Records Management Corporate Procedures

Name of Record	Records Management Corporate Procedures
Author	Senior Information and Improvement Officer
Owner	Chief Executive's Business Manager
Date	28/4/21
Review Date	28/4/23

Version	Notes	Author	Date
0.1	First draft	HJ	20/02/2021
0.2	Updated following CMG review	HJ	20/04/2021
0.3	Update following CMG final review	HJ	21/04/2021
1.0	Saved as V1.0	SIIO	28/4/21

Introduction

This document provides high level procedures to assist East Renfrewshire Council in implementing effective records management in line with Council policy, accounting for legislative, regulatory and council requirements throughout the life of Council information and records.

Scope

These procedures apply to:

- all employees of ERC, third party organisations or contractors and anyone else who uses, administers or is accountable for ERC's corporate and line of business systems, shared and personal filing repositories on the Council network and Microsoft 365 to support their work
- all records and information created, sent, received, shared or used by ERC in the undertaking of its functions

Responsibilities

All staff are accountable for the appropriate creation, management and use of Council information and records, based on their role as set out in the Council's Records Management Policy add link. This includes:

- All Council staff, including temporary staff, students and volunteers who access and use Council information and the information systems that store them.
- All third parties that manage and process information on the organisation's behalf when supporting delivery of Council statutory or business functions.

Creation and capture

Full and accurate records of activities and decisions must be systematically created and captured based on the value and function of the records to the Council and its employees, the individuals and communities that it serves, the public, regulatory and statutory bodies and all other stakeholders to which it is accountable, considering both current and future needs.

Records should be created, captured, managed and retained in digital format except where there is a business reason for the production of hard copy

The records must be accurate and complete, so that it is possible to establish what has been done

and why.

The quality of the records must be sufficient to allow staff to carry out their work efficiently, demonstrate compliance with statutory and regulatory requirements, and ensure accountability and transparency expectations are met.

The integrity of the information contained in records must be beyond doubt; it should be created at the time of the activities to which it relates, or as soon as possible afterwards, and be protected from unauthorised alteration or deletion.

Where appropriate, templates should be used, so that documents are produced consistently and quickly. In addition, version control procedures are required for the drafting and revision of documents, so that staff can easily distinguish between different versions and readily identify the latest copy.

Individuals or roles must be identified within business areas to take responsibility for records or record sets and fulfil the role of Information Asset Owners and Administrators.

More detailed guidance on the creation and capture of digital records can be found in the relevant sections of Taking Control of Our Digital Records add link

Storing and organising records

Records must be managed and stored in the appropriate Council system or file repository and in a suitable format to retain quality, relevance, accessibility, durability and reliability. Any transfer to another format must have due regard to retaining these qualities.

Both paper and digital records systems should contain metadata - information about the structure of the records system or series - to enable the systems and the records to be understood and used efficiently, providing business context for effective management of the records, and to enable individual and aggregated records to be identified and accessed efficiently. This must be based on the Council's integrated business classification scheme and retention schedule add link, recordkeeping metadata standard add link and file naming conventions.

The Council's file naming convention and other detailed guidance on storing and organising digital records in shared drives, MS Team Files and business systems can be found in the relevant sections of Taking Control of Our Digital Records add link.

Protecting finalised records

Organisational and technical controls must be designed and applied to processes and systems to ensure finalised records are protected from further change.

Authenticity and reliability controls must be designed into processes and systems to ensure that records can be trusted and relied upon as credible and verifiable evidence by ensuring that they are created through routine and repeatable processes, can be proven to be of undisputed origin and trusted to be genuine.

Security and access

Appropriate levels of security must be in place to prevent the unauthorised or unlawful use and disclosure of information. Protection and security controls must be designed and implemented to ensure records are only accessed, amended, used, shared or disposed of, as authorised.

All records in any format must be held in accordance with the Council's Information Security and Data Protection Policies, procedures and guidance add links. Records must be stored in a safe and secure physical and digital environment taking account of the need to preserve important information in a useable format enabling access proportionate to the frequency of use.

The Council's Security Classification Scheme add link should be used to classify information and records to enable compliant practice regarding storage, access, handling and disposal of records.

Records should not be only accessible by a single person but should be stored in the appropriate business system or file repository, so that Services can operate efficiently when individual members of staff are absent.

Where possible, records should be created, captured and stored once and access provided appropriately across the Council in order to provide a single source of the truth and avoid

recreating information that already exists or storing duplicate documents unnecessarily.

Vital records business continuity and disaster recovery

Records that would be vital to the continued functioning of the Council in the event of a disaster must be identified and protected. These include records that would recreate the Council's legal and financial status, preserve its rights, and ensure that it continues to fulfil its obligations to its stakeholders.

All critical business information must be protected by appropriate preservation, backup and disaster recovery policies.

Preservation and sustainability

Records must be preserved for the period of time they must be retained.

All records must be maintained in a format which is expected to survive and be readable for the required life of the record.

Physical records must be in a format and made of materials which mean they are likely to survive and be readable for the required life of the record.

Digital records must be in a format that is expected to survive and remain accessible and readable using readily available software for the required life of the record.

All records must have sufficient descriptive information attached to them to allow access and management over time. Typically, for both physical and digital records this information is represented as metadata held in systems.

All records must be managed to facilitate migration or relocation over time. Digital records must be held in systems that provide effective export of the records (including metadata) from the system. Physical records must have sufficient information maintained to identify their content and location and must be held in facilities and under arrangements which mean they can be relocated efficiently.

