

Northern Ireland Community Relations Council

Records Management Policy and Procedures

V4 April 2026

Document Control

The Current status of the document is issued Final.

Version No.	Approval by	Approval date	Issue date	Summary of Updated
1.	CEO	Dec 2023	1st January 2024	
2.	J Irwin & F&GP Committee	19th Nov 2024	19th Nov 2024	- Updated following TEO's information management framework update
3.	F&GP Committee	29th April 2025	29th April 2025	- DFAP Director replaced with appropriate member of staff
4.	F&GP Committee	28th Oct 2026	28th Oct 2026	- Following feedback from PRONI, Retention Schedule Removed from Document - 'Introduction' language updated - Scope and objectives of policy added - Related policies added - Opening paragraph added to roles and responsibilities, along with CEO and Directors responsibilities - Details of CRC's corporate record keeping added - Info Admin Officer job title added - Duplication of roles and responsibilities removed - Retention and disposal summary added

Contents

	Page No
Introduction	4
Scope and Objectives	4
Roles and Responsibilities	5
Corporate Records Keeping	7
Departmental File Plan	8
Naming Conventions and Standards	8
Saving Documents/Creating Records in the Shared Drive	10
Security and Access Controls	12
Retention and Disposal	14
Information Asset Register	14
Contact Details	15
Appendix 1: Definition of Key Terms	16
Appendix 2: Records Retention Schedule Tables	19

1. Introduction

This Records Management Policy details the commitment of the Northern Ireland Community Relations Council (CRC) to achieving the highest possible standards in records management**.**

NICRC handles a large amount of information, This information relates to specific topics and policies as well as records of decisions, action taken and the rational behind these decisions. CRC recognises that its records are a vital asset and are required to ensure the effective operation, openness and accountability of the organisation. Like any asset, records require careful management and this policy sets out CRC's responsibilities and activities in respect of this.

Effective records management goes a long way to ensuring that we have the right information at the right time to make the best informed decision we can. It also provides evidence of what we do and why, therefore protecting the interests of CRC, our staff, our Board and Committees, and all who interact with CRC. We aim to balance our commitment to openness and transparency with our responsibility as an effective information controller and processor.

We continually create records and will work to ensure that we manage them efficiently, make them accessible when requested, and retain them securely with our responsibility as an effective information controller and processor.

By adopting this policy, CRC aims to make sure that the record, whatever form it takes, is accurate, reliable, ordered, complete, useful, and accessible whenever it is needed.

2. Scope and Objectives

This policy applies to the management of all documents and records, in all formats or media, created or received by CRC in the conduct of business activities. It also applies to all staff, Board and Committee members, contractors, consultants, and third parties who may be given access to our documents and records. A systematic approach to the management of the records we hold is essential to protect and preserve the evidence of our actions and decision-making, and the spending of our public money.

In order to achieve this systematic approach, CRC will:

- Create and capture accurate, authentic, and reliable records
- Maintain records to meet CRC's business needs
- Operate a "digital first" policy, maintaining only one corporate copy of a record in one location
- Dispose of records that are no longer required in an appropriate manner
- Protect vital records
- Conform to any legal and statutory requirements relating to record keeping
- Comply with rules on best practice
- Comply with government directives

Relevant Policies and Procedures:
Internal:

- Document Retention & Disposal Schedule
- Freedom of Information Policy
- Publication Scheme
- Data Protection Policy
- Privacy Note
- Information Security Policy

External:

- The Data Protection Act 2018
- The Freedom of Information Act 2000
- Regulation (EU) 2016/679 (General Data Protection Regulation)
- The Environmental Information Regulations 2004
- The Public Records Act (NI) 1923
- Disposal of Documents Order 1925

3. Roles and Responsibilities

CRC has a shared responsibility to maintain its records and record keeping systems in accordance with the regulatory environment as described above. In order to achieve this, certain members of staff have specific roles in relation to records Management.

Each individual who logs onto CRC systems as a User, IT Support User or System Administrator, has a specific user profile and will therefore only be able to carry out pre-designated tasks within the system. An individual's profile will be determined when their account is created and amended as necessary via the System Administrator. The roles can be summarised as follows:

User

Within those areas of the CRC shared drive to which they have access, a User (i.e. the majority of staff) will be able to:

- create, save and edit documents;
- open and read all documents and records;
- search for documents (and save these searches if required);
- finalise documents as a corporate record.

