Carmarthenshire County Council Records Management Policy

sirgar.llyw.cymru
carmarthenshire.gov.wales

Cyngor Sir Gâr
Carmarthenshire
County Council

Information Governance

Records Management Policy

Contents

Cyngor Sir Gâr
Carmarthenshire
County Council

1. Introduction

1.1 Carmarthenshire County Council (the Council), in common with all local authorities, creates and receives records. Having accurate and relevant information is vital to the efficient management of the Council and the delivery of our services.

1.2 We also need to balance our statutory obligations and our desire to be open and transparent (for example providing information under the Freedom of Information Act 2000) with our legal duty to keep personal data confidential, and process it in accordance with relevant legislation.

1.3 There is a range of legislation relating to Records Management, the three main provisions being:

- Section 224 of the Local Government Act 1972 – requiring that
- Section 60 of the Local Government (Wales) Act 1994 – this requires a Councils to make and maintain schemes for the care, preservation and management of their records.
- The Lord Chancellor's Code of Practice issued under Section 46 of the Freedom of Information Act 2000 – this provides guidance to public authorities in connection with the keeping, management and destruction of their records, including the need to have a Records Management Policy in place.

1.4 In addition, the majority of records created and managed by the Council contain or are wholly comprised of personal data and therefore fall within the scope of the Data Protection legislation, which is:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018

1.5 This policy is based on the international standard for Records Management ISO15489 and is supported by The National Archives' standards. It also takes into account the Section 46 Code of Practice and the requirements of Data Protection legislation in order to ensure that the Council complies with its obligations in this regard.

2. Policy statements

2.1 The Council values its records and the information contained within them as corporate assets.

2.2 We will create and manage all records efficiently, make them accessible when needed, but protect and store them securely and dispose of them safely at the appropriate time.

2.3 Compliance will be monitored by the Records Management Unit (RMU) with the aid of data analysis software that will identify records due for disposal. The RMU also manages paper records in the same manner.

2.4 We produce and maintain detailed Retention Guidelines to assist with Records Management.

2.5 The Council ensures that our employees have access to Records Management and Data Protection training to ensure that they manage records properly, including provision of induction training to new employees.

2.6 The Council owns all records created and used by employees, in any format, when carrying out its functions.

2.7 Unless an external source of a record keeps legal ownership (for example records seized as evidence during an enquiry) records received are also owned by the Council.

2.8 Any records produced or received by the Council which are not in the public domain and which contain information on identifiable individuals will always be treated as strictly confidential.

2.9 The RMU will review this policy regularly to ensure that it continues to be relevant and up to date.

3. Purpose and scope

3.1 This policy sets out the roles and responsibilities for managing records, in any format, and stored in any media within the Council.

3.2 It aims to ensure that all Council employees understand what they must do to protect and manage records effectively, efficiently and economically.

3.3 The policy and the standards that go with it apply to all permanent and temporary employees, contractors and volunteers who have access to the Council's records, wherever these records are and whatever format they are in.

4. Definition of terms - records

4.1 The term 'record' is defined as:

> *'information created, received and maintained as evidence and/or information by an organisation or person, in pursuance of legal obligations or in the transaction of business'.*

4.2 We can also further define four distinct categories of records:

- Current – records needed to efficiently and effectively conduct current business;

- Semi-current – records not needed to support current business, but which need to be retained for defined periods for operational, regulatory or legal reasons. These records are often referred to as 'Modern Records';
- Archival – records retained permanently because of their value as evidence. The Council operates a public archive service for such records;
- Redundant – records which are no longer required and which are not archival. Redundant records should be destroyed.

5. Definition of terms - personal data

5.1 'Personal data' is defined in the UK GDPR as any information relating to an identifiable person who can be identified directly or indirectly by referring to an 'identifier'. In practice, a wide range of identifiers will constitute personal data, including names, addresses, unique reference numbers, online identifiers and narrative about a person.

5.2 The actions or operations we perform on personal data, including collection, recording, use, storage and destruction are referred to collectively as processing.

5.3 The UK GDPR also defines special categories of sensitive personal data, which are also processed by the Council as part of our records. The special categories are personal data about:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health
- Sex life or sexual orientation

5.4 Criminal convictions data is specified as a separate category in the UK GDPR and is defined as information about criminal allegations, proceedings or convictions.