Where documents or records are either “born digital” or where hard copies are digitised, the Council will ensure that there are appropriate standards and guidance in place to ensure that records of permanent or continuing value remain accessible and preserve their integrity for as long as required, accounting for changes in IT software and hardware. Adherence to these standards and guidance will safeguard the authenticity and integrity of digital records in the long term and will allow the storage of digital records safely through adoption of security mechanisms appropriate to each classification of information.

Retention

Records must only be kept for as long as is required to meet operational, business and legal needs. It is a legal requirement established by Data Protection legislation to only retain records containing personal data for as long as is strictly necessary, and the Council could be subject to enforcement action for failing to comply. By having clearly defined procedures for the retention and disposal of records, the Council can demonstrate corporate responsibility in the management of its information and records.

The Council’s Records Retention Schedule sets out the appropriate retention periods for different categories of record. It applies to all formats of records, regardless of format or location and promotes consistency and the retention of the minimum volume of records while accounting for requirements imposed by legislation and regulation.

Business areas must agree retention periods for the information and records they are responsible for, using the Records Retention Schedule. Service managers are responsible for ensuring that retention periods are regularly reviewed to determine whether any retention periods applying to information held by the Service have expired.

The principles governing the retention and subsequent disposal of records apply regardless of their format but the procedures we use to apply these in practice differ between paper and digital records and the different systems they are stored in and processed by.

For procedures and guidance for retention and disposal of records in specific systems and file

repositories, refer to:

- M365 Information Governance Policy add link
- Taking Control of Digital Records add link
- Using the Records Store add link
- Records Store Procedures add link

Records life-cycle retention

Where relevant, detailed life cycle management of information assets and records (including retention and disposal) should be developed and incorporated into procedures, processes and systems relevant to the related core business activity. This is likely to include:

- the individual records that make up a final aggregated record
- working documents and drafts that do not form part of the final record that can be destroyed at finalisation of work
- the process and point at which individual documents should be declared as records and closed down to further amendment
- the explicit process that represents the retention trigger

Disposal

Once the retention period has expired, relevant disposal action for Council records must be taken, in line with the Council's Records Retention Schedule.

The possible outcomes are:

- destroy
- extend retention period
- retain permanently

Need for records disposal review

Where the records and associated business activity represents no business risk e.g. administrative records of no ongoing value, there will be no need for review, and the records can be destroyed as part of normal business. For other activities, before action is taken to permanently preserve or destroy a record at the end of its retention period, a review should be undertaken to identify any need for longer retention.

Where a change in retention requirement for the records series is identified, for example where there has been a change in governing legislation or regulation or internal policy that requires the retention period to be increased, the Council retention schedule should be updated to reflect this change. All related procedures, processes and business system settings governing retention should also be updated.

Records destruction holds

In certain circumstances it may be necessary to retain specific records even though their formal retention period has expired as they are required for to support ongoing action. This includes public inquiries, active litigation (or threat of litigation), investigations and access request received under data protection or freedom of information legislation. These are known as records destruction holds.

In these circumstances, the records and information affected must not be destroyed until the activity that has prompted the hold action has been completed or resolved with a new retention timescale should be assigned to it. Record destruction holds apply equally to hard copy and digital records.

Extending retention periods

If a Service wishes to retain any records beyond their approved retention

periods contact the Senior Information and Improvement Officer to receive approval to assign a new destruction date. If the records include official-sensitive data, the reason for assigning a new destruction date must be documented.

Destruction

Departments are responsible for ensuring that records are destroyed in a timely and secure manner. Destruction must be carried out in a way that takes full account of the confidentiality of the record using the Council's Security Classification Scheme.

Other than for material stored in the corporate records store, the process for the destruction of records should be documented and should seek to ensure that all copies of a record are

destroyed, taking account of records dispersed across different physical locations and digital systems.

Records Transfer and Destruction Procedures

Departments are responsible for assuring that the records are properly prepared for storage and identified so that they can be easily retrieved if needed. Complete instructions for transfer, retrieval and destruction of physical records can be found in Using the Record Store add link

Permanent preservation

Some of the Council's records are retained permanently because they have long term evidential or historical value.

The Council's Records Retention Schedule helps to identify Council records considered worthy of permanent preservation and provides two different disposal actions for these records.

- Retain for business or historical value: the full record must be retained
- Review for business or historical value**:** a random sample or selected examples of particular significance or interest may be considered worthy of preservation

Guidance on arrangements for the permanent preservation of paper records and transfer to archives are available in Using the Records Store add link and Records Store Procedures add link.

The Council does not yet have a digital archive repository. However guidance for Departments on identifying and managing digital records of archival value can be found in Taking Control of Our Digital Records. add link

Records of disposal

For potentially significant information, a record should be kept of what has been disposed of. For paper records, this is managed at the Records Store. For more information see Using the Records Store add link and Records Store Procedures add link.

For digital records, Departments must complete a Records Disposal Form stating what has been disposed of, why it was disposed of and who authorised it, covering both destruction and retention for permanent digital preservation.

This ensures that there is a transparent audit trail detailing evidence of records that have been destroyed in line with the Council's Records Retention Schedule add link.

Disposal of IT equipment

All disposal of IT equipment must be conducted via IT Services to ensure that it is done securely and that any information remaining on any storage device is securely wiped. IT Services have further information and advice in relation to the disposal of IT equipment.