The Executive Office
www.executiveoffice-ni.gov.uk

The Executive Office

Records Management Policy and Procedures

September 2023 (version 3.0)

Document History

Version	Date	Update position	HoB approval	SIRO approval
1.0	March 2008	Initial roll out of TRIM across OFMDFM		
2.0	July 2010	Post 2-year roll out revisions		
2.1	October 2011	IMCAB Personnel revisions and minor amendments		
2.2	July 2014	• Minor textual amendments. • Updated links for legislation and standards and movement to end of guidance. • Movement of Definition of Key Terms to end of guidance. • Additional key terms Information Asset Owner and IMCAB. • Amendment to key term Offline Access. • New government security classification scheme. • Responsibility for document categorisation and naming conventions • IAO approval required to remove a record • Ministerial Special Advisors do not have TRIM access • Information should only be accessed for business reasons, inappropriate access to be reported to IAO • Restricted TRIM areas may be widened when staff leave post • retention and disposal process		

		• workflow process for FOI requests • revision of personnel		
2.3	June 2015	Added contact to Contact Details		
2.4	09 May 2016	9 May 2016 Document updated to reflect the establishment of the new Executive Office.		
2.5	07 March 2019	Document updated to ensure all policies and procedures are up to date		
2.6	29 January 2021	Document updated to include new columns in the Document Control (History) section to record Head of Branch (HoB) and Senior Information Risk Owner (SIRO) approvals and associated dates. This change was recommended by the Information Commissioner's Office in its Audit Report of December 2020, and accepted by TEO Management.	DL 04/02/21	NJ 04/02/21
2.7	04 February 2021	Formal approval of the Records Management policy document as it stands.	DL 04/02/21	NJ 04/02/21
2.8	21 April 2021	Document updated to take account of new HoB, upgrade to CM and ICO FOI Audit recommendations	MC 21/04/21	NJ 21/04/21
2.9	06 October 2021	Change of ITSO	MC 06/10/21	N/A
3.0	01 September 2023	Change of Departmental Information Manager. Update to the introduction. Inserted review period information in the document history as per NICS version control guidance. New sections on IMCAB, the CM reference library and the senior manager section. Updated section on naming conventions. Removed paragraphs lifted directly from Retention and Disposal Schedule. Replaced with link to the retention and disposal schedule.	DM 01/09/23	NL 01/09/23

Review Period

The current version of this document will be reviewed by Name Redacted on 31/12/2023.

Table of Contents

Introduction 1
Roles and Responsibilities 2
Roles 2
End User 2
Power User 2
System Administration 3
Information Management and Central Advisory Branch 4
Responsibilities of All Staff 4
Departmental File Plan 6
Guidance on Development 6
File Plan Administration - Creating New Containers 6
File Plan Administration - Closing Containers 6
Reference library 7
Senior Manager Section 7
Naming Conventions and Standards 8
Naming Documents 8
Elements Required in a Document Name 8
Elements Not Required in a Document Name 9
Practices to Adhere to in Naming Documents 10
Practices to Avoid in Naming Documents 10
Naming E-mails 11
Saving Documents / Creating Records in CM 13
Maintaining the Official Record 13
Ensuring Completeness of Record-keeping 13
What Not to Save into CM 14
Finalising Documents into Records 14
Removing Document Revisions 15
Deleting Documents and Records 15
E-mail Management 16
Existing E-mail Policies / Guidance 16
The '3 Month' Rule 16
Which E-mails Should be Saved into CM? 16
Who Should Save E-mails? 16
Sending Attachments 17
Security and Access Controls 19
The Principle of Information Sharing 19
Content Manager Security 19

Access Controls at Container Level 20
Audit Trail 21
Further Guidance on Access Controls 21
Personal Containers within CM 22
Registered Files 23
Records to be Retained in Paper Format 23
Security Classification of Records Retained in Paper Format 23
Titling of New Registered Files 24
Access and Security of Registered Files (Physical Records) 24
Retention and Disposal Schedule 24
Scanning Documents 25
Posting Manual Data 25
Printing – Best Practice 25
Line of Business Applications 26
FOI Requests 26
Contact Details 26
Legislation and Standards 27
Legislation 27
Standards 27
Definition of Key Records Management Terms 28

Introduction

The NICS Records Management Policy details the commitment of the NICS to achieving the highest possible standards in records management. The NICS recognises that information is a valuable asset used to support the many services offered to both internal and external customers. Information, and its management, is of particular importance to The Executive Office (EO).