5.5 The Council must process all of the personal data contained in its records in accordance with the principles set out in the UK GDPR. These require that personal data must be:

- Processed lawfully, fairly and transparently
- Used for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is needed
- Accurate and up to date
- Kept for no longer than necessary
- Secure

6. The need to manage records

6.1 Maintaining efficient records management practices will help us meet our statutory obligations and business responsibilities under our Corporate Strategy.

6.2 In any format, records must be protected. Records must also be accurate, ordered, complete, useful, up to date and accessible whenever they are needed, in order to:

- Help us carry out our business, discharge our functions and deliver our services;
- Make sure we comply with relevant legislation, including but not limited to Data Protection legislation and the Freedom of Information Act 2000;
- Help us all make informed decisions;
- Keep track of policy changes;
- Ensure that legal precedents are identified;
- Support continuity and consistency in management and administration;
- Protect the rights of employees, regulated entities and the general public;
- Provide an audit trail to meet business, regulatory and legal requirements;
- Increase efficiency and cost-effectiveness by ensuring that records are disposed of when no longer needed. This enables more effective use of resources, for example space within office premises and IT systems;
- Make sure that we work effectively as a regulator and prosecuting authority and meet our lawful obligations for disclosing evidence.

7. Roles and responsibilities

7.1 Executive responsibility

The Senior Information Risk Owner has overall executive responsibility for our Records Management Policy, and for supporting its application throughout the organisation.

7.2 Records Management Unit (RMU)

The RMU is a corporate service responsible for managing all records efficiently, making them accessible when needed, but protecting and storing them securely and disposing of them safely at the appropriate time in line with our Retention Schedules.

- Policy – the RMU is responsible for making sure that the Records Management Policy and associated Retention Guidelines are reviewed, kept up to date, and are relevant to the needs and obligations of the organisation;
- Advice and guidance - the RMU is responsible for giving records-management advice and guidance to employees;
- **‘**Orphan’ records - the RMU is responsible for seeking decisions about the management of records for which there is no clear business unit

responsibility, for example records for entities that are no longer run by the Council;
- Modern Records - The RMU is responsible for managing the authority's Modern Records (semi current paper records).
- Preservation – the RMU is responsible for identifying records which may be of historical value by referring them to the County Archive Service for permanent preservation.

7.3 Managers

Managers are responsible for ensuring their employees are aware of the requirements of this policy and their responsibilities for managing records.

Managers at all levels are responsible for:

- Developing and operating records management procedures within their services/business units, covering both electronic and hard copy records, that are efficient and fit for purpose and comply with this policy;
- Communicating these local records management procedures to their employees;
- Ensuring that appropriate resources exist within their business unit or service area for fulfilling the responsibilities for managing records;
- Quality assurance of records management processes and procedures;
- Ensuring that employees follow policies and procedures for the management and storage of electronic records;
- Co-ordinating responses to retention reviews on behalf of Heads of Service and informing the RMU of changes to retention periods as a result of service related legislation or changes in the business need of the service;
- Ensuring that records are accurate and up to date;
- Ensuring the appropriate disposition of records.

7.4 Project records

Records about projects, which involve two or more Council departments are the responsibility of the designated project manager. Project managers are responsible for:

- Identifying project related records and liaising with relevant local contacts to ensure that the records are managed efficiently and comply with this policy;
- Ensuring that there are appropriate resources within the project for fulfilling the responsibilities for managing records;
- Quality assurance of records management processes and procedures within the project;
- Ensuring the appropriate disposition of project records.

7.5 Employees

All employees who create or receive records are responsible for following the records management procedures that apply within their business unit.

8. Storing and handling records

8.1 Records that continue to be useful and relevant, whether in paper or electronic format, need appropriate storage and handling to preserve them for as long as they are needed.

8.2 Storage of records must be in accordance with the following Council policies and guidance:

- Handling Personal Data Policy
- Information Security Policy
- Email Usage & Monitoring Policy

8.3 Paper records deposited with the RMU will be stored in locked strong rooms where temperature and relative humidity is monitored and electronic records' format will be monitored to ensure that they can still be read for the duration of their retention period.

8.4 Electronic records identified for long term or permanent preservation will be stored within a specialist archival collections management system.

9. Access to and security of records

9.1 The Council's Information Security Policy and Handling Personal Data Policy address access to and security of records and are available for employees to view on the intranet.

9.2 All employees must complete an e-learning module on Data Protection. This includes new members of staff when they commence employment with the Council.

10. Business continuity

10.1 With regard to records held in electronic formats, the Council's ICT division has produced a Disaster Recovery and Business Continuity Plan which ensures business continuity in the event of one or both data centres being impacted for an extended period of time. This plan is regularly reviewed and updated.

