Rewarding Learning

Business Assurance
Records Management Policy

Records Management Policy

Version 9

21 April 2022

Contents

Introduction

1.1 CCEA recognises that management of its records is essential, both for effective administration and to enable it to comply with legal and regulatory requirements.

1.2 CCEA's records are a corporate asset and a resource of administrative, evidential and historical data. They are vital for current operations, for CCEA accountability, and for an understanding of company history and procedures.

1.3 Records are created to document business transactions, policies, procedures, programmes, and events. Only a small percentage of records continue to have value indefinitely and are kept permanently. Most CCEA records have value for 7 years or less (for example, they are kept for an entire audit cycle plus several years) at which point they are destroyed.

Policy Statement

2.1 Records will be created, maintained and retained in order to provide information about and evidence CCEA's transactions and activities.

CCEA will comply with its responsibility for lawful records management and aims to comply with relevant codes of practice and ethics in managing its records, in all media and formats.

Records will only be retained where there is a business or legal reason and will be held securely and efficiently.

Scope

3.1 This policy is applicable to CCEA and its direct predecessor bodies and the records created or received by those entities, in all media or formats.

3.2 The policy covers:

- All records held by CCEA for the purpose of conducting its business including digital records
- the requirements that must be met for records to be considered as a proper record of the activity of the organisation;
- the place of records management within CCEA's strategic and policy framework;
- the preservation of records;
- access to records; and
- the security of records.

Definitions

3.3 Records are defined in the Lord Chancellor's Code of Practice as: '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. This is any information, regardless of format or medium, captured in a reproducible format. Records may also be needed for a wide variety of reasons such as:

- personal and educational research
- public accountability, and
- to support or defend legal action.

3.4 Records are more than just information or discrete pieces of data. Records must have context and structure, to give the information meaning. Content, context, and structure contribute to a record's authenticity and to its ability to be used as evidence.

3.5 A document is any piece of written information in any form, produced or received by an organisation or person.

3.6 Records Management is the creation, maintenance, control, storage and disposal of records in a way which facilitates their most appropriate, efficient and effective use.

3.7 Destroying records of limited value saves both space and money. Keeping records and destroying records are equally important elements of CCEA's approach to records management. The decision on whether to keep or destroy is based upon the content of the records, rather than the media upon which they are recorded or the systems used to create them.

3.8 Destroying records outside an approved Disposal of Documents Schedule can have serious legal consequences and should not be undertaken without consulting Business Assurance

3.9 A Disposal Schedule is a list of records and the appropriate time limits that they must be kept for before they can be confidentially destroyed or transferred to archives for permanent storage.

Responsibilities

4.1 All staff who create, receive and use records have records management responsibilities and must comply with The Records Management Policy and associated policies. They must ensure that records are accurate, organised, and disposed of according to CCEA's approved Disposal of Documents Schedule.

4.2 Directors and Business Managers/Operational Leads within CCEA have overall responsibility for the management of records generated by their activities i.e. for ensuring that records controlled within their unit are managed in a way, which meets the aims of CCEA's records management policy.

The Business Manager ICT is responsible for the design and implementation of management arrangements in relation to digital records management. He is responsible for data security arrangements and management of ICT teams in implementation.

4.3 The Chief Executive has overall responsibility in ensuring that CCEA corporately meets its legal responsibilities, and internal and external governance and accountability requirements.

4.4 The Business Assurance Manager will advise on policy and best practice and will update the policy as required.

Records Management Requirements

5.1 Records must be able to be preserved and stored for the required period according to the CCEA Disposal of Documents Schedule. Ultimately they will be:

- preserved in the CCEA archive;
- transferred to other organisations for future preservation; and
- destroyed when their retention period is complete.