The NICS introduced its NICS Electronic Document and Record Management system (EDRMS) in 2005. Content Manager (CM) (formerly known as HPRM and TRIM) is the current NICS EDRMS used to manage electronic records. Content Manager allows EO to streamline business processes, modernise information practices and achieve compliance with important pieces of legislation such as the General Data Protection Regulation, the Data Protection and the Freedom of Information Acts.

It provides flexibility for potential restructuring and increase the opportunities for sharing information. It also facilitates the retention of the official record of government business in electronic format.

The implementation of the EDRMS established a virtual, single repository for corporate information allowing EO to promote a consistent and effective approach to creating, accessing, sharing, protecting and structuring our electronic information. This in turn facilitates the management of such information, including its review and disposal, in an ongoing corporate manner for the first time. It also helps the Department to meet its statutory obligations in relation to records management.

Roles and Responsibilities

Roles

1. Each individual who logs onto CM as an End User, Power 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:

End User

2. Within those areas of the File Plan to which they have access, an End User (ie 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; and
    - request deletion of a document via their Power User.

Power User

3. Power Users who have been identified within each business area will provide local user support. They will have received additional training to supplement the standard End User training. In addition to the functions of the End User, and in line with system access controls, a Power User will have the following permissions and responsibilities.

    - To act as first line of support within the local business area and advise on appropriate security and access control measures.
    - To provide local guidance on the use of the CM File Plan, for example on where to file documents, e-mails, etc.
    - To move documents between containers.

- To provide advice on the creation of containers at a local level in specific areas of the File Plan.
- To delete documents and the associated metadata.
- To assist the Local Information Manager (LIM) in the management of the disposal process.

System Administration

4. System administration is comprised of two elements – ongoing day-to-day administration and information management. Activities associated with the administration role would typically include:
    - location management, for example the creation of locations / user accounts, activation of temporary locations;
    - security implementation - assigning security levels to the File Plan and locations; and
    - report running – the creation and maintenance of reports.
5. Activities typically associated with the information management role would include:
    - RM configuration - configuration of systems options to reflect NICS and departmental policies and any updates to these;
    - File Plan management – the creation and maintenance of all levels of the File Plan);
    - monitoring the use of 'proper' naming conventions;
    - security management - decisions on the creation and maintenance of caveats, security levels and user types;
    - creation and maintenance of record types;
    - management of the retention / disposal scheduling process; and
    - management of document deletion (as appropriate).

6. The number of System Administrators with full system control should be kept to an absolute minimum.

Information Management and Central Advisory Branch

7. Within TEO the systems administration role is provided centrally by staff from the Information Management and Central Advisory Branch (MCAB). IMCAB is responsible for all administration, maintenance and procedural guidance for the Content Manager System.

Responsibilities of All Staff

8. It is the responsibility of every member of staff to ensure that the work they carry out on behalf of the Department is correctly saved and maintained within CM. 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 CM. 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 CM to the appropriate electronic container;
- naming (and renaming, where necessary) e-mails, documents and records properly to ensure that they can be retrieved easily, in conjunction with naming convention guidelines;
- deciding what needs to be filed within CM, including e-mails;
- declaring documents as records, ie 'finalising' them;
- ensuring record-keeping is kept up-to-date;
- determining, from the outset, the sensitivity and protective marking of documents, in line with Government Security Classification Scheme; and
- ensuring that all electronic information is afforded the necessary protection, commensurate with its inherent sensitivities, through the application of the appropriate access controls.