10.2 The RMU has produced and implemented an Emergency Plan for the paper records deposited with the unit.

10.3 Each business unit that relies on paper records to deliver its functions in whole or part should apply the principles of the Emergency Plan to its premises and records. The Emergency Plan is published on the Council's intranet site and can also be obtained by contacting the RMU.

11. Disposition of records

11.1 Disposition is the process of deciding whether to keep, move or destroy records.

11.2 Within the Council, the following disposition actions may be considered:

- Permanent physical disposal of hard copy records and deletion of electronic records;
- Retention for a further period within the business unit;
- Transfer to an appropriate storage area;
- Transfer to the RMU (in the case of hard copy semi-current records);
- Transfer to a storage area managed for the Council by an external provider where appropriate contractual arrangements have been entered into;
- Transfer of records to the County Archive Service, if the records are selected for permanent preservation;
- Transfer to another organisation that has assumed responsibility for the business activity through restructuring, transfer or privatisation;
- Transfer of responsibility for management to an appropriate authority while physical storage of the record is kept by the creating organisation.

12. Retention Guidelines

12.1 As a requirement of this policy, the Council has put in place Retention Guidelines which are available on the intranet and Council website and set out how long each record type should be kept.

12.2 They include, where applicable, the justification for these periods.

12.3 The Retention Guidelines are regularly reviewed and updated to reflect changes in legislation, service delivery and so forth.

12.4 Once records have met their required retention period and are identified for destruction, they must be permanently destroyed or deleted from storage media.

12.5 The requirement to destroy or delete records does not apply where they are subject to an active 'Embargo/Legal Hold'. An Embargo/Legal Hold is a written directive that requires the suspension of the destruction of records even if the applicable retention periods have expired. An example would be where records identified in the embargo are subject to potential or active litigation, or a government inquiry.

12.6 In the event that the Retention Guidelines do not specifically refer to the type of record considered for disposition, the RMU should be consulted.

13. Permanent destruction or deletion of redundant records

13.1 Before disposing of records in any format, the following steps must be taken:

- The Retention Guidelines must be consulted in order to confirm that the specified retention period has passed. When calculating this, employees should refer to the last month and year in the date range. If the records are only identified by year, employees should confirm whether it relates to a calendar year or financial year;
- It must be confirmed that all known audits, investigations or litigation are completed or resolved;
- The type of destruction/disposition required must be determined and a record kept containing a brief description of the records to be disposed of and the date of disposal;
- A form for recording disposal details is made available on the intranet. The RMU will keep completed forms permanently.

13.2 The UK GDPR requires that appropriate measures be taken to guard against unauthorised or unlawful use of personal information and against its accidental loss. It is therefore a legal requirement that records containing personal data are disposed of safely.

13.3 It is therefore essential that any paper records which contain personal data (as well as otherwise confidential information) are either shredded or destroyed via a confidential waste service.

13.4 It should be noted that inappropriate disposal of personal data could lead to enforcement action, including a significant financial penalty being imposed on the Council and disciplinary action taken against the employees responsible.

13.5 When using the confidential waste service to dispose of records containing personal data or otherwise confidential information, the following steps must always be taken:

- Confidential waste sacks containing personal or confidential information must be stored securely until they are collected. Storage should be in a locked room where available – sacks should not be kept within offices as this introduces the risk of them being picked up in error and disposed of incorrectly;
- Alternatively, lockable bins can be obtained from the company providing the service;
- Under no circumstances should filled confidential waste sacks be stored in areas accessible to the public or unauthorised persons, such as in corridors;
- The provider of the confidential waste service must be asked to contact a responsible officer shortly in advance of their arrival on the day of collection to enable the sacks to be moved to a designated collection point.
- The collection point must be within secure premises and not accessible to the public;

- Following collection, a certificate should be obtained from the service provider recording their receipt.

14. Ensuring equality of treatment

14.1 This policy must be applied consistently to all irrespective of race, colour, nationality, ethnic or national origins, language, disability, religion or belief, age, sex, gender identity, sexual orientation, parental, marital or civil partnership status.

To obtain this policy in another format or for further information and advice regarding records management, please contact the Records Management Unit on 01267 224183 or email **RecordsManagement@sirgar.gov.uk**

Policy approved by the Executive Board on: 1st April 2019
Policy reviewed: August 2023
Policy written by: Nia N Thomas