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, General Data Protection Regulations (GDPR) 2018, 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 the 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 sufficient in content, context and structure to reconstruct the relevant activities and transactions that they document.

- **Comprehensive**
  Records must document the complete range of an organisation's business.

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

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

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

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 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.

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.

Related Policies

NMDDC's Retention & Disposal Schedule
NMDDC's Information Security Policy
NMDDC's Access to Information Policy & Procedures
NMDDC's IT Policies & Procedures
NMDDC's Media Policy & Procedures
NMDDC's Privacy Notice
NMDDC's Publication Scheme
NMDDC's Customer Service Standards

Breach of this Policy

Any breach of this Policy and its associated procedure 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.

Policy Owner

Assistant Director Corporate Services (Administration)

Contact Details

Assistant Director Corporate Services (Administration)
Records Manager

CMT Authorised On	30 August 2019 (version 0.1)
SMT Authorised On	05 September 2019 (version 0.2)
Strategic Policy and Resources Committee Authorised On	13 September 2019 (version 0.3)
Council Authorised On	07 October 2019
Policy Effective Date	15 October 2019
Policy Review Date	15 October 2023 *4 years as per equality scheme commitment 4.31, or sooner to ensure it remains reflective of business requirements and legislative developments.*

Procedures

The Records Management Procedures attached hereto 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

Procedure Overview

The purpose of this procedure is to outline the framework for:

1. Compliance (Section 1) with 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, General Data Protection Regulations 2018, 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;
2. Implementation (Section 2) for the above pieces of legislation; and
3. Appendices (Section 3) provide detailed guidance for sections of the procedure.

Aim

The aim of the Newry, Mourne and Down District Council (NMDDC) Records Management Procedure is to ensure 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 achieves this objective.

Scope

The procedure provides clear guidance on the management of NMDDC records in accordance with statutory and regulatory requirements. It applies to all records, regardless of format, created, received, maintained and disposed of by the Council. The procedure applies to all Council staff, including temporary staff, Elected Members, contractors, consultants, volunteers, third parties and contracted out services who have access to, process and manage records in the course of Council business. Non-compliance with the procedure will be dealt with in accordance with the Records Management Policy.

Contents

Section 1: Compliance

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.

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

Non-records have the same physical characteristics as records but as they have no evidential value they can be destroyed after a short retention period. Examples of non-records are drafts, routine e-mail, and duplicate copies of records created for convenience or reference purposes.

NMDDC's 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.

Information is a record if it:

- contributes to a policy or decision-making process;
- contributes to an action or decision made;
- contributes to a change to policy or procedure;
- has financial or legal implications, e.g. contracts, accidents, investigations, etc.;
- supports the running of NMDDC's corporate or departmental business;
- needs to be approved by, or reported to, another individual, an internal or external body, e.g. approved by SMT, Committee, Council, Government Department, etc.;
- sets a precedent or contains something unique or of historic interest; and
- has to be created as a result of specific legislation, e.g. Finance Acts, Employment Acts, etc.

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 this procedure 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.

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 Lord Chancellor's Code of Practice under Section 46 of the Freedom of Information Act (FOIA) 2000 sets out what the Lord Chancellor requires from public authorities as they carry out their duties in relation to the Freedom of Information Act.

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 code is currently under review and the revised edition is due for publication in spring 2020 at which time this procedure will be updated accordingly.

The (FOIA) 2000 and the Environmental Information Regulations (EIR) 2004 give the public the legal right of access to recorded information held by public authorities, unless a relevant exemption applies.

The Data Protection Act (DPA) 2018 and General Data Protection Regulations (GDPR) 2018 give anyone the right to information held about them by a public authority and sets out rules to ensure that information is handled properly, unless a relevant exemption applies. The Re-Use of Public Sector Information Act (RPSI) 2015 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 community planning. Additionally, Council has 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 & Procedures
NMDDC's IT Policies & Procedures
NMDDC's Media Policy & Procedures
NMDDC's Privacy Notice
NMDDC's Publication Scheme
NMDDC's Customer Service Standards

Section2: Implementation

Records Management Procedure

Introduction

The NMDDC Records Management Procedure applies to all corporate and departmental records in all formats (paper and electronic), active and inactive, created, processed, maintained and disposed by NMDDC.