IT Support User

The IT Support User will provide local user support. They will receive additional training to supplement the standard User training whenever necessary and resource permitting. In addition to the functions of the User, and in line with system access controls, a IT Support User will be able to:

- act as first line of support within the local business area and advise on appropriate security and access control measures;
- provide guidance on the use of the shared drive File Plan, for example on where to file documents, emails, etc.;
- provide advice on the creation of folders at a local level in specific areas of the File Plan;

System Administration

System administration is comprised of two elements – ongoing day-to-day administration and information management. Activities associated with the **IT Support User** role would typically include:

- Creation of and maintenance of permissions for folders.
- Password controls and maintenance.
- Active director resetting.
- Email management.
- Update software.
- Printer and photocopier installation and issues.
- Installation of new programmes.
- File Plan management – the creation and maintenance of all levels of the File Plan.
- location management, for example the creation of locations / user accounts, activation of temporary locations.
- in general provide first line support service and escalate to systems administrator where appropriate.
- The shared drive configuration.
- creation and maintenance of record types.

Chief Executive

The Chief Executive/Accounting Officer has overall responsibility for this policy and is the Senior Risk Owner.

Directors/Information Asset Owners

Each business area head has overall responsibility for the management of the records generated by their business area. They are responsible for making sure that a complete record of the business undertaken by their area is captured, and that records management systems (electronic or otherwise) and procedures are used appropriately. CRC's Directors are the Information Asset Owners.

All Staff

It is the responsibility of every member of staff to ensure that the work they carry out on behalf of CRC is correctly saved and maintained within the shared drive. Anyone with responsibility for a particular area of work in which documents and

records are generated has a duty to create, name appropriately and store such information within the shared drive. This includes:

- knowing the documents and records for which you are responsible in relation to your work;
- creating documents and records as required and saving them correctly within the shared drive to the appropriate folder;
- naming (and renaming, where necessary) emails, documents and records properly to ensure that they can be retrieved easily, in line with naming convention guidelines;
- deciding what needs to be filed within the shared drive, including emails;
- managing emails effectively within the shared drive;
- declaring documents as records, i.e. 'finalising' them;
- ensuring records for which they are responsible are maintained and logged onto the Information Asset Register.

4. Corporate Records Keeping Systems

Paper Records

CRC initially maintained a paper-based records system. Certain documents are retained off-site and have been included in file reviews and compliance with the Retention and Disposal Schedule.

CRC now operates a 'paperless' office and all records should be stored electronically in the appropriate system.

Shared Drives

CRC migrated to a paperless, Microsoft 365 document filing system. This has become the corporate repository for the majority of information created and received by CRC in the course of business, including emails that must be retained for business purposes as evidence of a decision of transition. This system holds data that must be managed and considered in line with records management policies and procedures.

Grants Management System

CRC holds a licence for access to external software where grant applications, awards, and monitoring in conducted. This website acts as the file repository for this area of business. This system holds data that must be managed and considered in line with records management policies and procedures.

Websites

CRC maintain a Good Relations Week website and Good Relations Awards website, where nominations and submissions are made. These websites are not considered to be record repositories, and therefore all documents are downloaded and saved on CRC's SharePoint system.

5. Departmental File Plan

Detailed guidance on the development of CRC's File Plan and the File Plan itself can be obtained from the Information Administration Officer.

File Plan Administration / Creating New Folders

- The Data Protection Officer (DPO), usually the Governance, Admin & Assistant Finance Manager and the Information Administration Officer will retain responsibility for the ongoing administration of the departmental File Plan, including the creation of new first level 'Functions',
- Management of the second level 'Sub-functions' and third level 'Activities' folders are the responsibility of the Directors.
- Directorates should monitor, on an ongoing basis, the categorisation of documents and the effective use of naming conventions.
- Managers within each area will be responsible for checking every quarter that the files within their area of responsibility are compliant with the file plan and should report amendment's to the IT Support User who will report to the DPO. Directors may delegate this role to a member of their staff.
- The file path will be reviewed by the Information Administration Officer and DPO each quarter.

