Northern Ireland Community Relations Council

Records Management and Document Retention policy and procedures

May 2018

Document Control

The Current status of the document is issued Final.

Version No.	Approval by	Approval date	Issue date

Contents

Introduction

As part of its commitment to streamlining business processes, implementing best information practices and achieving compliance with important pieces of legislation such as the Data Protection Act, the Freedom of Information Act, and the General Data Protection Regulations (GDPR), the Northern Ireland Community Relations Council (CRC) has revised and updated its Records Management and Document Retention policy and procedures.

CRC recognises that information is a valuable asset used to support the many services offered to both internal and external customers.

The implementation of this policy aimed to establish a single, and wherever possible an electronic, repository to hold all of the corporate information held in email accounts, shared and personal network drives and on hard disks. This will enable CRC to promote a consistent and effective approach to creating, accessing, sharing, protecting and structuring our information. This in turn facilitates the management of such information, including its review and disposal, in an ongoing corporate manner. It also helps CRC to meet its statutory and public record obligations in relation to records management.

Roles and Responsibilities

Roles

1. 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

2. 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

3. 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

4. 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 (ECNI) where appropriate.
- The shared drive configuration.
- creation and maintenance of record types.

Responsibilities of <u>All</u> Staff

5. **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.

6. It is the responsibility of Directors and the CEO to ensure that this guidance is adhered to at a local level and that staff are aware of their individual roles and responsibilities.

Departmental File Plan

Guidance on Development

7. Detailed guidance on the development of CRC's File Plan can be obtained from the IT Support User.

File Plan Administration / Creating New Folders

8. The Data Protection Officer (DPO), usually the Director of Finance, Administration and Personnel, will retain responsibility for the ongoing administration of the departmental File Plan, including the creation of new first level 'Functions',

9. Management of the second level 'Sub-functions' and third level 'Activities' folders are the responsibility of the Directors.

10. Directorates should monitor, on an ongoing basis, the categorisation of documents and the effective use of naming conventions.

11. 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.

12. The file path will be updated by the IT Support User and reviewed by the DPO each quarter.

Naming Conventions and Standards

Naming Documents

13. All of 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.

14. 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.

Elements Not Required in a Document Name

15. The following information is not required in a name as it is ***normally*** 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

16. 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.

17. 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.

18. 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.

19. 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'

Saving Documents / Creating Records in the Shared Drive

Maintaining the Community Relations Council Record

20. **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.**

21. 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

22. 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

23. 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'

24. 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.

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

Email Management

The '12 Month' Rule

26. 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.

27. 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?

28. 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?

36. 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;

Security and Access Controls

The Principle of Information Sharing

37. 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

38. 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.

39. 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

40. 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.

41. 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

42. 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

43. 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.

44. 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

45. 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.

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

Registered (Paper) Files

Records to be Retained in Paper Format

47. 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

Retention and Disposal

Schedule

48. CRC's Retention and Disposal Schedule identifies the arrangements for all records which fall within the responsibility of CRC. .

49. The guidelines stated in the Schedule are applied irrespective of format. The term:

- 'record' applies to both documents held within registered paper files and electronic documents within folders on the shared drive which have been finalised; and
- 'file' applies to registered paper files and electronic folders on the shared drive.

50. There are 4 categories of final action - Destroy, Review and transfer (to PRONI) and Permanent.

Roles and Responsibilities

51. All staff - Responsible for documenting business actions and decisions in records, and maintaining the official record of CRC business in accordance with records management best practice.

52. Data Protection Officer - Provides guidance on the principles of retention and on the preparation of disposal scheduling. The Information Manager is the overall owner of the retention schedule and the Information Asset Register. Coordinates disposal and retention arrangements for CRC including arranging secure disposal of hardcopy registered records and providing advice and guidance to staff.

53. Directors - Ensure compliance with Records Management standards within Directorate and will co-ordinate activities relating to disposal and retention of records within their business area.