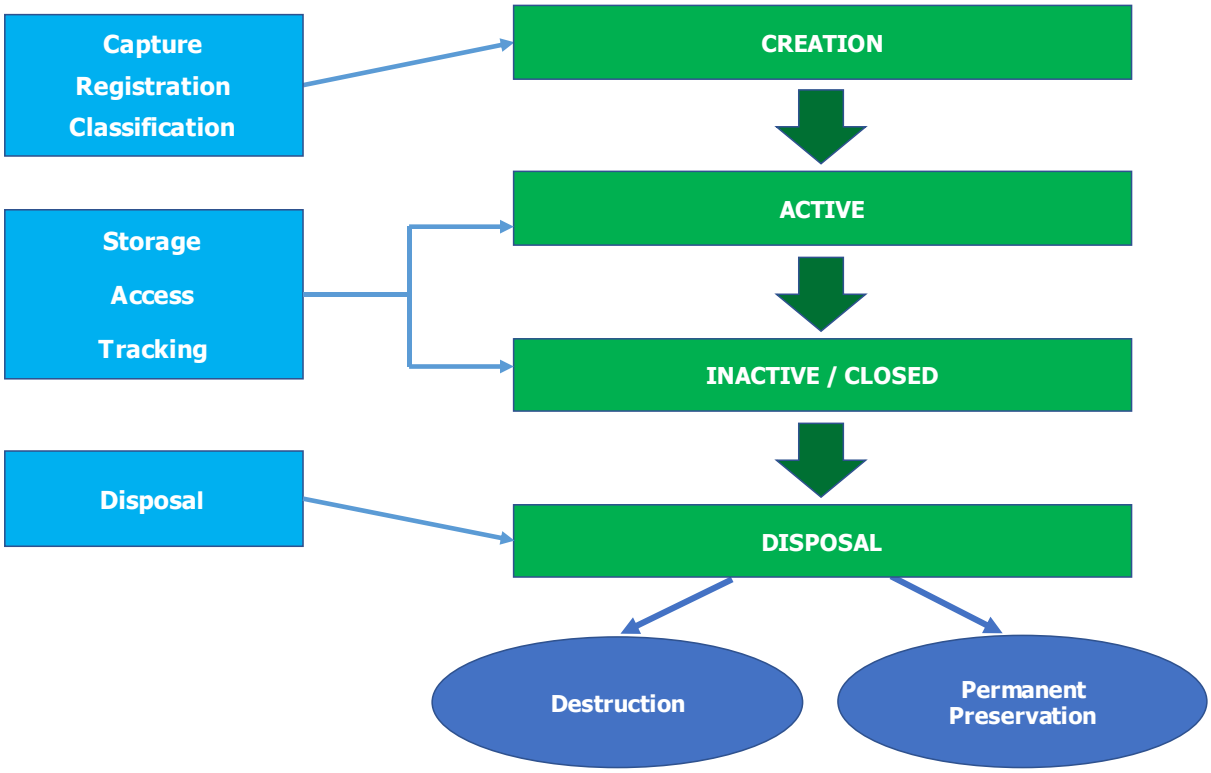
A records management system captures, manages and provides access to records from creation through to disposal.

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.

These are all, by definition, records management systems, however, NMDDC will consider a corporate Electronic Document and Record Management System (EDRMS) that either complements these systems, serves to migrate unstructured data alongside these processes, or, in some cases, will replace these systems.

Record Life Cycle Management

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.



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.

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, 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.

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 Naming & Good Practice

A filing structure reflects the relationship of business activities through careful structuring of folders (with meaningful titles) related to the records. In doing this the structure illustrates the department's business and provides a means of managing its records.

A filing system is the method for storing and organising computer files and the data they contain to make it easy to find and access them.

Naming folders, files, datasets, documents and records consistently, logically and in a predictable way through the application of accurate and descriptive references will distinguish similar records from one another at a glance. This will assist with the storage and retrieval of records enabling users to browse file names more effectively and efficiently. Naming records according to agreed conventions also makes file naming easier for colleagues because they will not have to 're-think' the process each time.

