


Organisation	Somerset County Council	
Title	Data Destruction Policy	
Author	Peter Grogan	
Owner	Information Governance Manager	
Protective Marking	Unclassified	

POLICY ON A PAGE

Somerset County Council will ensure all users of Council data are aware of the rules that apply to data destruction of both paper and electronic records.

This policy provides information on the types records and the methods of destruction that are within scope, the rules and guidance that must be followed, the standards to be maintained, the risk to users, clients and the Council and the potential consequences of misuse

This document will be distributed to: **All Elected Members, Somerset County Council Staff, 3rd Party Contractors, Seconded and Volunteers**

Key Messages

- All persons who use Council records must ensure their effective management and disposal, thus ensuring authenticity, accuracy, accessibility, usability, completeness, compliance, reliability, security, accountability, transparency and integrity of SCC records.
- The term “records” covers all media electronic, paper and magnetic
- All records created, captured and maintained will have a retention period assigned, so it is clear how long they should be retained and thus ensuring appropriate retention and subsequent disposal.
- All destruction of records should be adequately documented for audit, evidential and accountability purposes.
- Physical destruction of records should include all back-up copies, security copies, preservation copies and duplicate copies.
- Physical destruction should be carried out by methods appropriate to the format and security classification of the records and in a manner that preserves the confidentiality of the information they contain and prevents unauthorised access.
- Ephemeral material such as “email chatter” and office messaging should not be captured or held in records systems, but should be routinely removed and destroyed.
- The destruction and cleansing of electronic media must be carried out by the SCC ICT contractor.
- If you are unsure as to how to manage retention of Council records contact the Records Management Service.

This “policy on a page” is a summary of the detailed policy document please ensure you read, understand and comply with the full policy

Revision History

Revision Date	Revisor	Previous Version	Description of Revision
01.11.11	Andrea Binding	v.01	Initial Draft
13.03.12	Peter Grogan	v.02	Redraft & reformat
04.05.12	Peter Grogan	v.03	Electronic media
17.07.12	Peter Grogan	v.04	Logos & Unison
18.03.13	Peter Grogan	V.05	HR amendment (Appx 1)

Document Approvals

This document requires the following approvals:

Approval	Name	Date
Information Governance Manager	Peter Grogan	06.01.2012
SIRO	Richard Williams	20.03.2013
Unions / JCC	Carrie Anne Hiscock	25.02.2013
SCC HR	Richard Crouch	25.02.2013
Elected Members	David Huxtable	

Document Distribution

This document will be distributed to: **All Elected Members, Somerset County Council Staff, 3rd Party Contractors, Secondees and Volunteers.**

FULL POLICY DOCUMENT

1 Policy Statement

The Lord Chancellor's Code of Practice on the Management of Records under Section 46 of the Freedom of Information Act 2000 states "*Authorities should ensure they keep records they will need for business, regulatory, legal and accountability purposes*"¹, that "*Authorities should define how long they need to keep particular records, should dispose of them when they are no longer needed and should be able to explain why records are no longer held*"² and that "*disposal of records...should be undertaken only in accordance with clearly established policies [which] have been formally adopted by the authority[and which are enforced by] properly authorised staff*".³

ISO 15489-1:2001 states "*No disposition action should take place without the assurance that the record is no longer required, that no work is outstanding and that no litigation or investigation is current or pending which would involve relying on the record as evidence.*"⁴

The Data Protection Act requires that personal information should not be retained for longer than necessary (Principle 5) and that personal information must be kept secure (Principle 7).

Somerset County Council (SCC) is committed to the application of Retention Schedules, Codes of Practice and corporate guidelines, to ensure the timely, secure and effective disposal of information and records, in all formats, once legislative and business use has been concluded. All information and records, in all formats, will be subject to an assessment of the evidential, operational, cultural and historical value prior to destruction.

SCC will ensure every officer and elected member is aware of, and understands, their responsibilities for the timely, secure and effective disposal of council information and records.

This policy should be read and applied in conjunction with the [Records Management Policy](#), [Data Destruction Policy](#) and [Generic Retention Schedule](#).

2 Purpose

The purpose of this policy is to provide a framework for destruction of records and information created, maintained, used and held by SCC in the course of business and service delivery. Together with the Records Management Policy, Records Retention Policy and Generic Retention Schedule, the policy will ensure compliance and assist with contributing to supporting evidence of operation and decision-making relating to the retention and disposal of records within the Council.

The policy:

Provides a framework for the effective, efficient and secure disposal of records and information created, maintained, used and held by SCC.

Ensures disposal of all Council records and information is controlled, in accordance with security and confidentiality requirements.