9. IMCAB can provide guidance on all aspects of records management and the use of CM. However, it is the responsibility of individual business areas 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

10. Detailed guidance on the development of EO's departmental File Plan is contained within the following documents (available on the IMCAB pages of the EO intranet).

    - Guidance on the structure of the TEO File Plan
    - Guidance on Using the Business Area Sections of the Corporate Functions

File Plan Administration - Creating New Containers

11. IMCAB will retain responsibility for the ongoing administration of the departmental File Plan, including the creation of new first level 'Functions', second level 'Sub-functions' and third level 'Activities'.

12. IMCAB will also retain responsibility for the creation of fourth level electronic 'containers'. End users should submit a container request form when new containers are required.

13. A unique reference is generated by EO for each container. To enable the more effective management of electronic information, each container will hold a maximum of 300 documents. When the 300 limit is reached, RM will automatically close the container. A "Part 2" container will then be created which automatically captures the "Part" number within the new container's name.

File Plan Administration - Closing Containers

14. In order to apply appropriate retention and disposal schedules on records, IMCAB will close containers once they reach two years of age. At the same time IMCAB will finalise all documents in these containers and all document revisions will be retained. Any empty containers of two years of age will be deleted. As no further documents can be added to a closed container, business areas should request the creation of a new part container if the subject is still current.

Reference library

15. The Reference library section of the file plan can be used to store departmental information and documents which are of general interest to staff. The Reference Library will be used as an internal departmental information resource.

16. On many occasions, the information placed in the Reference Library will already be stored within the operational or business area section of the file plan. This is because the Reference Library is to be used purely as a resource to communicate information to staff. The official record of departmental business must continue to be maintained within the operational section of the relevant business area file plan.

Senior Manager Section

17. Senior Managers within TEO have the opportunity to develop their own area within the Senior Managers' section of the departmental file plan. This can be used to store documents of a more sensitive nature that are not suitable for filing within their operational part of the file plan. This might include issues such as workforce planning, the departmental board, strategic planning and branch work plans.

18. All records within a senior manager's area are subject to the same records management standards set out in this policy. Records saved in these areas will form part of the Department's official record.

Naming Conventions and Standards

This section should be read in conjunction with the NICS Naming Conventions Best Practice Guidance.

Naming Documents

19. If we are to derive maximum benefit from the EDRMS, it is essential that all of the documents it contains, including e-mails, 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. The following best practice guidance has been approved by PRONI.

20. Business areas should monitor on an ongoing basis the effective use of naming convention guidance. It is recommended that the topic - action format is adopted for general use when naming documents, putting the strongest element first, for example –

    - Relocation – Options Appraisal
    - Service Lift Complaint – Remedial Action
    - Telephone Cable Damage – New Cable Quote
    - Website Strategy Group – E-newsletter Use
    - E-library Steering Group – Risk Assessment Report

Elements Required in a Document Name

21. The following naming convention is likely to be able to describe a document uniquely and therefore make it easier to find in any search. There are five elements to consider but not all elements will be appropriate for every document. However, a document name is more likely to be unique if more elements are used. The five elements are -

    I. Recipient Name – the name of the person, group or organisation to which the document is to be sent. For example, the addressee of a letter or

memo or a business area, directorate or organisation to whom a report is to be issued.

II. Recipient Address – the location of the recipient. For example, the street address, building name, town or city where the recipient is located. The choice of which to use will be determined in conjunction with the recipient's name.

III. Subject Matter – the topic of the document, i.e. what it refers to. For example, with minutes and memos it is likely to be the heading, for reports it would invariably be the title, or for an agenda or minutes of a meeting it would be the title of the group meeting, e.g. Departmental Board.

IV. Period Dates – the dates relevant to the document, i.e. what period it covers. For example, the date may relate to the subject matter, e.g. the date the meeting took place, or the period covered by a report, e.g. a calendar year or a specific to and from date range.