Retention

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

55. Documents should be 'finalised' into records whenever staff determine no further amendment is likely. Document should be closed in line paragraph 24 and logged as a Record on the Information Asset Register by notifying XXXX.

56. There are 4 final actions in the schedule – Destroy, transfer to PRONI, permanent retention, or determined on review.

57. During Q4 of each financial year the DPO 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;
- Retained for longer than scheduled; and
- Determined in review.

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

Information Asset Register

58. 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.

59. 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.

60. The IAR provide the following guidance and 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

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

Contact Details

62. For assistance on any records management-related issue, please contact the Director of DFAP.

by emailing gmckeown@nicrc.org.uk

Or by post: Mr Gerard McKeown, Director of Finance Administration and Personnel, Northern Ireland Community Relations Council, 2nd Floor, Equality House, 7-9 Shaftesbury Square, Belfast, BT2 7DP.

Legislation and Standards

There are a number of legislative drivers that necessitate the creation and management of records within all government departments and agencies. The sections below provide details of the legislation that governs records management, as well as the best practice standards which provide the necessary framework for effective and efficient records management. Please refer to the website / reference material listed for more detailed guidance.

Legislation

The Copyrights, Designs and Patents Act 1988
www.cla.co.uk

Public Records Act (Northern Ireland) 1923
www.proni.gov.uk/nirms_-_filing_systems.pdf
www.pro.gov.uk/public_records_act_1923.pdf

Freedom of Information Act 2000
www.dca.gov.uk/rights/dca/foidcaintro.htm

Environmental Information Regulations 2004
www.legislation.gov.uk/uksi/2004/3391/contents/made

Data Protection Act 1998
www.legislation.gov.uk/ukpga/1998/29/contents

GDPR
http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

The Re-use of Public Sector Information Regulations 2005
www.opsi.gov.uk/si/si2005/20051515.htm

Standards

Northern Ireland Records Management Standard
www.proni.gov.uk/nirms_-_filing_systems.pdf

ISO15489 Records Management Standard
www.iso.org/iso/catalogue_detail?csnumber=31908

ISO/IEC 27001 Information Security Standard
www.iso.org/iso/home/standards/management-standards/iso27001.htmBritish Standards Institution BIP 0008 Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically
www.thecabinetoffice.co.uk/page28.html

Guidance on Electronic Records and Metadata

www.nationalarchives.gov.uk/electronicrecords/reqs2002/

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 1: 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.

Grant and funding applications			
Grant application decisions – successful	Retain until completion of grant Then retain for 6 years	Funding and Development Director	N/A
Grant application decisions – unsuccessful	Retain until completion of grant application process including appeal time limits + 1 calendar month Dispose of after this time	Funding and Development Director	N/A
Grant programme information	Retain for the life of the grant programme + 6 years Transfer to PRONI after this time	Funding and Development Director	Website
Policies and procedures for administration of grant	Retain until superseded + 1 year Transfer to PRONI after this time	Funding and Development Director	N/A
Database Administration Documentation	Retain to end of financial year + 1 year Dispose of after this time	Funding and Development Director	N/A
Funding and Development Policies	Retain until superseded + 1 years Dispose of after this time	Funding and Development Director	N/A
CR/CD project files *(including claims)*	Retain until completion of grant Then retain for 6 years	Funding and Development Director	N/A
Pathfinder Project Files *(including claims)*	Retain until completion of grant Then retain for 6 years	Funding and Development Director	N/A

North Belfast Project Files *(including claims)*	Retain until completion of grant Then retain for 6 years	Funding and Development Director	N/A
Project Grants Project files - Media Grants - Publications (including claims)	Retain until completion of grant Then retain for 6 years	Funding and Development Director	N/A