Ensures records containing personal or sensitive data are timely and securely disposed, as required by the Data Protection Act 1998, Principles 5 and 7.

¹ Lord Chancellor's Code of Practice on the management of records, 8 – Keeping records to meet corporate requirements – p.14

² Lord Chancellor's Code of Practice on the management of records, 12 Disposal of records – p.20

³ Lord Chancellor's Code of Practice on the management of records, 12 Disposal of records – p.20

⁴ ISO 15489-1, 9.9 Implementing disposition - p.16

Ensures records are destroyed in accordance with legislative, regulatory and statutory compliance and business requirements, as stipulated in the Generic Retention Schedule, service specific retention schedules, business classification schemes and records systems.

Ensures records are authorised for disposal, by senior officers with designated responsibility and ensures all records scheduled for disposal are recorded for audit and accountability purposes.

Supports other key Council policies, such as the Records Management Policy (RMP), Records Retention Policy (RRP), Corporate Information Security Policy (CISP) and Data Protection Policy (DPP).

3 Scope

The policy applies to all Employees, Elected Members, Committees, Directorates, Services, Partners and contractual third parties and agents of the Council who create, manage and dispose of records held or processed by SCC. It stipulates their duties and responsibilities for the effective management of disposal of records, in order to comply with the policy and legislative, regulatory, financial and best practice requirements.

The policy applies to the disposal of all records, in all mediums, for all security classifications, whether retention is governed by legislation, statute, best practice or business need.

SCC undertakes a wide range of activities, with different record-keeping systems and requirements in operation. This policy aims to provide a broad framework for the effective management of disposal of records, across all directorates and activities that support service policies and procedures.

4 Definition

This document defines the framework for policy, practice and procedure to ensure the effective disposal and security of all information held by SCC.

Destruction

Destruction can be defined as:

"[The] process of eliminating or deleting records, beyond any possible reconstruction"⁵

ISO 15489-1 states:⁶

- Destruction should always be authorised
- Records subject to pending or actual litigation or investigation should not be destroyed, even if the retention period has expired
- All backup copies, security copies, preservation copies and duplicate copies of all records authorised for destruction should be destroyed at the same point time or as soon as practical afterwards

Effective destruction at the end of the retention period ensures that office and server space are not used and that costs associated with the storage and maintenance of records are no longer incurred.

⁵ ISO 15489-1, 3.8 Terms and definitions – p.2

⁶ ISO 15489-1. 9.9 Implementing disposition – p.16

Principles governing disposal decisions:

- Expiry of applicable retention rationale
- Conclusion of business use
- Whether there is pending or actual litigation or investigation
- Whether the information is subject to a Data Protection or Freedom of Information request
- Corporate, historical or research value
- Access requirements
- Confidentiality and security requirements

Due to public accountability, transparency and the public right of access to certain Council and personal information, it is vital that disposal of records is a managed process and is adequately documented.

Disposition

Disposition can be defined as:

“[The] range of processes associated with implementing records retention, destruction or transfer decisions which are documented in disposition authorities or other instruments”⁷

Disposition may include:

- Physical destruction, overwriting and deletion
- Retention for a further period of time, based on business need
- Transfer to the Records Management Service for off-site storage and management
- Transfer to an alternative storage format e.g. scanning
- Transfer to the Archives and Local Studies Service for permanent preservation

5 Risks

Somerset County Council recognises that there are risks associated with the destruction of information and records managed in order to conduct official Council business.

This policy aims to mitigate the risks. This will ensure compliance with other key record-keeping policies and legislative obligations, including the Corporate Information Security Policy (CISP), Data Protection Policy (DPP) and the Data Protection Act 1998. There are a variety of risks some of which can culminate in the Information Commissioner applying fines in excess of £500,000.

Examples of the common risks associated with data destruction are:

- Data breach
- Loss
- Theft
- Poor decision making, based on inaccurate or incomplete information
- Inconsistent or poor levels of service
- Insufficient administrative and technical controls
- Malware
- Inappropriate destruction method compromising confidentiality and security
- Lack of accountability and transparency
- Lack of business continuity

⁷ ISO 15489-1 3.8 Terms and definitions – p.3

- Loss of public reputation
- Loss of corporate memory
- Non-compliance with legislative, regulatory, financial or best practice obligations
- Premature destruction
- Excessive retention
- Inappropriate storage

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

6 The Application of the Policy

This document describes the framework for managing destruction of Council information and records within SCC.

6.1 Training and Awareness

Since all SCC officers and elected members are involved in creating, maintaining and using records, it is vital that everyone understands their responsibilities as set out in this policy.

