CYNGOR SIR CEREDIGION COUNTY COUNCIL

Information and Records Management Policy

2019

Document Control

Author and service: Corporate Lead Officer Customer Contact
Date approved by Cabinet: 19/02/2019
Publication date: 19/02/2019
Policy Review Date: February 2022

Date	Version	Author	Status
14/12/2018	1.0	Helen Palmer	Initial Draft
18/12/2018	1.1	Arwyn Morris	
14/01/2019	2.0	Arwyn Morris	Final Version
19/02/2019	2.0	Cabinet	Approved

Contact Details:

Information and Records Manager (IRM)

Phone: 01970633520 (3520)

E-mail: recordsmanagement@ceredigion.gov.uk

Contents

1 Definition of the policy

1.1 Purpose of the Policy

The information held by, and records of, Ceredigion County Council ("the authority") are its corporate memory, providing evidence of actions and decisions. Information and records support policy formation and managerial decision-making, protect the interests of the authority and the rights of employees, elected members, clients and members of the public. They are a key resource to effective operation, to accountability, and to compliance with legal and statutory requirements.

The purpose of this policy is to establish a framework for the creation, maintenance, storage, use, and disposal of the recorded information created or owned by the authority, in support of the above.

1.2 Scope

This policy will ensure that records are managed effectively through the organisation in accordance with professional principles and specified legislation and guidelines.

It applies to the whole authority – including elected members, employees (including temporary and contracted employees), and employees of organisations holding records on behalf of the authority, partnership organisations, contractors, agents and consultants to the authority, volunteers and the records of local authority schools in the county.

It applies to all recorded information of the authority whether held electronically, on film, on paper or any other media.

It applies to recorded information originating from within the authority and from outside the authority.

This policy should be used in conjunction with other policies adopted by the authority including the Information Security Policy, the Data Protection Policy, the Freedom of Information Policy and the Environmental Information Regulations Policy (see Appendix 2).

1.3 Policy Statement

This policy defines the framework for corporately managing the authority's records to ensure that the authority:

- Knows who is responsible for implementing all aspects of this policy in the authority

- Creates and captures authentic and reliable information to demonstrate evidence, accountability and information about its decisions and activities
- Manages records according to the agreed procedures, and to relevant standards. Records will be held securely and appropriate access to them ensured, regardless of medium.
- Conforms to any legal and statutory requirements relating to record-keeping including the Data Protection Act 2018, the Environmental Information Regulations and the Freedom of Information Act 2000.
- Maintains records to meet the authority's business needs.
- Addresses the needs of the authority's stakeholders, including the public, elected members, employees and Ceredigion Archives, the county record office.
- Can facilitate auditing and can protect its legal and other rights
- Disposes appropriately of records that are no longer required, including the preservation of records of long term and historical value
- Protects critical records, which it needs in order to function effectively

2 Identification of roles and responsibilities

The **Chief Executive** has overall responsibility for ensuring that records are managed responsibly and with regard to legislation within the authority.

The **Senior Information Risk Officer** (SIRO) is responsible for the oversight of records management provision in the authority and for the ultimate approval of recommendations of changes to the Corporate Retention Schedule

The **Information Governance Group** (IGG), chaired by the SIRO exists to provide advice and assurance to the authority on information and records management, and to ensure that effective policies and practices are in place.

The **Information and Records Management Service** (IRMS) is responsible for the development and implementation of methodologies for information and records management. It will maintain and develop the Corporate Records Retention Schedule, and provide advice and guidance to the Authority. It will work with others to ensure that the policy is understood and implemented by the whole authority.

Corporate Lead Officers (CLO) are responsible for ensuring that the policy is implemented in the services for which they have responsibility. They will nominate service representatives, who will work with the Information and Records Management Section on the management of records in the service.

Information Asset Owners are the nominated representatives with responsibility for the implementation of the Information and Records Management Policy in their service areas. They will be identified in the Corporate Retention Schedule and have

responsibility for the safety of the information and records, and will work with the Information and Records Management service.

It is the responsibility of **Legal Services** to review and comment on proposed changes to the Corporate Retention Schedule, and advice as necessary on matters relating to the legal admissibility of records.

It is the responsibility of **ICT** to provide technical support for applications which facilitate information and records management, and to advise the IRM section on the presence of records held in obsolete software systems.

It is the responsibility of **Internal Audit** to regularly review the management process and provide comment on any new/changes to the retention schedule.

It is the responsibility of **all employees, elected members and schools** to practice good information and records management in accordance with this policy and with any policies and guidance subsequently produced.

3 Implementation of the policy

3.1 Training and Awareness

All employees of the authority are involved in creating, using and maintaining records. It is important that everyone understands their responsibility for records management as set out in this policy.