V. Document Type – the type of document, i.e. what style the document is prepared in. For example, the document may be in the form of a letter, memo, minute, report, submission, etc. Note that this is not the same as the electronic format of the document.

Elements Not Required in a Document Name

22. The following information is not required in a name as it is normally automatically associated with the document – **author, date created, department, i.e. EO and the electronic container name**. However, if the content of the document requires you to identify the department, date, author, etc in order to describe it properly, then these elements should be included in the name.

Practices to Adhere to in Naming Documents

- Use capital and lower case where appropriate.
- Name your document so that the name is meaningful to others and easily located,
- Provide keywords to the content to facilitate searching.
- Remove all instances of "FW", "RE" from e-mail titles.
- If using a dash " – ", include a space immediately before and immediately after the dash to enable proper searching within CM.

Practices to Avoid in Naming Documents

- Do not use all capitalisation letters in the naming of your document.
- Do not include the electronic file format information, for example e-mail, word document (or 'Doc'), Excel, etc.
- Do not include the date the document was created as this is automatically captured.
- Do not base names on your ownership of the document, for example 'Jenny's documents';
- Do not use words such as 'Miscellaneous' or 'General', as these encourage poor filing practice;
- Do not use generic names like 'Latest Version', 'Lecture', etc.
- Do not compress two or more words into one word, eg 'CorpSer' or 'RecordMan' - always separate words with spaces and type the words in full.
- Do not automatically accept the title of an e-mail contained within its Subject line as the appropriate name when saving the e-mail in CM. It is likely that you will have to rename e-mails with a more appropriate and descriptive title.

Examples of Bad Practice	Examples of Good Practice
Untitled	Archive Centre Proposal
General docs	Audit Committee – Risk Management Review
Jenny's work	Highlight Report – Dec 2022
Excel spreadsheets	Costings 1st Quarter 2022
Mtg mins	Management Committee Minutes – 11.02.23
Recommendations for new services in the Picture Library	Picture Library – new services – recommendations
Presentation on EDRMS	Electronic Document and Records Management – Benefits Presentation – Departmental Board

Naming E-mails

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

24. E-mails 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 e-mail such as sender, date sent, recipient, date received, etc as these will be automatically generated by CM.

25. Where attachments are received with an e-mail, 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 e-mail message.

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

Saving Documents / Creating Records in CM

Maintaining the Official Record

27. It is essential to identify all electronic documents, records and e-mails 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 CM when created. This will also facilitate business continuity and provide the requisite 'official' record of departmental business activity.

28. There are some exceptions where documents of a particular nature will continue to be retained in paper format – see page 23 for section on Registered Files.

29. Saving documents and records within the EDRMS helps to promote a culture of information sharing. This makes for more effective working due to the ability to access information much more quickly. Information that is not filed within CM cannot be shared or retrieved by other users.

Ensuring Completeness of Record-keeping

30. The Department 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 e-mails, 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 CM

31. While it is important to ensure that all important business-related information is stored in CM, 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 / e-mail already held in CM.

Finalising Documents into Records

32. A document can be defined as structured units of recorded information, in hard copy or electronic format. While the term record most commonly refers to documents, it should be noted that not all documents are necessarily records. Documents need to meet specified criteria before they should be considered a record. That is, the document should provide evidence of a transaction, decision or action, which is worthy of preservation. A document becomes a record in CM when it is finalised.

33. A document should be finalised as a record within CM when it can be said to be 'completed' and where it provides evidence of a business transaction or activity. During its status as a document, the creator (and other contributors with the permissions to do so) can edit and update the information which a document contains. Once a document is finalised into a record, the content is secured so that it cannot be edited or deleted – it is then 'frozen' and forms part of EO's official record. As noted in paragraph 14, IMCAB will close a container once it reaches two years of age and finalise all of the documents within it.

34. Every individual end user is responsible for ensuring that records they generate in the course of their work are finalised appropriately. To finalise a record, a user must right click and select 'electronic', then select 'final'. Documents should be 'finalised' as soon as possible. Any e-mails that have been stored in CM should, by their nature, be finalised as records (as they should not be subject to editing).

