

# 2009

## Records Management Policy



### Policy Overview

The purpose of this policy is to outline the framework for implementing the records management standard ISO15489 and the roles and responsibilities employees have in ensuring that the council's information is managed efficiently.

**Version 2.0**

# Version Control

**Title:** Corporate Records Management Policy  
**Version Number:** 2.0  
**Version Type:** Final  
**Author:** Dawn Waller, Corporate Records Manager  
**Issue Date:** 19 October 2009  
**Approved By:** Approved  
**Document Review Date:** July 2012  
**Circulation:** All staff

## Amendment History

| Version   | Date                            | Author   | Comment   |
|-----------|---------------------------------|--|---|
| 0.1 – 0.5 | 24 February 2006 – 20 June 2006 | Dawn Waller,<br>Corporate Records Manager                |   |
| 1.0       | 11 September 2006               | Dawn Waller,<br>Corporate Records Manager                | Approved by Operational Management Team   |
| 1.1       | 7 July 2009                     | Dawn Waller,<br>Corporate Records Manager                | Amended in line with recent updates in records management guidance including Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000   |
| 1.2       | 13 October 2009                 | Andrew Shipway, Corporate Information Governance Manager | <p><b>Circulated to:</b></p> <ul style="list-style-type: none"> <li>• Philip Lloyd Williams Director of Corporate Governance,</li> <li>• Deborah Merry Democratic Services Manager,</li> <li>• Alan Haycock Information Governance Manager (Solihull Care Trust),</li> <li>• Kath Keating HR Business Partner,</li> <li>• Liz Welton Head of Procurement,</li> <li>• David Butt Information Strategy Manager,</li> <li>• Steve Fenton Business &amp; Performance Manager,</li> <li>• Penny Davison Business Analyst,</li> <li>• Deborah Martin-Williams Head of Communications,</li> <li>• Gordon Smith Audit Manager (Operational Audit),</li> <li>• Steve Halliday Head of ICT,</li> <li>• Stephanie Gardner Governance and Risk Management Officer,</li> <li>• Neil Pearson Financial Manager - Treasury Mgt &amp; Insurance,</li> <li>• Peter Hobbs Information Governance Officer,</li> <li>• Michael Enderby Emergency Planning Manager,</li> <li>• Melanie Lockey Head of Partnership Commissioning.</li> </ul> <p>Updated to reflect any feedback received.</p> |
| 2.0       | 19 October 2009                 | Operational Leadership Team                              | Approved by OLT   |

# Contents

|   |    |
|---|----|
| <b>1. Purpose</b> .....   | 5  |
| <b>2. Scope</b> .....   | 5  |
| 2.1 What is a record?.....  | 5  |
| 2.2 What media is covered? .....  | 5  |
| 2.3 Who does this policy apply to? .....  | 6  |
| 2.4 What sort of information is not covered?.....   | 6  |
| 2.5 Other relevant legislation & standards .....  | 7  |
| <b>3. Why is Records Management Important?</b> .....  | 8  |
| 3.2 The organisation benefits from.....   | 8  |
| 3.3 Partnerships benefits from.....   | 8  |
| 3.4 The external customer benefits from .....   | 8  |
| <b>4. Policy Statement</b> .....  | 9  |
| <b>5. Responsibilities</b> .....  | 10 |
| 5.1 Corporate, Service Directors and Heads of Service.....  | 10 |
| 5.2 Corporate Records Manager (CRM) .....   | 10 |
| 5.3 Individual Employees & Elected Members.....   | 11 |
| 5.4 Records Management Lead Officers .....  | 12 |
| 5.5 Internal Audit.....   | 12 |
| 5.6 Legal Services.....   | 12 |
| 5.7 ICT .....   | 12 |
| 5.8 Working Groups.....   | 13 |
| 5.9 Schools.....  | 13 |
| 5.10 Partnerships/Organisations (where the Council wholly owns the records, e.g. Solihull<br>Community Housing) ..... | 13 |
| 5.11 Partnerships/Organisations (where ownership of the records is jointly held, e.g. Solihull Care<br>Trust).....    | 13 |
| 5.12 Home Workers.....  | 14 |
| 5.13 Monitor & Review .....   | 14 |