Documents held on shared drives need to be consistently named for prompt and accurate retrieval as they are accessed by other users and may be retained for many years.

Naming conventions will help you:

- create consistent names for electronic documents;
- distinguish documents from one another;
- determine the relevance of documents without having to open them; and
- sort documents logically and group related documents together.

Naming 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.

Keep folder names short and meaningful. Folders should be named according to function or service rather than directorate, department or personal names. They should describe the work that is being done, not who is doing it; e.g. a folder should be called Compliance at the top level, with sub-divisions describing the relevant areas of work such as Requests for Information or Policy as opposed to Compliance Department, Compliance Correspondence, etc.

Folder names should not be repeated in the hierarchy. For example, if the top level is Tourism, the second level should read Strategy, rather than Tourism Strategy. The only exception to this rule is where a proper noun is concerned, e.g. where the second level reads Tourism Strategy Committee (TSC), as that is the name of the committee itself.

When creating new documents, spreadsheets, presentations, etc on the Q Drive they must be saved within a 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.

Naming records
It is important that documents can be sorted by date, number or name and for all titles to be meaningful and relevant.

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.

The following rules should be followed:

- keep file names short, but comprehensible, using uppercase only for the first word or a proper noun;

- avoid acronyms and abbreviations unless regularly in use in the course of the department's business and easily recognisable and understandable during the retention period;

- 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 provide assistance with such files;

- do not 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;

- do not use terms such as 'stuff', 'general' or 'miscellaneous';

- order the elements in a file name in the most appropriate way to retrieve the record, with the most important element first;

- avoid repetition and redundancy;

- documents which will be used and reviewed by groups of people must contain version information - the version number should be indicated in the file name by the inclusion of 'V' followed the version number and, where applicable, 'DRAFT' or 'FINAL';

- 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.

- when using a number in a file name always give it two digits, i.e. 01 – 99;

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

- the file name of an email attachment should include the name of the correspondent, an indication of the subject, the date of the correspondence, 'att' and the number of attachments sent with the covering email;

- date, subject and author should be given if appropriate, e.g. for a letter;

- digital photographs should be saved as '.jpg' files and must not exceed 2Mb in size. Exemptions must be approved by the IT Department;

- when saving items such as digital photographs and scanned images, the title should be changed from the system-generated number to a something meaningful;

- a description of the application, e.g. PowerPoint, Access, should not be included in the document title - this is apparent from the document icon and extension;

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

- 'FW' and 'RE' should be removed from the titles of emails saved to folders.

Departmental naming conventions are to be included in the Departmental Records Management Manuals.

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.

In addition to adding the version number to the end of the file title, it should also be displayed within the document. 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.

Version	Date	Author	Changes
0.1	21/03/2018	J Smith	Initial Draft to Working Group
0.2	02/04/2018	J Smith	Suggested amendments added by track changes
1.0	06/06/2018	J Smith	Final version approved by SMT
1.1	08/09/2018	E Brown	Revision of Section 2.3 to clarify procedure
1.2	03/05/2019	M White	Update to contact details

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 MS Windows.

Record Maintenance

Electronic files must be saved and stored in line with this procedure and updating and cleansing folders must be carried out routinely. Files must be moved to retention folders at the appropriate time and in accordance with the Retention and Disposal Schedule.

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 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 the Access to Information Policy and Procedure for further information on managing the disclosure of Council records and/or contact the Compliance Team.

Record Security

NMDDC is committed to ensuring the confidentiality, integrity and availability of Council's records. Data Classification, Protective Marking and Information Handling, Appendix B, provides detailed guidance on Council's procedures for record security.

Line Managers should ensure that when a member of staff leaves, responsibility for records held on personal drives, emails and other locations not accessible to colleagues is transferred to another member of staff and out of date information deleted.

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 Retention and Disposal Schedule. 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.

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 Retention and Disposal Schedule, saved in the R Drive:\Policies and Procedures folder, provides retention timescales for 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 6 monthly reviews of the contents and, where applicable, implement the disposal of relevant records and folders in accordance with the Retention and Disposal Schedule.

