date range of Information held on File:	
Date on which File was closed:	
Reason for File Closure:	
Review/Disposal Date:	
Recommendation of Retention & Disposal Schedule in relation to this Category of Records:	
Related Files (including electronic) and Any Other Information:	

I confirm that I am the Information Asset Owner responsible for the records described above. Having reviewed the records in question I am satisfied that the file(s) should now be closed.

I confirm that the recommendations of the Council's Retention & Disposal Schedule will be adhered to in respect of the above records.

Signed: .....

Print Name: .....

Date: .....

This Form, when completed, should be placed on the front of the File, a file note/diary entry added to the Departmental Records Management folder and a notification sent to the Records Management team.

Appendix D – Archive Box Label Template

Box # of #

Department Name

Review/Dispose [Insert Date]

Contents

File Ref	File / Project Name	Date closed	Disposal Date

Where possible, box together files with the same review and/or disposal date, if you have a mixed box please include the date range at the top of the page and against each file name.

Appendix E – Disposal of Records Form

NOTE: Records must not be destroyed if any litigation, claim, negotiation, audit, Freedom of Information or Data Protection request, administrative review, or other action involving the relevant information is initiated before the expiration of the retention period. They must be retained until completion of the action and the resolution of all issues that arise from it, or until the expiration of the retention period, whichever is later.

Authorisation of this form confirms that all records included are compliant with the above.

Department/Service:	**Name:** **Role:**	**Date:**

File Reference:						
Record Title / Description:						
Record Format:	Electronic / Hard Copy / CD / DVD / Other _____ If Electronic provide file location _____					
Record Dates:						
Classification:						
R&DS recommendation:						
Reason for disposal:						
Method of disposal: Tick as appropriate ✓	Destruction		PRONI		Council Archive	
Method of destruction (if applicable): Tick as appropriate ✓	Confidential Shredding No of Bags:		Digital deletion from Council network, e.g. shared drives, database, etc.		Digital deletion from other location, e.g. cloud service, mobile device, etc.	

The **proposed destruction** / **destruction** has been approved by the Information Asset Owner.

Information Asset Owner Name: _____ Date: _____	Sign or ✓ as appropriate: Signature: _____ Electronic authorisation via email: ✓

NOTE: Form must be sent to recordsmanagement@nmandd.org from IAO mailbox to confirm electronic authorisation.

Once completed, a copy of this form and authorisation must be retained by the relevant Information Asset Owner.

The RM Team will confirm hard copy file destruction by email to be retained with this Disposal form.

For **batch disposals**, please attach the list of records to this form.

Appendix F – File Tracking Schedule

File Tracking Schedule

Department / Team:	
File Reference Number:	
File Name (if applicable):	
File Location (Office):	

Borrower Name	Borrower Ext.	Date Out	Date Due	Date Returned

Appendix G – Records Management Guidance and Best Practice

The Records Management Team have complied the following Schedule, Guidance and Best Practice documents to help embed Council's Records Management Policy and Procedure.

Retention & Disposal Schedule

Guide to Email Records Management

Data Cleanse Guidance for Electronic Files

Electronic Files - Data Cleanse Flowchart

File Tracking Sheet

Confidential Waste Paper Disposal Process and Guidance

Archive Box Label Template