Training will ensure that all employees and elected members are aware of their obligations with regard to Data Protection, Freedom of Information, Information Security and Information & Records Management.

Information and Records Management awareness will form part of the induction procedure for new employees.

3.2 Record Creation

The authority will apply good information and records management principles to information and records created or received as part of its activities

3.2.1 Ownership

All records created by employees of the authority in the course of their work remain the absolute property of the authority unless otherwise specifically agreed

3.2.2 Evidential significance

Adequate records of all activities will be maintained to account fully and transparently for all actions and decisions of the authority.

3.2.3 Accuracy and authenticity

The authority shall ensure records are complete and accurate and that the information they contain is reliable and its authenticity can be guaranteed

3.2.4 Accessibility

Information and records should be created using clear and unambiguous language appropriate to the subject, suitable fonts and font size, and relevant corporate templates where appropriate, so that records can easily be read and understood.

3.2.5 Legislative compliance

All the information and records created by the authority may be used in requests for information under the Freedom of Information Act, Environmental Information Regulations and Data Protection Act. Employees must not create, delete or alter information that has been requested under legislation.

3.3 Record retention and record disposal

The authority will store information and records to maximize efficiency, reduce costs, enable sharing and minimize risks.

All information and records must be held in secure environments regardless of medium.

All records are subject to the authority's retention schedule.

Any record which might be used as evidence in a legal or regulatory process should be subject to access and audit trail controls to ensure that its reliability, integrity and evidential value can be demonstrated.

3.3.1 Responsibility for record keeping

All employees are responsible for the protection of records they process. It is employees' responsibility to ensure adequate secure storage arrangements are provided which protect information and records from unauthorised or inadvertent alteration or destruction, controls access and disclosure with appropriate audit trails, and maintains the information and records in a robust format which remains readable so long as the information and records are required.

They should work with the IRMS to achieve this outcome.

3.3.2 Arrangement of information and records

Information and records will be arranged so they can be retrieved quickly and efficiently for the length of their lifecycle. Each service should take into account the legal and regulatory environment specific to their area of work.

3.3.3 Ceredigion County Council's Classification Scheme

A classification scheme is a way of organising records to make the management of them easier. Classification schemes consist of classes that represent broad functions sub-divided into sub-classes.

The authority will continue to develop a corporate classification scheme for the storage of information and records, and to facilitate the application of access control and retention schedules. The authority will use and may adapt the Local Government Classification Scheme [LGCS] for this purpose.

3.3.4 Access Control

The security of the authority's records is essential. The security controls in place to safeguard the information and records of the authority are detailed in **the Information Security Policy.**

3.4 Records Storage

3.4.1 Storage of physical information and records

Storage accommodation for physical records should protect the records from damage, accidental loss or destruction, and prevent unauthorised access. Records storage facilities, shelving and equipment must meet occupational health and safety requirements.

Physical records that must be retained for legal or business purposes but are no longer required day to day should be placed in the care of the IRMS with access to the records provided on demand.

3.4.2 Storage of electronic information and records

The authority will continue to develop appropriate solutions for the storage and preservation over time of electronic records in a structured and managed environment.

The arrangements in place for managing electronic information and records in every service should be agreed with ICT and the IRMS, clearly documented and periodically reviewed.

3.4.3 Disposal and transfer

Services must have in place clearly defined and accountable arrangements for the appraisal and selection of records for disposal and transfer, and for documenting this work.

Specific requirements for keeping and disposing of all records regardless of medium are contained within the authority's ***Corporate Retention Schedule***. All records should be managed in accordance with this schedule. Any divergence from the schedule should be authorised by the SIRO.

Documentation of the disposal/transfer of records must be completed and retained for audit purposes.

Mechanisms for the regular transfer of records selected for permanent preservation should be in place to achieve transfer to Ceredigion Archives, the County Record Office,

Wherever records are held on corporate electronic data & records management systems [EDRMS], consideration must be given as to whether automated system retention, disposal & review dates should be used or whether manual ones should be given.

Records subject to an open request under the Data Protection Act or Freedom of Information Act must not be destroyed.

The SIRO will approve the methodology for the secure destruction of records.

4 Use of information and records

4.1 Using physical information and records

Physical information and records are the responsibility of the user, who should have regard to their safety and security at all times. Records should not be removed from the authority's premises except in cases of necessity, when adequate and appropriate security measures should be employed.

4.2 Use of the File Room and off-site storage

The File Room at Canolfan Rheidol, Penmorfa and all the authority's off-site storage is in the care of the IRMS. Requests for documents should be made to IRMS using the proper methodology and logged. Records are the responsibility of the requestor until they are returned to IRMS. Records should be returned in a timely fashion.