Removing Document Revisions

35. Some documents which are worked on over a period of time may necessitate the creation of a large number of associated revisions. A number of these revisions may be considered inconsequential, for example minor formatting or grammatical amendments. These should be removed (by a Power User) at appropriate stages in the document's life cycle and / or when a document is being finalised into a record.

36. To streamline this process, CM provides the functionality to "tag" the revisions that should be removed. Only those revisions that are key to the document's final outcome, for example where a significant amendment has taken place, should be retained when the document is "finalised". In many cases, it may be appropriate to remove all previous revisions at this time.

Deleting Documents and Records

37. End Users cannot delete documents. Requests to delete documents which are no longer required for business purposes should be made to the business area Power User(s). It is not possible, nor would it be appropriate, for End Users or Power Users to delete a document which has been subsequently finalised as a 'record'. If deletion of a record is required, written IAO approval is needed. Further guidance on deleting a document or a record from CM is available from the IMCAB pages of the TEO intranet.

E-mail Management

Existing E-mail Policies / Guidance

38. Staff should refer to existing NICS policies and procedures for guidance on the ongoing use and management of e-mails.

The '3 Month' Rule

39. The '3 month rule' has been implemented on the Outlook accounts of all CM users. E-mails that have not been saved into CM and remain within the Outlook e-mail application will be automatically deleted from inboxes, sent items, associated folders and deleted items 3 months after their receipt / issue. Appropriate size limits are also applied to mailboxes.

Which E-mails Should be Saved into CM?

40. All e-mails which form part of the 'corporate record' must be saved into CM, preferably as soon as possible after receipt / issue. E-mails not relevant to, or required for, business purposes should be deleted. An e-mail 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; or
    - was drafted as a result of policy or legislation.

Who Should Save E-mails?

41. For those e-mails 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 -

    I. For sent e-mails, whether internal or external, the sender should generally save the e-mail to their appropriate part of the File Plan. If some of the recipients of the e-mail are from a different business area to the sender, it may be appropriate, depending on the prevailing circumstances, for a

recipient to also file the e-mail to their particular part of the File Plan. The key determining factor will be the potential differing business needs of different business areas.

II. For external e-mails received by one person, the recipient should save the e-mail.

III. For e-mails received by more than one person within a business area, it will be necessary to establish internal business area protocols regarding the filing of such e-mails in CM. This will ensure that the official record is maintained and that information is not duplicated within the same, or a variety of, containers.

IV. For external e-mails received by more than one person, the individual with responsibility for the area of work relating to the message should save it (assuming they are one of the recipients). Where this is not clear, or where several recipients may be involved, it may be necessary to liaise with the other recipients so that the necessary protocols can be established.

V. For conversation strings (where an e-mail 'conversation' is ongoing between two or more individuals), where possible wait until the dialogue has finished or has settled at a reasonable point before saving into CM (and applying the appropriate naming conventions). Note that any attachments sent in the original e-mail will not be included in subsequent e-mails when the 'Reply' or 'Reply to All' options are used. In such circumstances, the original e-mail and its attachments may also need to be retained in CM for record purposes.

Sending Attachments

42. Where possible attachments should not be circulated within the Department. Where access controls allow, a link to the document which is stored within CM should be sent via e-mail. This will dramatically cut down on the size of e-mails sent across the Department and will substantially reduce the volume of network traffic and the size of e-mail accounts. This is particularly important to help manage the standard 350mb limit on e-mail accounts. However, a document

link will only work if the recipients of the link have been given the appropriate access to the document, as provided for by the application of the appropriate access controls.

43. As Ministerial Special Advisors may not have access to the EO File Plan, staff should continue to send attachments to EO Private Offices / Central Correspondence Unit.

44. Where documents have to be sent electronically to recipients outside the NICS, attachments will always need to be used.