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, each box must be numbered in sequence starting with the oldest files and will need a list of the contents in a table with the following information attached to the top and side of the box:

- Department name;
- File reference;
- File name;
- Date file closed; and
- Proposed disposal date

See Appendix D for a copy of the Certificate of File Closure Form. For further information on closing files and associated forms refer to Council's Retention and Disposal Schedule.

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 by the Head of Service, authorisation by the Director and in accordance with the Retention and Disposal Schedule. All final action decisions must be agreed with the Records Manager and the Assistant Director of Corporate Services, Administration. Destruction will be conducted by passing to a confidential 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 the business processes of units 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 Missing/Lost Record Recovery Plan below.

Should a record be mislaid or lost there are four main elements the Council will focus on:

- Recovery of the record;
- Assessment of the ongoing risk caused by the record being mislaid or lost;
- Notification of the loss and potential breach; and
- Evaluation of Council's response.

Council's Missing/Lost Record Recovery Plan
The missing record should be reported as soon as possible to the departmental manager or Head of Service and the Compliance team notified of a possible breach in the event that the record is not recovered. If the file contains personal data or sensitive personal data, the Data Protection Officer must be notified as soon as possible. If the file contains sensitive commercial data the Chief Executive Officer must be notified immediately.

A thorough search should be carried out immediately with the progress of the search tracked and recorded to ensure no duplication of effort.

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 the Data Protection Officer immediately providing details for the breach report, see the Access to Information Procedure for further information on Council's breach management plan.

When a file containing sensitive commercial data has been recovered, notify the Chief Executive Officer 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 and Chief Executive Officer that the record is permanently missing, that the investigation is to be closed and relevant reports completed. 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 E for a copy of the File Tracking Schedule located at R:\Policies and Procedures\Procedure Forms.

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/Councillors should refer to page 11 of the Access to Information Procedure for further security guidance.

It is the responsibility of the staff member to note on the File Tracker sheet that the file is being removed from the office and ensure that they return it as soon as practicably possible.

The file must not remain out of the office 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.

Email

Emails record actions and decisions and must be managed as effectively as paper and other electronic records. Messages should be arranged in a record-keeping system to allow information to be easily located and retrieved, and regularly reviewed and deleted according to the retention schedule. Save relevant emails into shared mailboxes/folders and regularly delete emails which have only short-term value.

Email is merely a format and messages cannot be treated as a uniform series with a single retention period. Retention should be determined by the subject matter or business purpose, as for any other record.

Staff leaving Council or moving to another department must transfer any business-related emails to either the departmental mailbox/folder or a nominated colleague to ensure that 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 Retention and Disposal Schedule.

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

CCTV
NMDDC operates a number of CCTV Cameras at various Council premises throughout the district and images captured on CCTV footage must be processed as a Council record in accordance with this procedure and the Access to Information Procedure which also provides further information on the purpose, operation and security of Council CCTV.

Social Media
Social media is one of the defining applications for next-generation business environments and every social media related activity represents a potential corporate record. If the information contained in a social media post or blog is unique and not available anywhere else and is a record of Council business, it must be managed in accordance with this procedure for Council to be compliant with statutory and regulatory requirements.

The use, storage and disposal of information collected from social media sites must be included in associated privacy notices to identify how Council manages these records.

Photographic Images
Photographic images form a record of Council's activities and, as photographic images of individuals and small groups can be defined as personal data, the collection, processing, sharing, storage, retention and disposal must be carried out in accordance with this procedure, NMDDC's Media Policy and Procedure, the DPA 2018 and the GDPR 2018.

Photographic images can only be used for the purpose they were originally taken and must be stored in clearly marked folders relating to that purpose. If relying on consent under article 6(1)(a) of the GDPR as the lawful basis for processing the image(s) the consent paperwork must be stored with the images themselves including any consent to share the data with defined third parties.

Mobile Devices
The use of any mobile device to process and access Council information creates risks including those relating to data protection, virus infection, copyright infringement, unintentional or unlawful compromise of data and even loss or theft of device and / or data. Personal data must be processed in accordance with the Records Management Procedure, the GDPR and the DPA regardless of the device used to access the information. Users are required to keep Council information and personal data secure.