4.3 Digital continuity

Electronic records are dependent on technology to access and read them. The IRMS will work with ICT to ensure that information created digitally is accessible for as long as necessary. This may involve the use of non-proprietary formats and the use of PDF/A standards where necessary.

4.4 Critical Records

In the event of a disaster critical records will have the highest priority for preservation, rescue and / or restoration. The authority must be aware of its critical records and services should have contingency plans in place.

4.5 Business Continuity and Recovery

If records are damaged the service area must undertake a risk assessment to decide whether restoration would be beneficial. Advice should be sought from the IRMS or Civil Contingencies Unit.

4.6 Risk Management

Information and records form part of the corporate assets of the authority. Issues relating to the management of information and records should be incorporated into the corporate risk management framework and included on each service's Risk Registers.

The authority will manage risks relating to the confidentiality, integrity and availability of records.

4.7 Information sharing and sharing of personal data

In delivering its services the authority must have proper regard to the sharing of personal data in accordance with legislation.

4.8 Partnership Working

Data-sharing protocols will be drawn up with partners to reflect agreement in data sharing**.** The authority will ensure that any partners involved in projects or the delivery of services have proper management with agreed standards in place for records created under partnership initiatives.

4.8.1 Partnership working: where Ceredigion is the lead partner

- Core records will be retained and managed by the authority under retention schedules agreed by the authority.

- The authority's Corporate Information and records Management Policy will apply

4.8.2 Partnership working where another organisation is the lead partner

- Core records will be retained by the other organisation
- The authority will identify and manage records relating to its role in the partnership under retention schedules agreed by the authority.

4.8.3 Partnership working where no single organisation is the lead partner.

- The authority will ensure that an agreement is in place with one partner for the management of core records

5 Policy Monitoring and Review

The SIRO and IRM will formally review the policy annually and amend if necessary. The amended policy will be distributed to all staff.

The policy will be reported to Council on a 5 yearly basis or when significant changes are made.

Appendices

Appendix A: Definitions

What is a record?

A record is any recorded information regardless of medium (including paper, microform, electronic (including e-mail), audio-visual and record copies of publication) created, collected, processed, used, stored and/or disposed by The authority or its employees, as well as those acting as its agents and consultants, to support and show evidence of The authority activities.

What is records management?

Records management is that "*field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and [disposal] of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records*".

BS ISO 15489-1: 2001 Information and documentation – Records Management

Records management is about controlling the authority's records to ensure authenticity, reliability, integrity and usability.

What is the retention schedule?

This is a document setting out what records the authority holds and how long they will be retained before disposal. It can also be used to set out what needs to happen to records at various different stages of their lifecycle to ensure that they are stored efficiently.

What are critical records?

These are records without which the authority could not effectively function or be reconstructed in the event of a disaster. These include records the authority requires to recreate its legal and financial status, to reserve its rights and to ensure that it can continue to fulfil its obligations to its stakeholders.

What is metadata?

Metadata is the information attached to a record which describes technical aspects of the creation, use and retention of the record and its relationship with other records.

What is protective marking?

A protective marking system formalizes the levels of sensitivity of information within documents and allows different levels of protection to be applied depending on the expected impact of loss or compromise of the information. It may also determine how a document can be accessed, stored, shared and disposed.

Appendix B: Legislation, regulations, standards and policies

Legislation which affects the management of the authority records includes:

- Public Records Acts 1958 and 1967
- Local Government (Records) Act 1962
- Local Government Act 1972
- Local Government (Access to Information Act) 1985
- The Environmental Information Regulations 2004
- Local Government (Wales) Act 1994
- Data Protection Act 2018
- General Data Protection Regulations 2016
- Local Government Act 2000 (ss 97-98)
- Freedom of Information Act 2000
- Taxes Management Act 1970
- Value Added Tax Act 1994
- Limitation Act 1980

Records Management Standards and Guidelines

Standards

BS4783 - 8:1994	Storage, transportation and maintenance of media for use in data processing and information storage
ISO 27001	Code of practice for information security management
ISO 15489	Information and Documentation - Records Management
ISO 15489	Code of practice for legal admissibility and evidential weight of information stored on electronic document management systems
BSI DISC PD0010	Principles of good practice for information management

Other Standards and guidelines

- The National Archives' standards for the management of public records
- The National Archives' Requirements for Electronic Records Management Systems
- The Lord Chancellor's Code of Practice on the Management of Records issued under Section 46 of the Freedom of Information Act 2000
- Retention Guidelines for Local Authorities by the Local Government Group of the Records Management Society Great Britain
- Guide to the General Data Protection Regulations produced by the ICO
- Data Protection Gov.UK advice https://www.gov.uk/data-protection
- Ombudsman : Principles of Good Administration and Good Records Management and Summary