6. Naming Conventions and Standards

All saved documents, including emails, are accurately titled. Poorly named documents are not easy to retrieve and can cause confusion. Care should therefore be exercised when naming or titling documents. Names must be concise, meaningful and descriptive of content and / or the purpose of the document.

It is suggested that the **topic – action** is adopted for general use when naming documents, putting the strongest element first, for example –

- T:BUC Event – Attendee List.
- Core Fund Evaluation – Funded Group.
- Audit and Risk Assurance Meeting – April 18 Minutes.
- E-newsletter - Draft to be circulated.

Users may wish to include the year in which the document relates.

The following information is not always required in a name as it is ***no****rmally* automatically associated with the document – author, date created, department.

Practices to Adhere to in Naming Documents

DO:

- name your document so that the name is meaningful to others;
- remove all instances of “FW”, “RE” from email titles; and
- if using a dash “ - “, include a space immediately before and immediately after the dash to enable proper searching within the shared drive.

Practices to Avoid in Naming Documents

DO NOT:

- include the date the document was created as this is automatically captured;
- base names on your creation of the document, for example ‘Jenny’s documents’;
- use words such as ‘Miscellaneous’ or ‘General’, as these encourage poor filing practice;
- compress two or more words into one word, e.g. ‘CorpSer’ or ‘RecordMan’ - always separate words with spaces and type the words in full; and
- automatically accept the title of an email contained within its Subject line as the appropriate name when saving the email in the shared drive. It is likely that you will have to rename emails with a more appropriate and descriptive title.

Examples of Bad Practice	Examples of Good Practice
Untitled	ARAC April 18 Minutes
General docs	Audit Committee – Risk Management Review
Damo’s work	Core Funding Evaluation Report – Dec 2018
Excel spreadsheets	CR/CD Projections 1st Quarter 2008
Mtg mins	Management Committee Minutes – 11.02.18
Recommendations for new services in on Website	Website – new services – recommendations
Presentation on DRRMP	Document Retention Records Management Policy Presentation

Naming Emails

It is highly likely that you will need to rename emails when saving them into the shared drive, as very often the title in an email's subject line does not either (a) correspond with the actual subject of the email, or (b) describe it appropriately. This will be the case, for example, where an email string has been created and the subject matter has changed as the discussion has progressed.

Emails should be named in accordance with the guidance detailed above for naming documents. The name does not need to duplicate information already identified with the email such as sender, date sent, recipient, date received, etc; as these will be automatically generated by the shared drive.

Where attachments are received with an email, the message and attachment should be saved together. The name of the attachment should be left unchanged, regardless of naming conventions, as it will be referenced in the main body of the email message.

Where the email message does not contain relevant information (i.e. where there is no information contained within the actual email message, other than the attachment itself) it may not be necessary to save the email. In such circumstances, only the attachment may need to be saved. It is, however, also important to note that the email itself may be evidence of when and to whom the document was sent. If this is an important consideration, both the email and its attachment(s) should be saved for record purposes.

The Golden Rule is to ask yourself - 'Could an informed third party knowing that subject of a file find that file by following the logic of the file and folder naming
conventions'

7. Saving Documents / Creating Records in the Shared Drive

Maintaining the Community Relations Council Record

It is essential to identify all electronic documents, records and emails which provide evidence of a business transaction / decision or require the maintenance of an audit trail. Such information must be retained and stored directly into the shared drive when created.

Saving documents and records will also help to promote a culture of information sharing. This will make for more effective working due to the ability to access information much more quickly. Information that is not filed within the shared drive cannot be shared or retrieved by other users.

Ensuring Completeness of Record-keeping

CRC must be able to provide a complete and verifiable record of its business activities and therefore needs to be able to demonstrate a complete event or

transaction from inception to completion, and of course all important stages in between. Staff must ensure that complete records are retained in relation to those areas of work for which they have responsibility. The following are only some examples of complete record-keeping -

Example 1 - complete records of a meeting may include the agenda, minutes, any papers tabled at the meeting and circulation lists.

Example 2 - complete records of project work may include authorisation for events or transactions, including emails, minutes and documents requiring signature; records that demonstrate how decisions were arrived at, including reports, minutes and advice; and business cases, progress reports, risk analysis, plans and specifications.