|   |    |
|---|----|
| <b>6. Principles of Good Records Management</b> ..... | 15 |
| 6.1 Accountability.....                               | 15 |
| 6.11 Governance.....                                  | 15 |
| 6.12 Risk Management .....                            | 15 |
| 6.13 Responsibility.....                              | 16 |
| 6.14 Partnerships.....                                | 16 |
| 6.2 Integrity .....                                   | 16 |
| 6.3 Protection .....                                  | 17 |
| 6.31 Security and Access.....                         | 17 |
| 6.32 Storage.....                                     | 17 |
| 6.33 Critical Records .....                           | 18 |
| 6.34 Business Recovery .....                          | 18 |
| 6.4 Compliance .....                                  | 18 |
| 6.5 Availability .....                                | 19 |
| 6.51 Readability .....                                | 19 |
| 6.52 Ownership.....                                   | 19 |
| 6.53 Digital Continuity .....                         | 19 |
| 6.54 Traceability .....                               | 19 |
| 6.55 Business Continuity.....                         | 20 |
| 6.6 Retention .....                                   | 20 |
| 6.7 Disposal.....                                     | 20 |

# 1. Purpose

Solihull MBC recognises that the efficient management of its records is essential to support its core functions, to comply with its legal and regulatory obligations and to contribute to the effective overall management of the Council.

The purpose of this policy is to outline the framework for implementing the records management standard ISO15489 and the roles and responsibilities employees have in ensuring that the Council's records are managed efficiently.

## 2. Scope

### 2.1 What is a record?

Within this policy, the word "record" means any information created, received and maintained as evidence and/or information in pursuance of legal obligations or in the transaction of business (regardless of format). For example,

- Information relating to the approval/authorisation of actions.
- Business communications between staff or external recipients.
- Detail policy change or development.
- Relate to significant projects/activities.
- Contain advice/guidance.
- Relate to business decisions including contributory emails.

### 2.2 What media is covered?

This policy covers all information (from creation to disposal) regardless of the format or media it is held in, for example it will include:

- Paper.
- Microfilm/fiche.
- Faxes.
- Emails.
- Information created digitally.
- Scanned Images.
- Website contents.
- Business & information systems.

## 2.3 Who does this policy apply to?

This policy applies to all records created, received, maintained or disposed by or on behalf of the Council. Typically, therefore, it will apply to the following groups.

- All council employees including temporary and contracted employees.
- All employees of organisations holding records on behalf of the Council but is restricted to only those records in which the Council has a vested interest.
- All elected members who hold records relating to the business of the Council.
- Solihull Community Housing (Housing records only).
- Partnership organisations.
- Records held by Schools.
- Adult Social Service Records (Case files only).
- Contractors.

For ease of reading, all these groups are referred to as 'employees' throughout this policy

## 2.4 What sort of information is not covered?

Records are not:

- Published or reference materials from external organisations (including Trade/business journals, catalogues).
- Transmission documents – fax receipts, telephone messages unless they form part of a record.
- Message slips.
- Duplicated documents (provided the original copyholder retains the original for the full retention period).
- Personal diaries, address books provided no business information is contained within.
- Out-of-date distribution lists.
- Junk mail.
- Blank/template forms.
- Personal emails unless they form part of a business email.
- External information sent FYI only.
- Working papers which contribute to an official document but which are not required to support the document.
- Draft emails.

## 2.5 Other relevant legislation & standards

- The principal legislation affecting the management of records within local government are:
  - a) Freedom of Information Act 2000.
  - b) Data Protection Act 1998.
  - c) Local Government Act 1972.
  - d) Limitation Act 1980.
- The Local Government Act places responsibilities on councils to make provision for the care of their records whilst the Lord Chancellors Code of Practice issued under section 46 of the Freedom of Information Act requires the implementation of the good and effective records management practices.
- This policy must be read in conjunction with the following Council policies.
  - a) A Protocol for Partnerships.
  - b) Business Recovery Plans.
  - c) Data Protection Act 1998 - Code of Practice for Employees of the Council.
  - d) Electronic Communications Policy.
  - e) Freedom of Information Policy and Operational Manual.
  - f) Information Quality SORP12.
  - g) Information Security Policy.
  - h) Information Sharing Code of Practice.
  - i) IT Backup Policy.
  - j) Portable ICT Equipment Policy.
  - k) Premises Security Policy and Guidance.