NMDDC reserves the right to refuse to allow access to particular devices or software where it considers that there is a security or other risk to its information.

NMDDC is the owner of all Council information which is created on, transmitted to, received on or printed from, stored or recorded on each mobile device, either during the course of Council business or on Council's behalf, irrespective of who owns the mobile device.

Mobile device users are responsible for:
- the security of Council information and of the device on which the information is held, applying additional security measures as required for Official-Sensitive information;
- storing Council information on the Mobile Device only for so long as necessary;
- transferring information only to permitted recipients;
- storing or transferring information only to Council approved cloud computing services;
- deleting Council information from the mobile device when no longer required or sooner if required by Council to delete it; and
- complying with this procedure and related policies;

Mobile devices used to access/store OFFICIAL-SENSITIVE information should be subject to additional protection measures, such as encryption, to reduce opportunities for loss or compromise of the information.

Mobile devices must never be left unsecured. When unattended the device must be locked (password / passcode / PIN protected) and the mobile device should be secured.

In the event of loss or theft of any mobile device the staff member, Elected Member or third party contractor must act promptly to minimise the risk of compromise to Council information by immediately notifying the IT Service Desk and the Data Protection Officer of the incident and reporting theft of a device to the Police and Facilities Management.

NMDDC reserves the right to carry out an investigation into the circumstances of the loss or theft of a mobile device.

Roles and Responsibilities

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

Responsibilities of Council Staff

The Chief Executive and Directors have a general responsibility to ensure that all records management systems and information within their control are managed according to statutory responsibilities and Council policies and procedures.

Assistant Directors and Heads of Department, as 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.

The Records Manager is responsible for developing policies, procedures, guidelines, records classification systems, and retention and disposal schedules and for the provision of staff training in Records Management processes.

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 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:

- ensuring they keep appropriate records of their work in Council and manage those records in keeping with this policy and procedure and with any guidance subsequently produced;
- creating records which are consistent, reliable, accurate and complete;
- identifying records which should be captured for business function or content;
- recognising e-mails which are records and filing accordingly;
- storing records in accordance with this procedure and the departmental process;
- applying data classification and protective marking to records where appropriate;
- handling records containing personal information in line with the GDPR and Data Protection Act;

- ensuring that searching, viewing and browsing records is done only for official Council business purposes;
- creating and managing drafts and finalising documents when appropriate to ensure they become Council records; and
- applying appropriate disposal and retention actions to records based on this procedure and NMDDC's Retention and Disposal Schedule.

Responsibilities of Elected Members

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 Procedure and the Retention and Disposal Schedule and associated legislation. Elected Members are responsible for ensuring:

- they support good records management and comply with the principles of data protection and freedom of information as public representatives;
- records are complete, accurate and meaningful to provide a valid and accurate account;
- records are created and named in accordance with this procedure;
- records of conversations or telephone calls relating to official Council business are written up and saved as a file note in the appropriate folder as soon as practicable after an event, decision, agreement or business activity;
- any correspondence sent or received, and any record created as official records, in any format, are saved in the appropriate electronic or hard copy folder;
- records are provided, when requested by the Democratic Services Manager and Records Manager, for inclusion in the retention and disposal schedule; and
- members must return official records, including emails, to the Democratic Services Manager for the purposes of retention and disposal when their term of office comes to an end.

Elected Members must not use private email systems for official Council business purposes.

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 records 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.

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

Compliance with the policies and procedures laid down in this document will be monitored via the Records Manager together with independent reviews by both Internal and External Audit on a periodic basis.

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

Section 3: 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 departments have a folder on the 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 as outlined in the section on Creating Records above. The structure of each departmental folder will reflect the department's business and provide an environment where a common understanding of how records should be stored and retrieved can be presented.

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. 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 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. Sharing a folder in this manner minimises the risk of data being accessed by a third party and also ensures that all involved are working on the correct version of a document.