Example 3 - complete records of the development of a report would include the final report, important stages in its drafting, evidence of contributions of those who provided comments, related working papers and evidence that pre-determined targets had been met.

What Not to Save into the shared drive

While it is important to ensure that all important business-related information is stored in the shared drive, there are various instances when information does not need to be retained. Examples include information of a personal (i.e. non- business) nature, if it is of 'information value only' or where it is a duplication of a document / email already held in the shared drive.

Finalising 'Documents' into 'Records'

A document should be finalised as a record within the shared drive records management system when it can be said to be 'completed' and where it provides evidence of a business transaction or activity.

A finalised record is locked and may not be edited once finalised by making the file read only.

Email Management

The '12 Month' Rule

The '12 month rule' has been implemented on the Outlook accounts of all shared drive users. Emails that have not been saved into the shared drive and remain within the Outlook email application will be automatically deleted from inboxes, sent items, associated folders and deleted items 12 months after their receipt / issue.

After one year emails are archived and can be accessed through GFI Mail Archive software.

Which Emails Should be Saved into folders on the shared drive?

All emails which form part of the Community Relations Council record must be saved into the shared drive, preferably as soon as possible after receipt / issue. Emails not relevant to, or required for, business purposes should be deleted. An email is likely to be required for record purposes if it -

- has long term administrative or historical value;
- contains information, advice or explanation not duplicated elsewhere;
- relates to decisions taken and has evidential value; and
- was drafted as a result of policy or legislation.

Who Should Save Emails?

For those emails that are evidence of a decision or a business transaction and therefore need to be retained as part of the 'corporate record', the following guidelines will be appropriate in most cases -

- for '**sent**' emails, whether internal or external, the sender should generally save the email to their appropriate part of the File Plan.
- for external emails received by one person, the recipient should save the email;

8. Security and Access Controls

The Principle of Information Sharing

Good information management practice suggests that as much information as possible held within the shared drive should be made available to colleagues to that require it.

Shared Drive Folder Security

The principal components to the shared drive folder security system is access controls.

Access Controls can be used by System Administrators and IT Support User to restrict the access which all staff, or a select grouping, may have to all of the documents held within an electronic folder or indeed to an individual document.

The default starting position is that documents, including emails, saved to the shared drive are accessible to all Directorate staff. However, it is also recognised that there will be occasions when a clear business need exists to restrict access, plus the type of access, to a specific group of staff or, on occasion, to only one or two individuals. Documents related to various personnel matters (including personal and sensitive

personal data), policy development are all areas where restrictions are likely to be needed.

Access Controls at Shared Drive Folder Level

Access Controls at level two of the shared drive folder level will be determined by the Director Responsible for the level two folder and will be processed by the System Administrator.

A map of the shared drive including access rights will be maintained by the IT Support User and subject to quarterly review by the DPO.

Scanning Documents

Documents which are held in paper copy and which need to be retained for 'official record' purposes should be scanned and appropriately filed within the shared drive. Business areas should encourage the senders of hard copy documents to supply the information in electronic format, where it is practical to do so.

Printing

Whenever appropriate, staff should avoid printing hard-copy versions of emails, electronic documents and records. Printers should be formatted to produce double-sided printing. This should be used whenever viable, ie on the majority of occasions when printing is necessary. Printing multiple pages per sheet should also be considered, where practical, to further reduce paper usage.

Examples of occasions when it is appropriate to print information held within the shared drive include when –

- papers are required for internal or external meetings, for example with external organisations or members of the public;
- the size or nature of the document makes it impractical to view, consider or work on its content on screen; and
- documents need to be distributed to external sources, for example sent in hard copy format to a member of the public.

Personal folders within the shared drive

Each member of staff has been provided with a personal folder within the shared drive which can be used to hold only information of a non-business nature. All work related files should be saved directly to the shared drive, in the appropriate folder. Any personal documents saved in Onedrives should be deleted prior to the staff member leaving the organisation.

Business-related information must not be stored within these folders.

Onedrive accounts are retained for one year after a member of staff has left the organisation.