Managers will ensure that officers responsible for authorising records for destruction are appropriately trained or experienced and that all officers understand the need for effective disposal of Council records.

The Records Management Service and the corporate Information Governance Manager will advise on methods of destruction applicable to maintain the confidentiality and security of the information to be destroyed.

6.2 Making and Implementing Disposal Decisions

Disposal decisions should be undertaken in accordance with the Records Management Policy, Records Retention Policy, Generic Retention Schedule and service specific retention schedules, which reflect retention governance rationale.

Records not already listed on Retention Schedules should be added, together with the governing rationale and retention period.

Records systems should enable routine identification of records due for disposal and records should be physically destroyed once their retention has been concluded.

Disposal decisions should reflect the current retention environment, which should be checked for current compliance and relevance prior to disposal and should be restricted to authorised officers, who are aware of retention governance.

Implementation arrangements should consider variations caused by litigation or outstanding requests for information.

All disposal decisions and physical destruction should be documented to provide an audit trail for evidential and accountability purposes.

Physical destruction should be carried out by methods appropriate to the format and security classification of the records and in a manner that preserves the confidentiality of the information

they contain and prevents unauthorised access and should include all back-up copies, security copies, preservation copies and duplicate copies.

All outsourced shredding contractors, should comply with BS 8470, the British Standard that specifies the disposal of confidential material, BS 7858, the British Standard that specifies a Code of Practice for security screening of individuals and third party individuals and be members of the United Kingdom Security Shredding Association (UKSSA).

Records for destruction should be cross-shredded. This should include anything that can identify an individual, such as an address. Shredded material should be recycled for sustainability.

6.3 Documenting Disposal Decisions

All directorates and functions of the Council should routinely document disposal of records on a Records Disposal Form (see Appendix A) that is authorised by a senior officer, thus providing audit trails and evidence of physical destruction.

Documentation should evidence that destruction took place during a managed disposal process, in accordance with established policies and retention schedules and with appropriate authorisation.

Documentation should include:

- The retention schedule reference
- The class and title of the records
- The inclusive dates of the records
- The format of the records
- Reason for destruction
- Evidence that destruction was authorised (authorised signature, email, destruction notification form)
- Evidence of method of destruction (destruction certificate issued by shredding contractor, details of who shredded on-site)
- Date of physical destruction

Destruction documentation should be kept indefinitely for audit, evidential and accountability purposes. Only destruction of those documents identified as a 'record' should be documented. There is no business need to document routine destruction of ephemeral information.

The Records Management Service has produced a list of Do's and Don'ts for effective destruction of records (see Appendix B).

6.4 Methods of Destruction

Paper records containing Council business or personal data must be made available for shredding by placing them in the bags or bins provided.

Electronic records on removable media such as CD's and memory sticks should be submitted to SWOne for secure destruction.

PCs and laptops must be returned to SWOne ICT for recycling, SWOne will ensure hard disks are cleansed or if necessary destroyed in a secure manner. For this reason Council business information and personal data must not be stored on personal devices unless SWOne have made provision by use of an encrypted SCC owned partition.

Appendix 1

Governance Arrangements

Policy Compliance

If any employee is found to have breached this policy, they may be subject to Somerset County Council's [disciplinary procedure](#).

Where it is considered that a criminal offence has potentially been committed, the Council will consider the need to refer the matter to the police.

If you do not understand the implications of this policy or how it may apply to you, seek advice from the Records Management Service or the Information Governance Team.

Policy Governance

The following table identifies who within Somerset County Council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation.
- **Informed** – the person(s) or groups to be informed after policy implementation.

Responsible	Information Governance Manager
Accountable	SIRO – Director of Business Development
Consulted	Senior Management Team, HR, Unions
Informed	All Members, employees, contractors, volunteers and 3 rd parties

7 Review and Revision

This policy will be reviewed every 12 months and, if appropriate, will be amended to maintain its relevance. Further reviews will be undertaken to reflect changes in legislation or standards.

Policy review will be undertaken by the Records Manager and Information Governance Manager.

8 References

Internal guidance on the Records Management Service is available to officers and elected members via the Intranet.

The following Council policy documents are directly relevant to this policy,

- [Corporate Information Security Policy](#)
- [Data Protection Policy](#)
- [Information Transparency Policy](#)
- [Acceptable Use Policy](#)
- [Legal Responsibility Policy](#)

Appendix A – Records Disposal Form

RECORDS MANAGEMENT SERVICE

Records Disposal Form

DIRECTORATE:		CONTACT NAME:	
SERVICE AREA:		DATE:	

CAUTION: A record cannot be destroyed if any litigation, claim, investigation, negotiation, audit, Data Protection or Freedom of Information enquiry is initiated before disposal. The record MUST be retained until completion of the action or resolution of all issues. A record cannot be destroyed unless any stipulated retention period has expired.