## 3. Why is Records Management Important?

The management of records is critical to the success of any organisation. Without records, the Council could not take confident decisions based on fact, services would not be provided to our customers and with partners and legislative compliance would not be possible. Good records management practice benefits all stakeholders.

### 3.1 Employees and other internal users benefits from

- Reliable, comprehensive and accurate information being available.
- Improvement of service delivery through information sharing, quicker access to information.
- Clear audit trail of decisions taken and actions occurring.
- Less duplication of information.
- Quicker and easier to locate the right information, at the right time.

### 3.2 The organisation benefits from

- Decrease in health and safety issues linked to excessive office storage.
- Operational efficiencies through freeing of office space for uses other than storage and reduced costs due to less duplication of information
- Positive impact on the Council's 'Carbon Footprint'.
- Protection of rights and interests.
- Less time spent seeking, retrieving and copying information.
- Legislative and regulatory compliance through ensuring the timely and appropriate disposal of records.
- Identification and protection of critical records.
- Improved risk management.
- Identifying those records which will create corporate memory for future generations.
- Improved overall performance.

### 3.3 Partnerships benefits from

- Accurate information being available when required and in the correct format.
- Improved mechanisms for sharing of information.

### 3.4 The external customer benefits from

- Protection of rights and interests.
- Improved service delivery.
- More accurate information existing.
- Transparency of decisions taken and a full accountability trail will exist.
- Increased trust in the organisation.

## 4. Policy Statement

The Council is committed to implementing efficient records management across the organisation to ensure that records:

- Are authentic, reliable, protected against unauthorised alteration, comply with regulatory and other business needs and remain accessible to those that need to use them for as long as they are required.
- Can be retrieved accurately and quickly to aid decision-making and increase management effectiveness.
- Are managed cost effectively, avoid unnecessary duplication and are retained only as long as required as defined in the Corporate Retention Schedule or similar guidance issued by the Corporate Records Manager.
- Having regard to the state of technical development and the cost of implementing any measures, records will be held securely to ensure a level of security appropriate to the type of information being processed and also to the harm that might result from unauthorised or unlawful processing, or loss, destruction or damage.
- Vital to the Council's business are identified and protected
- That are no longer current will be stored cheaply, retrieved promptly, reviewed and disposed of only in accordance with a defined approval process<sup>1</sup>.
- Worthy of permanent preservation as archives are identified as early as possible and preserved in appropriate archives.

All employees (including temporary, agency and contractors) have a responsibility to ensure that all physical or electronic information created, or received complies with section 5.

---

<sup>1</sup> Principles taken from the ARMA standard (ARMA develops and publishes standards and guidelines related to records management. It was a key contributor to the international records management standard, ISO-15489).

## 5. Responsibilities

The responsibility for the management of records lies with all employees although some employees will have additional responsibility. The responsibilities of employees are outlined below:

### 5.1 Directors and Heads of Service

- Support the overall records management programme of work by ensuring that their business areas participate in the project and ensure that resources are available for the implementation of records management.
- Nominate a person within the business area with responsibility for implementing relevant records management policy and guidance (Records Management Lead Officer (RMLO)). The Corporate Records Manager should be notified when a RMLO is replaced.
- Implement an annual review of records to ensure that information is destroyed (in accordance with the current retention schedule) when required in an appropriate manner.
- To approve the destruction of records when requested to do so by the Corporate Records Manager.
- Ensure that staff have necessary knowledge and skills to manage records and to request training and/or advice where appropriate.
- Agree and regularly review, in conjunction with the Corporate Records Manager, the measures through which the performance of records management within the business area will be measured.
- Ensure that records are held in safe, secure locations at all times and that appropriate security measures are applied.
- Approve payments for the recovery of damaged records where necessary.