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 and who is to have access to that folder. Once the shared project or piece of work has been completed then the data must be transferred to the correct departmental folder and maintained in accordance with NMDDC Retention and Disposal Schedule.

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 without the specific prior approval of senior management. The Records Manager will carry out regular checks of the R Drive to ensure non-compliant folders are removed to the correct location(s).

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 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.

These Drives are not for general use.

W & Z Drives

The W & Z Drives are the legacy Down District Council and Newry and Mourne District Council Drives. These Drives will be phased out in accordance with the IT transformation strategy.

OneDrive

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

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 Retention and Disposal Schedule.

As with automated departmental file references being replicated across all formats, these corporate file references must be replicated on the 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 currently in progress to review compliance with the 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.

Functional Business Classification Scheme

The next stage in the NMDDC records management process will be to create a functional business classification scheme (FBCS). 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 retention and disposal schedule; 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 a future cultural change programme for Council which will be carried out in consultation and participation with staff across all Directorates. 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.

Below is the existing corporate file plan 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.

The file plan is based on the departments and business functions within each Directorate. The electronic shared drive filing system may break down departments into teams/business functions when applicable.

1.0 Chief Executive's Directorate			
Department	**Mapping ID**	**Business Function**	**File Plan Reference**
Chief Executive's Office	1.1		CEO/
	1.1.1	Administration	CEO/AD
	1.1.2	SMT	CEO/SMT
	1.1.3	Local Government Chief Executive's Group	CEO/LGCEG
Democratic Services	1.2		DS/
	1.2.1	Elected Members Support	DS/MS
	1.2.2	Elections	DS/EL
	1.2.3	Council Constitution	DS/CC
Community Planning & Performance	1.3		CPL
	1.3.1	Community Planning	CPL/CP
	1.3.2	Local Development Programme	CPL/LDP
	1.3.3	Strategic Programmes	CPL/SP
	1.3.4	Transformation, Innovation & Performance	TIP/TIP

2.0 Enterprise, Regeneration & Tourism Directorate			
Department	**Mapping ID**	**Business Function**	**File Plan Reference**
Enterprise, Employment & Regeneration	2.1		EER/
	2.1.1	Regeneration & Business Development	EER/RBD
	2.1.2	Programmes	EER/
Tourism, Culture & Events	2.2		TCE/
	2.2.1	Tourism Product Development	TCE/PD
	2.2.2	Culture, Arts & Heritage	TCE/CA
	2.2.3	Events	TCE/EV
	2.2.4	Museums	TCE/MU
Area Planning	2.3		
	2.3.1	Development Management	PL/DM
	2.3.2	Planning Enforcement	PL/ENF
	2.3.3	Local Development Plan	PL/DP
Building Control & Enforcement	2.4		
	2.4.1	Building Regulations	BCR/BR
	2.4.2	Licensing	BCR/LIC
	2.4.3	Postal Numbering	BCR/PN
	2.4.4	Enforcement	BCR/ENF

3.0 Active & Healthy Communities Directorate			
Department	**Mapping ID**	**Business Function**	**File Plan Reference**
Health & Wellbeing	3.1		HW/
	3.1.1	Environmental Health	HW/EH
	3.1.2	Sustainability	HW/SUS
Leisure & Sport	3.2		
	3.2.1	Indoor Leisure	LS/LR
	3.2.2	Parks & Open Spaces	LS/POS
	3.2.3	Sports Development	LS/SD
Community Engagement	3.3		
	3.3.1	Engagement	CEN/CE
	3.3.2	Community Services, Facilities & Events	CEN/CS

4.0 Neighbourhood Services Directorate			
Department	**Mapping ID**	**Business Function**	**File Plan Reference**
Waste Management	4.1		WM/
	4.1.1	Waste Processing & Enforcement	WM/WM
	4.1.2	Refuse & Cleansing	WM/WD
	4.1.3	Fleet Management	WM/FM
Facilities Management & Maintenance	4.2		FMM/
	4.2.1	Facilities Management	FMM/FAC
	4.2.2	Cemeteries	FMM/CEM
	4.2.3	Council Markets	FMM/MKT
	4.2.4	Grounds Maintenance	FMM/GM