Registered (Paper) Files

Records to be Retained in Paper Format

These policies and procedures are designed to ensure that, whenever possible, records and documents are retained in an electronic form. However it is recognised that in some instances there will be a need to create manual files (e.g. leg

9. Retention and Disposal

Information and records must be held no longer than required to support CRC's business need and legal obligations. CRC has a detailed Retention and Disposal Schedule, which list record classifications and their retention periods. At the end of that time the record will either be: destroyed: retained permanently by CRC, appraised by PRONI, or shared with PRONI for permanent retention. Full details of the retention and disposal process can be found in the Schedule.

Retention periods have been determined by business need and legislative requirements.

Documents should be 'finalised' into records whenever staff determine no further amendment is likely. Document should be closed and logged as a Record on the Information Asset Register by notifying the Governance Manager.

During Q4 of each financial year the Governance Manager will review the Information Asset Register to consider the action to be taken. A report will be prepared for records that the DPO has recommended to be:

- Destroyed;
- Transferred to PRONI for permanent preservation
- Retain Permanently
- PRONI appraisal

The report will be submitted to CEO who approve the recommendation or provide alternative recommendation to implement.

10. Information Asset Register

An Information Asset Register (IAR) is a log that allows CRC to understand and manage its documents and records assets and their sensitivity either to CRC corporately or persons that interact with CRC. It is important to understand what information CRC holds, where it is located, if personal and even how to exploit that information to aid achievement of CRC objectives.

The IAR will track how long records should be retained, why they are being retained, if the information is within the scope of GDPR, which records should be destroyed and which records should transferred to the Public Records Office NI. It will therefore be an important tool to ensure CRC compliance with GDPR obligations.

The IAR contains the information:

- Function
- Asset Number
- List of box contents attached?
- Owner
- Manager
- Sensitivity (H,M,L)
- Date to be sent to Off Site Archives
- Retention Period in Off Site Archives
- Retention / Disposal Notes
- Usage
- Transfer

The IAR is the responsibility of the Governance Manager, who made delegate operating the IAR to another member of staff. The Information Asset Register will be reviewed by the Governance Manager during the first month of quarter end.

11. Contact Details

For assistance on any records management-related issue, please contact the Governance, Admin Assistant Finance Manager.

Appendix 1: Definition of Key Terms

Access Controls - A feature of CRC's information security system which allows the **Creator** of a document to specify which other persons will have access to that document, plus the nature of the access to be provided.

Author - The person who composes a document. CRC shared drive automatically captures this detail from a user's login details.

Folders - these are opened within the shared drive to hold all the **Documents** and **Records** relating to that subject.

Creator - This is the person who initially creates a document, or saves an email, in the shared drive. If you compose a document and then save it into the shared drive, you will be both the **Author** and Creator.

Disposal - The word disposal, when used by the Public Record Office NI (PRONI), can mean any of the following:

- Destruction of records
- Records to be appraised (if in paper format, to be reviewed)
- Records transferred for permanent preservation at PRONI
- Transfer of the ownership of records
- Damage, alteration or rearrangement of records
- Separation from, or disturbance to, contextual information, software, hardware or other equipment on which records depend.

Disposal Schedules - Disposal schedules determine the retention, destruction or transfer of records after a specified time period and are managed by CRC in conjunction with PRONI.

Document - The term 'document' in the shared drive is used to describe any electronic document created, edited and stored by an User prior to being finalised as a 'record', e.g. emails, Word documents, Excel spreadsheets, PowerPoint presentations, PDFs, TIFs, etc.

File Plan – The File Plan is a structured classification of documents and records which provides a full representation of the business of an organisation. The first three levels of the File Plan are referred to as the **Classification**.

Information Asset Owner - Have an understanding of the records held by their business area and approve decisions to ensure compliance against information assurance requirements within their business area.

Information Asset Register - is a log to help manage CRCs records and the risks to them. It is important to know and fully understand what information CRC holds in order to protect it and be able to exploit its potential in an efficient manner.

Locations - Locations in the shared drive are used to identify the various ownership, use and residence details for records.

Offline Access - When users need to temporarily 'Check Out' documents to enable offline working, for example laptop users who need to work on a document outside the normal office environment. Early drafts may also be saved here.