All records listed need to be authorised for disposal by an authorised senior officer. Senior Officer to complete tick boxes, below, and to sign form authorising disposal.

To be completed by Senior Officer:

- ☐ I certify these records are past the retention period specified on the Retention Schedule and have no further legislative, regulatory or administrative requirements.
- ☐ I certify these records are not subject to any open casework, enquiries, claims, investigation, negotiation, audits or litigation.
- ☐ I certify these records have been reviewed for extended retention and permanent preservation as historical records.
- ☐ I hereby authorise destruction of the records listed below.

Name (PRINT):		Signed:	
Job Title:		Date:	

To be completed by Administrative Staff: Please see accompanying notes for instructions on how to complete form.

Class ID	File Ref	Title / Description of Record	Date From	Date To	Volume	Format	Reason for Destruction	Destruction Method	Destruction Date

Completing the Records Disposal Form

Stages 1 and 7 – 15: to be completed by administrative staff.
Stages 2 – 6: to be completed by Senior Officer.

- 1 Insert your Directorate, Service Area, Contact Name and Date.
- 2 Senior Officer to tick the box to confirm the records are past their specified retention period, as stated on the Retention Schedule.
- 3 Senior Officer to tick the box to confirm the records are not subject to any open casework, claims, enquiries, audits or legislation.
- 4 Senior Officer to tick the box to confirm the records have been reviewed for extended retention and permanent preservation as historical records (if in doubt contact the Records Management Service or Somerset Archives and Local Studies Service).
- 5 Senior Officer to tick the box to authorise destruction.
- 6 Senior Officer to insert their name, job title, date and to sign form.
- 7 **Class ID:** Insert appropriate Class ID from your Retention Schedule. This is the identifier for the category of record.
- 8 **File Ref:** Insert any internal file reference that has been allocated to the record within your office. If no reference has been allocated leave box blank.
- 9 **Title / Description of Record:** Insert the file title and if appropriate any other applicable information relating to the file. Do not list files as 'Files A-Z', 'Miscellaneous files', 'John's files', etc. List each file individually.
- 10 **Date From / Date To:** Insert the dates the record was created and closed.
- 11 **Volume:** Insert number of volumes.
- 12 **Format:** Insert either 'paper', 'electronic', 'photograph, or other applicable format.
- 13 **Reason for Destruction:** Insert 'In accordance with Retention Schedule' or other appropriate reason.
- 14 **Destruction Method:** Insert either 'shredded in office', 'shredded by contractor', 'ordinary recycling waste', etc. The Records Management Service recommends shredding to safeguard confidentiality and security of information.
- 15 **Destruction Date:** Insert actual date of destruction or date waste collected by shredding contractor.

Appendix B – **Destruction of Records**

Do

- ✓ Ensure all records have an appropriate retention period and are listed on your Retention Schedule.
- ✓ Destroy records as soon as they cease to be required.
- ✓ Operate periodic file housekeeping – destroy records that can be destroyed, keep in office any that are still current and retain/archive any that are 'dormant'.
- ✓ Check records are no longer needed before destruction. Ask yourself "is it past its disposal date, do I need to keep it for legal reasons, has the case re-opened, is there an investigation, litigation, or public request for information"?
- ✓ Destroy confidential records by shredding.
- ✓ Destroy non-confidential records by putting into recycling sacks.
- ✓ Arrange shredding/recycling in plenty of time.
- ✓ Complete a Records Disposal Form, listing destroyed records, for audit purposes.
- ✓ Authorise destruction of records held by the Records Management Service as soon as you receive notification.
- ✓ Update your consignment lists, filing lists, databases, etc when records are destroyed.
- ✓ Consider any possible archival value, i.e. for research or historical purposes. If so, contact the Archives and Local Studies Service on 01823 278805.

Don't

- ✗ Destroy records unless you have checked with the Records Manager and/or your Line Manager and ensured there are no specific reasons for further retention.
- ✗ Keep records for longer than necessary. This will increase storage and management costs and could also result in breach of legislation, such as The Data Protection Act (i.e. keeping personal data for longer than necessary).
- ✗ Destroy records if they are part of an on-going investigation and are needed for evidence, e.g. Freedom of Information or Data Protection request, legal case, investigation, etc.
- ✗ Dispose of records in ordinary waste – ensure confidential records are shredded and non-confidential records are put in recycling sacks.
- ✗ Leave confidential shredding in public areas.