### 5.2 Corporate Records Manager (CRM)

- Responsible for issuing and communicating advice, guidance and support to help enable The Council to meet all its legal responsibilities through:
  - a) Developing, maintaining and the revision of guidance relating to all records management issues.
  - b) Create and maintain records management tools required to organise and manage records effectively.
  - c) Preserve records through business continuity, recovery, digital sustainability and for historical use. Additionally facilitate the document recovery contract, maintain a critical records list to enable business continuity.
  - d) Facilitate the transfer and storage of records offsite.
  - e) Provision of advice and training on all matters relating to all record keeping matters.
  - f) Supporting business areas in implementing record keeping systems.
  - g) Performance monitoring of record keeping systems.

- h) To hold information relating to all records and record keeping systems throughout the organisation (including critical records).
- i) Co-ordinating work of the Records Management Lead Officers and Business Continuity Leads.
- j) Providing advice and guidance to Care Trust to safeguard records that the Council has a vested interest in.
- k) Administration of the Electronic Document Records Management System (EDRMS) where implemented.
- l) Provision of training.
- m) Supporting business areas in implementing records management systems.
- n) To activate the document recovery contract in accordance with the agreed plan.

### 5.3 Individual Employees & Elected Members

- To adopt and implement guidance issued by the Corporate Records Manager.
- Employees must ensure that all records created are a true and accurate representation of the activities occurring. Records must be filed appropriately and retained then disposed of in accordance with the guidance issued. Care should be taken to ensure that all information (confidential or otherwise, paper or electronic) is disposed of appropriately.
- Metadata (descriptive information about the record describing context, content and structure of records) must be applied consistently and accurately.
- To consult with the Corporate Records Manager on all major projects affecting records management particularly data conversion (digitising, microfilming etc), migration (converting an electronic record from one format to another) and long term preservation (maintenance of records during their lifetime).
- To ensure that records are stored in conditions which will ensure their long term survival.
- To further ensure that all records remain accessible and secure (according to the confidentiality imposed on the record) for the duration of their business use and once the business use has concluded, dispose of the records according to the retention schedule.
- Where necessary procedures should be put in place to control access to records.
- If amendments are required to the retention schedule(s) then the Corporate Records Manager must be notified as soon as possible.
- To bring to the Corporate Records Manager's attention any records which are marked within the retention schedule as "Transfer to archives" or "Offer to archives" or which could be judged to be of historical significance.

## 5.4 Records Management Lead Officers

- To undertake information audits.
- To contribute to consultation on the file plan, retention schedule and related records management issues.
- Identifying new record types and those which cease to exist, informing the Corporate Records Manager as appropriate.
- Reviewing annually, the records due for disposal or transfer offsite and to arrange their disposal.
- Risk assessing business areas at regular intervals.
- Identifying records at risk of obsolescence, damage (actual or potential) or other factors which affect the longevity of the record.
- Testing the shared network file plan.
- Approving additions/deletions from the shared network file plan.
- Monitoring use of shared network file plan.
- Undertaking an annual review of the critical records listing.
- Analysis of performance monitoring.
- To disseminate information on behalf of the Corporate Records Manager.
- To advise the Corporate Records Manager of new, closed and transferred records.
- To support the local administration of the shared network file plan within the business area through:
- Controlling and monitoring the file structure implemented within the business area.

## 5.5 Internal Audit

- To audit the implementation of records management across the organisation.

## 5.6 Legal Services

- To approve all retention schedules.
- To offer legal advice to business areas who are considering digitising records about the need/importance of compliance with BSI 10008:2008 (the evidential weight and legal admissibility of electronic records).
- To advise on the destruction of digitised records prior to the expiry of their retention period.

## 5.7 ICT

- To provide technical support for the EDRMs.
- To advise the Corporate Records Manager of obsolete software where identified.
- To advise the Corporate Records Manager where upgrades to software and hardware or implementations of new software are occurring.
- To provide monitoring information relating the use of email and network systems.

## 5.8 Working Groups

- Temporary groups will be created to review and approve the retention schedules, file plans and any other necessary documentation after the completion of the information audit. These will be dissolved upon the implementation of records management and liaison will occur between the Corporate Records Manager and Records Management Lead Officer only.

## 5.9 Schools

- To liaise with the Corporate Records Manager when a school closure is announced.
- To use the corporate offsite storage contract.
- To adopt and implement the corporate guidance available on the intranet.