Personal Folder / Personal Information – Non work-related information of a personal nature such as a letter to a bank manager or note of a dental appointment can be stored within a user's Personal Folder in the shared drive. These Personal Folders, because of the nature of the information they contain, do not form part of the departmental File Plan. Work-related 'personal' information such as training invitations must be stored, however, within the appropriate HR folders within the departmental File Plan. It is also highly likely that **Access Controls** should be placed on such information to restrict access to the appropriate staff.

Record - A record provides evidence of a business transaction or decision. Once a document is finalised and becomes a record, it can only be deleted from the shared drive in accordance with the agreed retention / disposal schedule.

Records Management - Records Management is the field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposal of records. It includes processes for capturing and maintaining evidence of, and information about, business activities and transactions in the form of records.

Record Types - Record Types are templates for the creation of an organisation's records. The Record Type dictates, for example, how records of that particular type will be numbered and titled and how default security will be applied.

Redaction - When dealing with requests for information under either the Freedom of Information Act or the Data Protection Act, it is important to note that in certain cases the exemptions contained within these Acts may apply to the information sought.

In practice, this could mean that portions of the information requested should not be revealed under the terms of the relevant Act and should be redacted (i.e. blanked out), to ensure that the person who requested the information cannot view them. The Information Manager (DIM) will advise on when an exemption may apply. CRC will provide guidance to staff on how redactions can be achieved, cross referenced and retained within the shared drive.

Reference Material - Refers to information created by another department, business area or organisation and kept as a reference source.

Revisions - Any editing of a **Document** will automatically create a new revision of that document. TRIM provides the functionality to view the revision history, i.e. the previous

versions, of documents and records. When necessary, any earlier revisions can be deleted by IT Support Users and also during the Retention and Disposal process.

Secure Remote Access - When departmental networks are accessed from outside of the office, for example via departmental laptops or PCs located in the home.

Security Levels - A component of CRC's information security system that enables **Access Controls** to be established within the folders on the shared drive. These are set and operated by the System Administrators.

Storage Devices - A device capable of storing data, including USB pens and CDs.

Versions - A version is created manually by the user and a new record is generated for the document. Therefore versions are different documents with the same title, etc. whereas **Revisions** are successive alterations to the same document.

Workflow - Automation of business processes, in whole or in part, during which documents, information or tasks are passed from one participant to another for action, according to a set of procedural rules, e.g. CRC FOI Requests.

Appendix 2: Records Retention Tables

1. INTRODUCTION AND BACKGROUND

A Records Retention and Disposal Schedule is essentially a table that describes the length of time each business document or record will be retained and its final disposition (disposal or storage). The basic components consist of:

- a description of each type of record which the organisation generates
- a retention period for each type of record

A Records Retention Schedule is an essential component of an effective records management programme. It sets out an organisation's policy on retention of its business records. This provides a basis for consistent action across the entire organisation and eliminates the need for individual employees to make decisions about the retention of the records which they produce or receive in the course of their work.

AIMS, PURPOSE AND SCOPE OF THE TABLES

The aim of these tables is to set out the retention durations and disposal requirements for different record types with all legitimate and legislative considerations having been taken into account.

Disposal is as important as retention. The retention durations given here are meant to also imply secure disposal of records at the end of the retention period.

The scope of the schedule is the entire Northern Ireland Community Relations Council.

2. DEFINITIONS AND CLARIFICATION

A "record" is 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. These records may be in either electronic or traditional paper format.

A "Records Retention and Disposal Schedule" (RRDS) is a table that describes the length of time each document or record will be retained and its final disposition (disposal or storage).

A "Business Classification Scheme" (BCS) outlines business functions and activities for the purposes of structuring records management, structuring records management by BCS rather than by content or location.

The "Public Records Office for Northern Ireland" (PRONI) is an archival institution that holds both public and private records. It performs the functions of the Public Records Office, Manuscripts Department of a National Library, County Record Office for the six counties of Northern Ireland, and holder of a large range of private records.

3. PROCEDURE

Differentiation is made between paper and electronic records although the retention and disposal requirements by record type are still the same. The method of retention and disposal will be different.

The primary responsibility for

- Identifying record type
- Marking record (visibly or electronically) with type, retention and disposal dates
- Actual retention and disposal lies with the originating Department.