45. Where an attachment is being sent to both internal CM users and to external NICS users, then both the CM link and the electronic document options must be selected

Security and Access Controls

The Principle of Information Sharing

46. Good information management practice suggests that as much information as possible held within CM should be made available to departmental colleagues. The nature of the access will of course vary, ie in many circumstances read-only access will be sufficient while it may also, depending on business need, be appropriate to provide edit access to a select group of staff. On other occasions, because of inherent sensitivities, access should be applied on a relatively limited basis.

47. CM allows information to be restricted at the document or electronic container level or even to specific parts of the File Plan. The nature of the access can also be set to members of a departmental business area or a cross-departmental working group such as a project team. Access can also be set to individuals, but the use of groups promotes a smoother transition when staff transfer within or out of EO. Likewise, we are able to share electronic information across the NICS departments in a similar way (i.e. without having to send attachments).

48. Although the principle of information sharing is to be encouraged, only information required for business purposes should be accessed. The Active Audit Events function operates on all CM documents and includes a history of views and edits. The relevant IAO should be informed if information is being accessed where there is no clear business reason for doing so.

Content Manager Security

49. There are 2 components to the CM security system - security levels and access controls.

    - Security Levels enable System Administrators to control access to the documents and records stored in CM. These have already been applied by the System Administrators to the records (documents), the locations (users) and the classification (File Plan).

    - Access Controls can be used by System Administrators, Power Users and End Users to restrict the access which all staff, or a select grouping, may

have to all of the documents held within an electronic container or indeed to an individual document. Access controls are also used to restrict the nature of the access, for example one scenario is that staff may be able to view (ie read) the documents within a container but not have the permission to edit them. Other possibilities include restricting the ability to change document access controls to a particular group or preventing staff from outside a group from adding new documents to a container.

50. The default starting position is that documents, including e-mails, saved to CM are accessible to all departmental 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, the drafting of legislation, security matters and certain Ministerial papers are all areas where restrictions are likely to be needed.

51. When a member of staff leaves a post, tightly restricted areas in CM may be opened to replacement staff or the business area by the system administrator.

Access Controls at Container Level

52. The following is a description of the nature of the access controls which can be placed on individual electronic containers, many of which are then 'inherited' by the documents saved to that container.

View Document	Determines who is permitted to view, ie read a document or record.
View Metadata	Determines who is permitted to see the metadata about a document or record (in essence to see that a document or record exists).
Update Document	Determines who is permitted to edit a document (note that 'records' cannot be edited).
Update Record Metadata	Determines who is permitted to edit the metadata for a particular document or record.

Modify Record Access	Determines who is permitted to amend the access controls currently placed on a document or record.
Destroy Record	Determines who has the authority to destroy a 'document' ('records' cannot be destroyed).
Contribute Contents	Determines who is permitted to add new documents or records to a container.

Audit Trail

53. CM provides a complete audit trail of every occasion when an attempt is made to access documents, records and electronic containers, irrespective of the nature of the access. This includes those occasions when access was successful and also when access was denied because, for example, of stipulated access controls. To check the audit trail on a document, right click on it and select Security and Audit – Active Audit Events.

Further Guidance on Access Controls

54. Guidance on the use of access controls in Content Manager including how to restrict access to a document, is available from the IMCAB pages of the TEO intranet.

Personal Containers within CM

55. Each member of staff has been provided with a personal container within CM which can be used to hold only information of a non-business nature. This container is totally separate from those contained within the departmental file plan's 'operational' and 'corporate' functions. It is designed to hold information of a personal nature which staff are permitted to create / access through the use of departmental computer systems. Guidance on the personal use of NICS ICT facilities is included in the NICS HR Policy Section 6.11.

56. Under no circumstances should any business-related information be stored within these containers. They must also not be used for storing performance management or training and development information relating to an individual member of staff. This information should be stored within the appropriate containers created for this purpose within the Staff Section of the Human Resource Management function.

57. The personal container has been created as a separate CM Record Type and is able to hold a maximum of 50 documents. For further information on using the personal container, please refer to the Guidance on the use of Personal Containers in Content Manager which is available from the IMCAB pages of the TEO intranet.