Human Resources Records			
Recruitment Files – Unsuccessful candidates (Which will include a copy of the approval to recruit, the job description and personnel specification, the advertisement, all applications received, shortlisting report and all interview records)	Retain for recruitment period + 1 year Dispose of after this time except for files relating to recruitment of CEO and Chair; retain for 6 years.	DFAP *(HR Manager)*	N/A
Employee Personal File (Which will include all recruitment files information (application form, references), contract, any contractual changes, changes to personal information (name, address, next of kin etc.) and changes to salary point	Retain for duration of employment + 3 years Dispose of after this time	DFAP *(HR Manager)*	N/A
Human Resources Procedure Development (The Procedure and any key records that informed procedural development)	Retain until superseded + 1 year Dispose of after this time	DFAP *(HR Manager)*	N/A
Staff Surveys	Retain until completion of survey + 3 years Dispose of after this time	DFAP *(HR Manager)*	N/A
Trades Unions Records	Retain from derecognition + 3 years Dispose of after this time	DFAP *(HR Manager)*	N/A

Industrial Tribunal Files	Retain for duration of tribunal + 3 years Dispose of after this time	DFAP *(HR Manager)*	N/A
Health and Safety risk assessments	Retain until superseded + 3 years Dispose of after this time	DFAP *(HR Manager)*	N/A
Records documenting the development and evaluation of job specifications	Retain until termination of position; Or until revised. Dispose of after this time	DFAP *(HR Manager)*	N/A
Records documenting references provided in confidence in support of the employee's application(s) for employment by another organisation	Retain from provision of reference + 1 year Dispose of after this time	DFAP *(HR Manager)*	N/A
Promotions/Advancements	Retain until termination of employment + 6 years Dispose of after this time	DFAP	N/A
HR and Personnel Policies	Retain until superseded + 1 years Dispose of after this time	DFAP *(HR Manager)*	N/A
Staff meetings – agendas, minutes	Retain for current financial year + 1 year	DFAP *(Finance Officer)*	N/A

	Dispose of after this time		
Facilities Management Records	Retain for current financial year + 2 years Dispose of after this time		N/A

Equality and Diversity Services Records			
Fair Employment Monitoring Information	Retain current financial year + 6 years Dispose of after this time	DFAP	N/A
Section 75 screening and EQIAs	Retain until strategy or policy superseded + 6 years Dispose of after this time	DFAP	Website
Equality Scheme and Action Plan document	Retain current financial year + 6 years Dispose of after this time	DFAP	Website

Governance records			
Board Papers	Retain permanently. Transfer to PRONI after this time	CEO *(DFAP)*	Website
Audit and Risk Assurance Committee papers	Retain permanently. Transfer to PRONI after this time	CEO *(DFAP)*	Website
Other Board Sub-Committees *(None currently in existence)*	Retain permanently. Transfer to PRONI after this time	CEO *(DFAP)*	Not Publically Available
Annual report and Accounts	Retain permanently. Transfer to PRONI after this time	CEO *(DFAP)*	Website & Legal Deposit Libraries
Management Statement and Financial Memorandum	Retain permanently. Transfer to PRONI after this time	CEO *(DFAP)*	Website
Articles and Memorandum of Association	Retain permanently. Transfer to PRONI after this time	CEO *(DFAP)*	Companies House
CRC Strategic Plan	Retain permanently. Transfer to PRONI after this time	CEO *(DFAP)*	Website when in effect
CRC Business Plan	Retain permanently. Transfer to PRONI after this time	CEO *(DFAP)*	Website when in effect
Other CRC founding papers	Retain permanently. Transfer to PRONI after this time	CEO *(DFAP)*	N/a
CRC Photographs and early media	Retain permanently.	CEO *(DFAP)*	N/a

	Transfer to PRONI after this time		
MoUs and agreements	Retain until termination of contract + 6 years Dispose of after this time	CEO *(DFAP)*	N/a
Licenses and contracts	Retain until termination of contract + 6 years Dispose of after this time	DFAP	N/a
Subject Access Requests	Retain from last action on request + 1 year Dispose of after this time	DFAP	N/a
FOI requests	Retain from last action on request + 6 year Transfer to PRONI after this time	DFAP	N/a
Assembly questions	Retain from last action on request + 6 year Transfer to PRONI after this time	DFAP	N/a
Complaints	Retain from last action on case + 6 years Dispose of after this time	DFAP	N/a
Business Continuity Plan	Retain until superseded + 1 year	DFAP	N/a