## 5.10 Partnerships/Organisations (where the Council wholly owns the records, e.g. Solihull Community Housing)

- To consult with the Corporate Records Manager on all major projects affecting records management particularly data conversion (digitising, microfilming etc), migration (converting an electronic record from one format to another) and long term preservation (maintenance of records during their lifetime).
- To adopt guidance issued by the Corporate Records Manager for records in which the Council has an interest only. The Partnership/Organisation should create and adopt their own internal guidance for records which they own.
- To ensure that records are stored in conditions which will ensure their long term survival. If records are to be moved into offsite storage then the Corporate Records Manager should be consulted before they are moved and details provided to the Corporate Records Manager of which records are stored offsite accompanied by the procedures for storage and retrieval of the records.
- To seek the authorisation of the Corporate Records Manager before destroying any records belonging to the Council.

## 5.11 Partnerships/Organisations (where ownership of the records is jointly held, e.g. Solihull Care Trust)

- Where responsibility for the day to day use and maintenance of records has been legally delegated to another organisation the Council will want to ensure that the organisation has records management policy, procedure and training equivalent to that of the Council. The Corporate Records Manager will be responsible for monitoring the management of all records that the Council has a vested interest in and that are being managed on behalf of the Council.
- To seek the authorisation of the Corporate Records Manager before destroying any records belonging to the Council.

## 5.12 Home Workers

- All employees working from their home or other non-office based location have a duty to ensure that:
  - a) All records are held securely when travelling or when at home.
  - b) Access to the records is restricted.
  - c) Records are held on computer hardware supplied by the Council with appropriate virus/firewall software, business area fileplan and VPN installed.
  - d) Records must be transferred to the network each evening via the VPN network.
  - e) Reasonable measures are taken to prevent the loss or alteration of records.
  - f) Records are returned to the Council when the employee leaves their role either temporarily or permanently.
  - g) Information should be transferred via secure means.
  - h) Where home computers are used, sufficient protection is required to ensure the security of information held and transmitted.

## 5.13 Monitor & Review

- This policy will be reviewed in September 2012 or following major organisational or technical changes (whichever is the sooner).
- Individual offices should review and update their own internal record keeping policies and procedures on a regular basis.
  - a) The regular review of information gathered during the records management project.
  - b) Reviews of the risks identified during the records management project.
  - c) Monitoring by internal audit
  - d) Monitoring of performance indicators.

## 6. Principles of Good Records Management

### 6.1 Accountability

#### 6.11 Governance

- Senior responsibility for the records management programme has been assigned to the Head of Corporate Performance Policy and Information (CPPID).
- Operational responsibility for Records Management lies with the Corporate Records Manager.
- The Corporate Records Manager will report to the Records Management Project Board bi-monthly and to the Operational Management Team twice yearly. The Records Management Project Board consists of the following permanent members:
  - a) Head of Corporate Performance, Policy & Information.
  - b) Corporate Information Governance Manager.
  - c) Corporate Records Manager.

Additional members of this board will include representatives from business areas where records management is being implemented. These representatives will be temporary members of the project board from the start of the records management project to its conclusion.

- Business areas may be required to nominate representatives to help the Corporate Records Manager implement records management within their business areas.
- All employees are responsible for ensuring good records management and to help achieve this, records management is to be added to all job descriptions. The employee responsibilities are outlined within this policy.

#### 6.12 Risk Management

- Information is a corporate asset and so records management will be incorporated into the corporate risk management framework through the inclusion of a records management risk on each divisional risk register and regular monitoring of risks by risk owners and internal audit.
- Information Audit reports generated by the Records Management Project will be submitted to Internal Audit to allow the continued monitoring of issues.
- Key performance indicators will be identified for those areas where full records management has been implemented. These can be measured by random visits, formal monitoring or interviews and will be measured on a regular basis.

### 6.13 Responsibility

- The responsibilities of all employees are outlined within this policy.

### 6.14 Partnerships

- Each partnership should ensure that information is shared in line with the guidance and standards outlined in the Council's Code of Practice on Sharing Information and that it is clear:
  - a) Which party is contributing and retaining information.
  - b) How security is to be applied.
  - c) How Data Quality will be maintained.
  - d) Who the information will be shared with and which employees should have access.
  - e) What the disposal arrangements are.
- Should the partnership end then clear rules must exist regarding the retention of information.