5.2 In order to ensure that the information constitutes a record, CCEA endeavours at all times to ensure that:

- records are present – information necessary to document and reconstruct CCEA activity has been recorded;
- records are accessible – records can be located and retrieved in a way which is true to the original presentation of the information;
- records can be interpreted – context can be shown, establishing when, where and who created it, how it was used and how it is related to other records;
- records can be trusted – the integrity and authenticity can be demonstrated beyond reasonable doubt; and
- records can be maintained – records are present, accessible, interpreted and trusted for as long as they are required, through transfer to other locations, systems or technologies.

Records Management within CCEA's Strategic and Policy Framework

6.1 Records management contributes to CCEA's standards of integrity, accountability and openness. Records management is critical to CCEA's commitment that decisions 'will be evidence based'; to demonstrate its accountability to its subscribers and stakeholders; to be 'transparent in our work and methods'; and 'to provide information about the CCEA's work to the wider public'.

Preservation

7.1 CCEA will preserve its records according to the retention periods set out in the Disposal of Documents Schedule. This includes maintain a corporate archive. Appropriate storage conditions for paper records will be provided. Electronic records will be maintained during any changes in the infrastructure, so that they continue to fulfil policy requirements. The classification of electronic records must be maintained, so that they can be presented in a way consistent with the original understanding of the subject when the record was created.

Access

8.1 Access to current/live records will be controlled by CCEA. Archived paper records will be stored in the CCEA archive. The ICT and Multimedia business units will maintain and review archived electronic records and associated access controls.

8.2 All records are part of the corporate memory. Unless identified as restricted or confidential by the Protective Marking Policy, they will be made readily available within CCEA.

8.3 Records that have been identified as confidential by the Protective Marking Policy will continue to be restricted, as required. Decisions to allow access to confidential records will be made by Business Managers/Operational Leads and, if necessary, endorsed by the Executive Team.

8.4 The Records Management Policy will comply with the General Data Protection Regulation, the Freedom of Information Act 2000, the Data Protection Act 2018 and the Environmental Information Regulations 2004, while complying with legal record keeping requirements and the reasonable expectation of confidentiality of its stakeholders.

Security

9.1 CCEA takes all reasonable steps to ensure the security of its records. Once recorded and entered into CCEA records, CCEA seeks to ensure that information will be safe from alteration, misinterpretation or loss.

9.2 Staff are informed of records management good practice and are required to comply with issued policy and procedure.

9.3 A Disaster Recovery and Business Continuity Plan has been developed and implemented to ensure consistency and continuity of service including the backup of electronic records and the physical security of these backups. Information security is further assured by CCEA's successful accreditation of the ISO 27001 standard and subsequent reaccreditations.

Related Legislation/Policies

CCEA Policies

- CCEA Data Protection Policy.
- CCEA Disposal of Documents Schedule.
- CCEA Disaster Recovery and Business Continuity Plan.
- CCEA Use of ICT Policy.
- CCEA Protective Markings Policy.

Legislation & Best Practice

- Public Records Act (NI) 1923;
- Disposal of Documents Order No. 167, 1925;
- International Standard on Records Management (ISO 15489);
- Lord Chancellor's Code of Practice on the Management of Records under section 46 of the Freedom of Information Act 2000;
- Northern Ireland Records Management Standards (NIRMS); and
- Records Management Standards and Guidance (The National Archives, formerly the Public Records Office, from 1998).
- Data Protection Act 2018.
- UK General Data Protection Regulation.
- Freedom of Information Act 2000.
- Environmental Information Regulations 2004.

Revision History

Version	Originator	Summary of Changes	Date
1	N/A	N/A	N/A
2	N/A	N/A	N/A
3	McGovern/ Wilson	Full review	20 Nov 18
4	McGovern	Legislation updated	14 Mar 19
5	McGovern	Management feedback updated	4 Apr 19
6	D Wilson	Updated following NIPSA feedback	22 May 19
7	L. Scott	Updated following Director/ICT Manager feedback	21 June 19
8	McGovern/ Wilson	Pre ET formatting and content checks	28 June 21
9	McGovern	Change of date for Public Records Act (NI) and inclusion of UK against title of General Data Protection Regulation	21 April 22