5.0 Corporate Services Directorate			
Department	**Mapping ID**	**Business Function**	**File Plan Reference**
Administration	5.1		AD/
	5.1.1	General Administration	AD/GA
	5.1.2	Compliance	AD/FOI /EIR /SAR
	5.1.3	Legal Administration	AD/LEG
	5.1.4	Customer Services	AD/CS
Human Resources & Safeguarding	5.2		HR/
	5.2.1	General HR	HR/GEN
	5.2.2	Recruitment & Selection	HR/SA
	5.2.3	Learning & Development	HR/TR
	5.2.4	Safeguarding	HR/SF
Finance & Systems	5.3		FIN/
	5.3.1	Financial Management	FIN/FMA
	5.3.2	Audit & Risk Governance	FIN/ARG
	5.3.3	Pay & Pensions	FIN/SA
	5.3.4	Procurement	FIN/PPS
Information Technology	5.4		IT/
	5.4.1	Systems & Infrastructure	IT/
	5.4.2	ICT Support	IT/
	5.4.3	Security	IT/
Corporate Planning & Policy	5.5		CPP/
	5.5.1	Corporate Policy	CPP/PO

	5.5.2	Corporate Plan	CPP/CPL
	5.5.3	Equality, Disability & Irish Language	CPP/EDIL
	5.5.4	Projects	CPP/PROJ
	5.5.5	Marketing	CPP/MK
	5.5.6	Internal Communications	CPP/IC
	5.5.7	PR & Media	CPP/PRM
Estates, Capital Projects & Property Assets	5.6		EPM/
	5.6.1	Capital Projects	EPM/CPP
	5.6.2	Property Asset Management	EPM/PM
	5.6.3	Corporate Health & Safety & Emergency Planning	EPM/CHS

Appendix B - 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 COMMERICAL 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: COMMERICIAL and OFFICIAL-SENSITIVE: PERSONAL material should be stored securely in a secure encrypted device such as a secure departmental drive or encrypted pen drive or USB stick, password protected disk, lockable filing unit, drawers 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 secure 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;
- 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 correctly addressed and mark Private & Confidential.	Secured in lockable cabinets, drawers, rooms when not in use. Tidy desk policy and not left out when away from desk. Not permitted to be taken off-site. 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

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.	It is a requirement to use the shared Departmental Q Drive for Council business. If required, request a restricted folder for the shared drive from the IT Service Desk to store sensitive documents. Password protect documents if required for transit only.
P Drive	The P Drive is for personal work-related files only. Personal media is NOT to be stored on the P Drive.	Sensitive personal and/or commercial data is NOT to be created or 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 Head of Service and time limited to ensure good records management. Contact the IT Helpdesk to set up a folder if required.	Sensitive personal and/or commercial data is NOT to be created or stored on the R Drive. Secure folders for sharing sensitive information between departments can be set up on the R Drive. This must be approved by the relevant Heads of Service and time limited. Contact the IT Service Desk to set up a secure folder if required.
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. The remainder should be disposed of in accordance with Council's retention and disposal policy.	
OneDrive	OFFICIAL data may be stored on OneDrive, however all staff and Elected Members using OneDrive have a responsibility to ensure the information stored is secure and to take extra care when sharing data internally and externally.	It is not permitted to store and share OFFICIAL-SENSITIVE data on OneDrive.
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

	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 is not permitted.	the Subject field. 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. Do not send information to internet addresses, e.g. @gmail, @yahoo. Avoid putting a data subject's name in the Subject field where possible. Auto-forwarding to personal email 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 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.	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 must be deleted immediately. Council devices are for work use only.	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 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.

Appendix C - 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 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.

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.

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 D - Certificate of File Closure

Certificate of File Closure - to be completed by the Land Manager for the Service

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:	
Recommendation of Retention & Disposal Schedule in relation to this Category of Records:	
Related Files and Any Other Information:	

I confirm that I am the Line Manager responsible for the records described above. Having reviewed the records in question I am satisfied that the file(s) referred to 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: .....

Position: .....

Dated: .....

A copy of this Form, when completed, should be placed on the front of the File.

Appendix E – 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