## 6.2 Integrity

- A record should correctly reflect what was communicated or decided or what action was taken. It should also be able to support the needs of (have a useful purpose in) the business to which it relates and be used for accountability purposes. For example, minutes should provide an accurate record of the decisions taken at a meeting.
- Record keeping systems (electronic and manual) must be proven to be reliable and the information held within such systems must be authentic otherwise evidential value will be compromised. Additional consideration should be given to information which may need extra controls to prove legal admissibility under BS 10008:2008.
- Particular consideration must be given to records management issues when:
  - a) Planning or implementing ICT systems.
  - b) Organisational restructures occur.
  - c) Partnerships are formed.
  - d) Implementing new technologies.

## 6.3 Protection

- All records (electronic and physical) should be protected from damage and unauthorised access. Additionally their identity and location must be known. Critical records in particular should be identified and granted additional safeguards.

### 6.31 Security and Access

- Corporate information security policies must be complied with. When applying security the business area must consider:
  - a) Whether the information should be shared with others. If so whom?
  - b) The level of protection required.
  - c) Whether the information needs to be protectively marked (e.g. RESTRICTED or PROTECT).
  - d) The use of encrypted email or secure connections to transmit and receive electronic information from external sources.
  - e) How best to safeguard physical information during transit.

### 6.32 Storage

- Each business area must know what information they hold and where it is held. If necessary tracking systems should be implemented to ensure this.
- When selecting a storage area or filing system, the business area must consider:
  - a) Whether the physical storage area will be shared with other business areas. If so, additional security measures may be required.
  - b) The minimum standards of storage required. For the majority of cases the corporate minimum storage standards will apply but some information (e.g. adoption information) must be stored under additional, external standards.
  - c) The easy retrieval of information.
- Information must be stored on the network or in a manual filing systems. Electronic information must not be retained solely on memory sticks, CD's, DVD's or other removal media.
- Business information should not be kept solely within emails or confidential personal areas. It should be stored on the network so that staff with a business need can access the information. The danger of storing it solely in emails is that access is restricted to the email recipient and there are inherent dangers associated with this such as important information being restricted and controlled by just one person or important information (emails) being deleted when that person leaves. Guidance relating to the management of emails is available on the intranet.
- Information stored in offsite storage will comply with the required storage standards and must be checked on a regular basis to ensure that the information remains available.

### 6.33 Critical Records

- Critical records must be identified and protected

### 6.34 Business Recovery

- Should records suffer damage then the business area must undertake a risk assessment to assess whether restoration of the records would benefit the business. The Corporate Records Manager or Emergency Planning Manager can offer advice on the process for restoring records.

## 6.4 Compliance

- Compliance with corporate policies, legislative and regulations must be achieved to ensure that information is adequate to support the business.
- The creation of records should not be selective. Records need to be created for all aspects of the Council's operations and transactions for which a requirement for evidence exists. It is particularly important that all statutory records are created. Records must not be created or held for unknown reasons.
- Each business area needs to decide which records they should create based on which records are needed to support their business area and the risks involved in not having the record available.
- All employees must ensure that they know which records need to be created, the information they should contain, which should be retained and for how long.
- All employees have a responsibility to create records to document for example:
  - a) Decisions.
  - b) Oral decisions and commitments, including telephone discussions.
  - c) Meetings.
  - d) Other events.
  - e) Operation of outsourced or contracted functions.
- Records of a business activity should be complete and accurate enough to allow employees and their successors to appropriately fulfil their responsibilities, to:
  - a) Facilitate an audit or examination by the appropriate regulatory authority.
  - b) Protect the legal and other rights of the Council, its clients and any other person affected by its actions.
  - c) Provide authenticity of the records so that they can be shown to be credible and authoritative as evidence.
- Record keeping must comply with all corporate, regulatory and legislative standards. If particular information must be accurate, comprehensive and complete.
- The corporate Information Quality standard outlined in SORP 12 must be adopted.

## 6.5 Availability

- Care must be taken by the business area to ensure that all information (physical or electronic) remains available for the duration of the information lifecycle.