	Dispose of after this time		
Information logs, analysis and reports	Retain from the current calendar year + 6 years Dispose of after this time	DFAP	N/a
Information Management Policies	Retain until superseded + 1 years Dispose of after this time	DFAP	N/a
Governance Policies	Retain until superseded + 1 years Dispose of after this time	DFAP	N/a
Departmental returns	Retain from last action on request + 6 year Transfer to PRONI after this time	DFAP	N/a

Finance and Procurement records			
Financial planning and forecasts	Retain for current financial year + 1 year Dispose of after this time	DFAP *(Finance Officer)*	N/A
Management Accounts	Retain for current financial year + 1 year Dispose of after this time	DFAP *(Finance Officer)*	N/A
Accounting Journals	Retain for current financial year + 6 year Dispose of after this time	DFAP *(Finance Officer)*	N/A
Business Cases	Retain from termination of supply contract awarded + 1 years Dispose of after this time	DFAP *(Finance Officer)*	N/A
Sales Ledger records	Retain for current financial year + 6 years Dispose of after this time	DFAP *(Finance Officer)*	N/A
Purchase Ledger records	Retain for current financial year + 6 years Dispose of after this time	DFAP *(Finance Officer)*	N/A
Employee expense records	Retain for current financial year + 6 years Dispose of after this time	DFAP *(Finance Officer)*	N/A
Financial Statement file	Retain for current year + 6 years Dispose of after this time	DFAP *(Finance Officer)*	N/A
Payroll records	Retain for current tax year + 6 years Dispose of after this time	DFAP *(Finance Officer)*	N/A
Core Claims Files	Retain for current tax year + 6 years	DFAP *(Finance Officer)*	N/A

	Dispose of after this time		
Employer pension contribution records	Retain from termination of employment + 6 years Dispose of after this time	DFAP *(Finance Officer)*	N/A
Successful tenders	Retain from termination of contract + 1 years Dispose of after this time	DFAP *(Finance Officer)*	N/A
Unsuccessful tenders	Retain from award of supply contract + 1 year Dispose of after this time	DFAP *(Finance Officer)*	N/A
Purchase orders	Retain for current financial year + 1 years Dispose of after this time	DFAP *(Finance Officer)*	N/A
Contracts and Contract Management Papers	Retain for current financial year + 6 years Dispose of after this time	DFAP *(Finance Officer)*	N/A
CRC Finance or Procurement Policy Documents	Retain until superseded + 1 years Dispose of after this time	DFAP *(Finance Officer)*	N/A

Community Engagement			
Published external focused policy papers	Retain for 6 years plus current business year. Transfer to PRONI after this time	Community Engagement Director	Website
Consultation Reponses	Retain for 6 years plus current business year. Transfer to PRONI after this time	Community Engagement Director	Website

Other external focused policy papers	Retain until policy superseded + 6 years Transfer to PRONI after this time	Community Engagement Director	N/A
Event records	Retain for one calendar year unless event of significance in which case retain permanently and transfer to PRONI at the end of one calendar year	Community Engagement Director	N/A

CRC ARCHIVE

Originating departments should retain all records which they need for their own operational purposes (this defined as being used on a regular basis). Records should only be transferred to the CRC Archive when they cease to be operationally relevant.

Where it has been noted that records should be retained permanently by the CRC Archive, such records may eventually be deposited in the Public Record Office of Northern Ireland (PRONI) in accordance with any future strategy agreed between CRC and PRONI.

In the event of any required change in retention period, e.g. changes in legislation, the CEO will have the discretion to make such a change, consulting as appropriate the Departments concerned.