Registered Files

Records to be Retained in Paper Format

58. It is recognised that in some instances there will be a need to create physical files (e.g. Secret / Top Secret papers, legally signed documents, documents containing the departmental seal, some financial documents, records required in hard copy form and publications which cannot be scanned due to copyright issues).

59. CM allows for the registration of electronic containers and documents as well as holding information about any physical file created. Any new physical file will therefore inherit the unique container reference number from the CM container. There are 2 aspects to this:

    - If there are electronic documents and an associated physical file (perhaps containing papers marked "Secret") – the electronic documents are filed directly into the File Plan as usual and the properties of the container updated to indicate the relationship to a physical file.

    - If there are no electronic documents for the container but only physical papers – a physical registered file will be opened and a container in CM will be opened with the metadata indicating that a physical file exists. This allows the same file reference to be applied and enables effective tracking of ownership and physical location of the file. It also ensures that the appropriate disposal action can be applied to both the electronic and physical documents at the same time.

60. Where a new physical paper file may be required you should contact IMCAB to discuss how this will be best handled.

Security Classification of Records Retained in Paper Format

61. Network NI has security clearance to store information in the 'Official' classification as defined by the Protective Marking system (see the NICS Guidance on the Government Classification Scheme). In line with these important guidelines, documents and records with a Protective Marking of Secret or Top Secret should therefore not be stored in CM (or on any departmental

computer system) but retained on a separate manual registered file (the existence and location of which will be marked on the relevant CM container).

Titling of New Registered Files

62. The vast majority of the Department's records will now be retained, on an ongoing basis, in electronic format within CM. However, as outlined above, it is also recognised that there will be occasions when it will be necessary to create registered files to hold certain records in paper format. In such instances, it is likely that all other records relating to the same activity should be stored in CM.

63. In such circumstances, the same naming convention and reference number used in CM to create and identify the electronic container will also be used to create the corresponding registered file. The title and reference number of the paper registered file will therefore mirror that of its related electronic CM container. Both the paper file and its corresponding electronic container will also be cross-referenced to allow all related information to be readily identified and associated.

Access and Security of Registered Files (Physical Records)

64. In accordance with the NICS Information Asset Owner (IAO) Handbook, IAOs need to manage their information assets to comply with statutory obligations such as the UK General Data Protection Regulation (UK GDPR), and Data Protection Act (DPA) 2018, Freedom of Information Act 2000 (FOI), and the Environmental Information Regulations 2004 (EIR), in addition to Departmental records management, information assurance and security policies.

65. It is therefore the responsibility of the IAO to ensure the appropriate management and security of all the physical records within their business area/s. A record of the movements of all their business area/s physical records should be maintained, including the exact whereabouts of these records at any given time. Any access to these records must be recorded (including LIM or IAO approval).

Retention and Disposal Schedule

66. EO's Retention and Disposal Schedule identifies the retention and disposal arrangements for all records which fall within the responsibility of EO. The

schedule can be found at in the CM reference library (EO1/16/0091555) and should be reviewed by all staff.

Scanning Documents

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

Posting Manual Data

68. The transferring of manual business data (e.g., hard copy files or extracts from them) via post is prohibited and you should seek advice from IMCAB to discuss your specific requirements before transferring any data.

Printing – Best Practice

69. Whenever appropriate, staff should avoid printing hard-copy versions of e-mails, 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.

70. Examples of occasions when it is appropriate to print information held within RM 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.

71. When working with printed copies, staff must decide if any subsequent hand-written notes should be retained for 'official record' purposes, for example where comments have been added to a document during the course of a meeting. As necessary, the annotated document should be scanned and filed in CM.

72. All other printed copies should be disposed off, taking into account green housekeeping issues and, most importantly, in line with existing departmental guidance on effective and secure document disposal.