### 6.51 Readability

- Should electronic information become obsolete through any of the following events, the business area must contact the Corporate Records Manager for advice:
  - a) Support ending for file formats.
  - b) Support ending for software versions.
  - c) Software being superseded by newer versions.
  - d) Computer technology being superseded by newer technology.
  - e) Storage mediums being superseded.
  - f) Appearance, merging and disappearance of vendors.
  - g) Discontinuation of hardware devices e.g. 5 ½ inch drives, floppy drives.
  - h) Creation of new media types.

### 6.52 Ownership

- All records created, held or retained by Council employees whilst carrying out their corporate functions remain the property of the Council. If an employee leaves their role (either temporarily or permanently) all records must be left in a suitable condition and remain accessible for others who have a valid business reason for accessing them. They must not remain in the possession of the employee.
- Any given to third parties such as contractors, suppliers, partnerships and other organisations or created by third parties on the Council's behalf remain the property of the Council.

### 6.53 Digital Continuity

- The business area must carefully manage and monitor the migration of information between systems to ensure the availability and integrity of information.
- Risks to the information from accidental alteration must be assessed before implementing new technologies. Where necessary safeguards must be implemented to protect the information.
- All backup copies of information must be kept securely in an offsite location.
- Any information held in offline storage must be checked regularly to ensure that the medium is not degrading.

### 6.54 Traceability

- All records must be locatable when required. Where records are loaned to other business areas it will be necessary to implement a tracking system.
- Records should be filed and named in accordance with the corporate guidance.

### 6.55 Business Continuity

- Critical information must be identified and adequate safeguards applied.
- Details of all critical information must be included in the business continuity plans.
- A disaster recovery contract has been agreed under which the Council and schools can recover damaged information.

## 6.6 Retention

- All records must be retained in accordance with the retention schedule and related corporate policies.
- If amendments are required to the retention schedule(s) then the Corporate Records Manager must be notified as soon as possible.

## 6.7 Disposal

- Details about which records should be retained and for how long is held within the retention schedules available on the intranet. The schedules also note who the original record holder is. Records should be disposed of as soon as the business use has ended and in accordance with the retention schedule. Their disposal should be noted to within the disposal register to ensure that the business area knows which records are no longer retained. Disposing of records appropriately ensures that legal/regulatory duties are met, that the use office/server space is maximised and costs incurring in maintaining information is minimised.
- Records should only be kept beyond the retention period in the following circumstances:
  - a) The record is still of business use.
  - b) Legislation affecting the record has changed since the creation of the record.

*(If (a) or (b) apply then the Corporate Records Manager must be informed as such a decision may need to be reflected in the corporate retention schedules).*

- c) The record is required for historical preservation

*(If (c) applies then the record must be passed to the Corporate Records Manager after the completion of the relevant paperwork.)*

- d) The record is (or recently has been) subject to a freedom of information or other request.

*(If (d) applies then the record must be retained until the request processes (including appeals) have been completed and an additional six months have elapsed).*

- e) The record is required in a litigation case.

*(If (e) applies then retain until the conclusion of litigation and associated processes then contact the Corporate Records Manager for advice).*

- No original records can be destroyed before the end of their retention period without the completion of a risk assessment and prior approval of the Corporate Records Manager and Legal Services.
- A disposal register should be kept indicating when each record was disposed of and who authorised the disposal. Such a register will help prove that records were not destroyed in order to prevent disclosure. Within electronic systems an audit trail could hold this information.
- Each business area must implement an annual review to assess and dispose of any unnecessary information.
- When records are disposed of by a third party provider, a destruction certificate should be received following the act of destruction occurring.
- The retention schedules will be agreed by the Corporate Records Manager, the business area then approved by the Head of Service. Final approval will be given by Legal Services. Each schedule will clearly identify the record held, length of time it is to be held for, the authorisation for disposal and the disposal action. Additionally the function of the record will be recorded and the original copyholder.
- Each schedule will be reviewed by all parties every 3 years. Previous schedules will be retained to prove previous guidelines enforced.
- Where records have been missed from the schedule, it is the responsibility of the business area to notify the Corporate Records Manager who will arrange for the information to be audited and included in the schedule.
- Records should be disposed of in accordance with their confidentiality level. All copies of a record should be disposed of at the same time.
- Information selected for permanent preservation within the archives should be transferred to the Local Studies section. During the transfer to archives the information should be transported with the correct level of security applied.