Line of Business Applications

73. It is recognised that there are a number of Line of Business Applications (LBA) both service-wide (eg Knowledge Network) and at business area level which are used to manage day-to-day business operations. Integration of LBAs with CM was not undertaken as part of the Records NI Implementation Project.

74. The use of LBAs must be highlighted to IMCAB. To provide the necessary business continuity, operating procedures will be agreed to ensure that the LBA can continue to function effectively outside of the CM environment. The need to maintain, as necessary, effective records of LBA-related information is also an important consideration.

FOI Requests

75. The tracking and monitoring of the Executive Office's FOI requests is coordinated by IMCAB.

Contact Details

76. For assistance on any records management-related issue, please contact the appropriate member of IMCAB as outlined below.

Name Redacted	IMCAB Head of Branch Departmental Information Manager CM Manager	**I&S**

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

Public Records Act (Northern Ireland) 1923 (legislation.gov.uk)

Freedom of Information Act 2000

Freedom of Information Act 2000 (legislation.gov.uk)

Environmental Information Regulations 2004

www.legislation.gov.uk/uksi/2004/3391/contents/made

Data Protection Act 2018

http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

General Data Protection Regulation 2018

https://gdpr-info.eu/

The Re-use of Public Sector Information Regulations 2005

www.opsi.gov.uk/si/si2005/20051515.htm

Standards

Northern Ireland Records Management Standard

www.nidirect.gov.uk/publications/filing-systems

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.htm

Definition of Key Records Management Terms

Access Controls - A feature of CM's 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. CM automatically captures this detail from a user's login details.

Classification – In CM terminology, the classification relates to the first three levels of EOs departmental File Plan, ie the Function, Sub-function and Activity.

Container - Containers (equivalent to folders in a Windows environment) are opened within the File Plan to hold all the Documents and Records relating to that subject. This would be similar to opening a Registered File, although such a file is designed to hold only records while a RM container will hold both documents and records. The Container is also the 4th level, ie the Subject level, of EO's departmental File Plan.

Creator - This is the person who initially creates a document, or saves an e-mail, in CM. If you compose a document and then save it into CM, you will be both the Author and Creator. However, if you save an e-mail you have received into CM, you will be the creator while the sender of the e-mail will be the author. CM will automatically capture the creator's details.

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 EO IMCAB in conjunction with PRONI.

Document - The term 'document' in EO is used to describe any electronic document created, edited and stored by an End User prior to being finalised as a 'record', e.g. e-mails, Word documents, Excel spreadsheets, PowerPoint presentations, PDFs, , 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. Containers are opened at the fourth level to hold documents and records relating to the Functions, Sub-functions and Activities represented by the first three levels of 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.

IMCAB – Information Management and Central Advisory Branch coordinates processes, and provides advice and guidance on all aspects of information management in EO.

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

Metadata - This is information about the documents or records which have been created. It is either automatically generated when a document is created or it may require the user to fill in certain fields. For example, the metadata for a document would include the title, author and date created.

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 Container / 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 Container in CM. These Personal Containers, 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 containers 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. CM describes the action taken to create a record as 'finalising'. Once a document is finalised and becomes a record, it can only be deleted from CM 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 (ie blanked out), to ensure that the person who requested the information cannot view them. The Departmental Information Manager (DIM) will advise on when an exemption may apply. IMCAB will provide guidance to staff on how redactions can be achieved, cross referenced and retained within EO.

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

Renditions - A Rendition is part of the same document and is similar to a Revision except that it is the document presented in another format, usually for accessing in a different way or for displaying different information. For example, instead of releasing a Word document as part of a FOI request, we may instead release the rendered copy of it (eg in TIF format) possibly with sections redacted. The rendered copy would still be part of the original record.

Revisions - Any editing of a Document will automatically create a new revision of that document. CM provides the functionality to view the revision history, ie the previous

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

Security Levels - A component of CM's security system that enables Access Controls to be established within CM. These are set and operated by the System Administrators.

Content Manager - This is the current EDRMS product that has been chosen by the NICS.

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. EO FOI Requests.