DURHAM COUNTY COUNCIL

CORPORATE RECORDS MANAGEMENT POLICY

Version 3.0 **February 2015**

Table of Contents

Durham County Council

Corporate Records Management Policy

1. Purpose

The Records Management Policy aims to ensure that full and accurate records of all activities and decisions of Durham County Council (hereinafter referred to as 'the Council') are created, managed and retained or disposed of appropriately, and in accordance with legal obligations and professional standards.

In the event of a crisis such as a building fire of flood, information is of critical importance and value to all parts of the organisation. Those within the Council with responsibility for managing and protecting this vital asset have a central role to play in ensuring that the right processes are in place so that the impact of any disruption to the Council, whether natural or man-made will be minimised.

Information is essential to today's society. Within the Council information can take many forms, from data sets of confidential personal information through to records of sensitive meetings, personnel records, policy recommendations, correspondence, case files and historical records. Information can be in many formats, from databases through to emails, paper and video. Information is not the same as IT, IT systems are the platforms on which information is often exchanged and managed.

Risk Management is based on the uncertainty of the outcome, and good risk management allows an organisation to:

- Have increased confidence in achieving its desired outcomes;
- Effectively constrain threats to acceptable levels;
- Take informed decisions about future opportunities.

There are also risks to not sharing personal data appropriately, and of not keeping sufficiently accurate records, such as in the case of Victoria Climbie.

Business Continuity strategy is required to identify key information needed to keep the Council running. Tested business continuity plans, and simulation exercises which address critical data should be in place, with back-ups of information held in a secure, separate location. When Hurricane Katrina hit the Gulf Coast of the US in 2005 the lessons learned report highlighted that the Disaster Recovery Centres did not provide a single-point of access to apply for aid as staff did not have access to information on all programmes required.

Checklist for Assessing Risk to Paper and Electronic Records
(Appendix A)

2. Background

2.1 Council records are part of the corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations. They support policy formation and managerial decision-making, protect the interests of the Council and the rights of service users, staff and members of the public who have dealings with the Council.

2.2 Records support consistency, continuity, efficiency and productivity, and help the Council to deliver our services in consistent and equitable ways.

2.3 Records management, through the proper control of the content, storage and volume of records, reduces vulnerability to legal challenge or financial loss and promotes best value in terms of human and space resources through greater control of information and storage systems.

2.4 The records of the Council are an important public asset (see Appendix B for record types) such as:

- Current records – used daily;
- Semi-current records – which need to be kept for a defined period;
- Archival records – no longer have a business use but need to be kept permanently.

The management of them is essential to the Council's efficient operation.

3. Legislative Arena

3.1 Records, especially the retention of records, are covered by a variety of legislation, national standards and codes of practices. The following are an indicative, but not exhaustive, list of the legislation relating to records management:

- Freedom of Information 2000;
- Data Protection 1998;
- Environmental Information Regulations 2004;
- Local Government Act 1972;
- Limitation Act 1980;
- ISO 15489 (Parts 1 and 2) Best practice in Records Management;
- ISO 17799 Information Security Management;
- Lord Chancellor's Code of Practice S.46 of the FOIA 2000;
- Retention Guidelines for Local Authorities 2003:1.

Services will have specific Legislation for their own service area such as:

- CAS – Adoption records;
- Health and Safety – Asbestos records;
- Planning – Planning files.

(This list is not exhaustive)

4. Scope

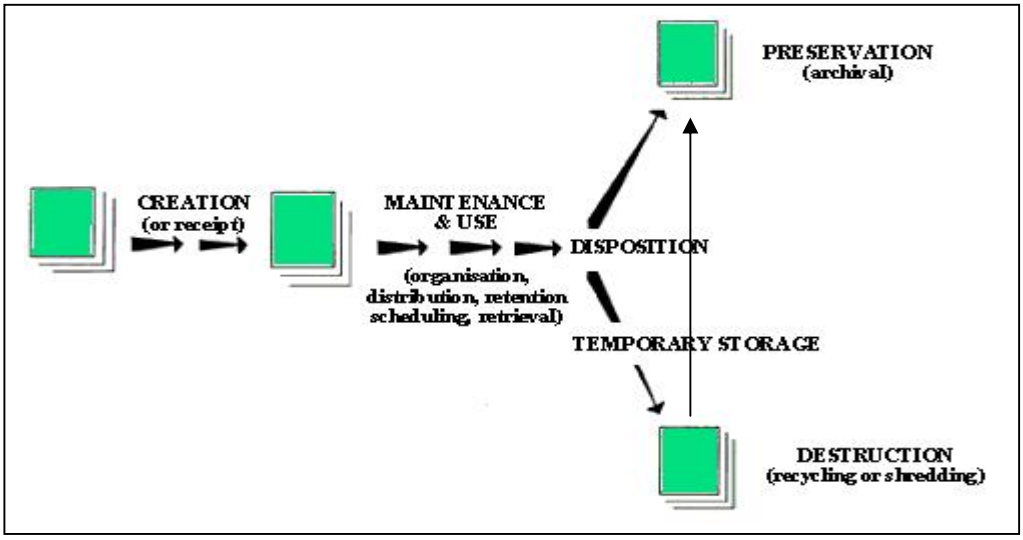
4.1 This policy encompasses all records and documents created by the Council. The policy covers paper and electronic records, although currently we do not capture social media records. The National Archives have recently developed guidance on the archiving of Social Media for Government records.

4.2 The policy applies to all records made and kept, or received and kept, by any person including permanent, temporary, casual, graduate, consultant, trainee, contract or work experience staff, third party providers of services in the course of the exercise of official functions for any purpose. The policy applies throughout the life cycle of records. That means the policy covers the time from when a document or record is created within the Council to the time it is either destroyed or preserved permanently within the County Record Office.

The stages of records, known as the lifecycle (shown below) are:

- Create or receive information in the form of records;
- Classify records into a logical system by use of a fileplan;
- Maintain and use the records;
- Destroy or archive records in line with retention guidelines.

Diagram of the Lifecycle of Information



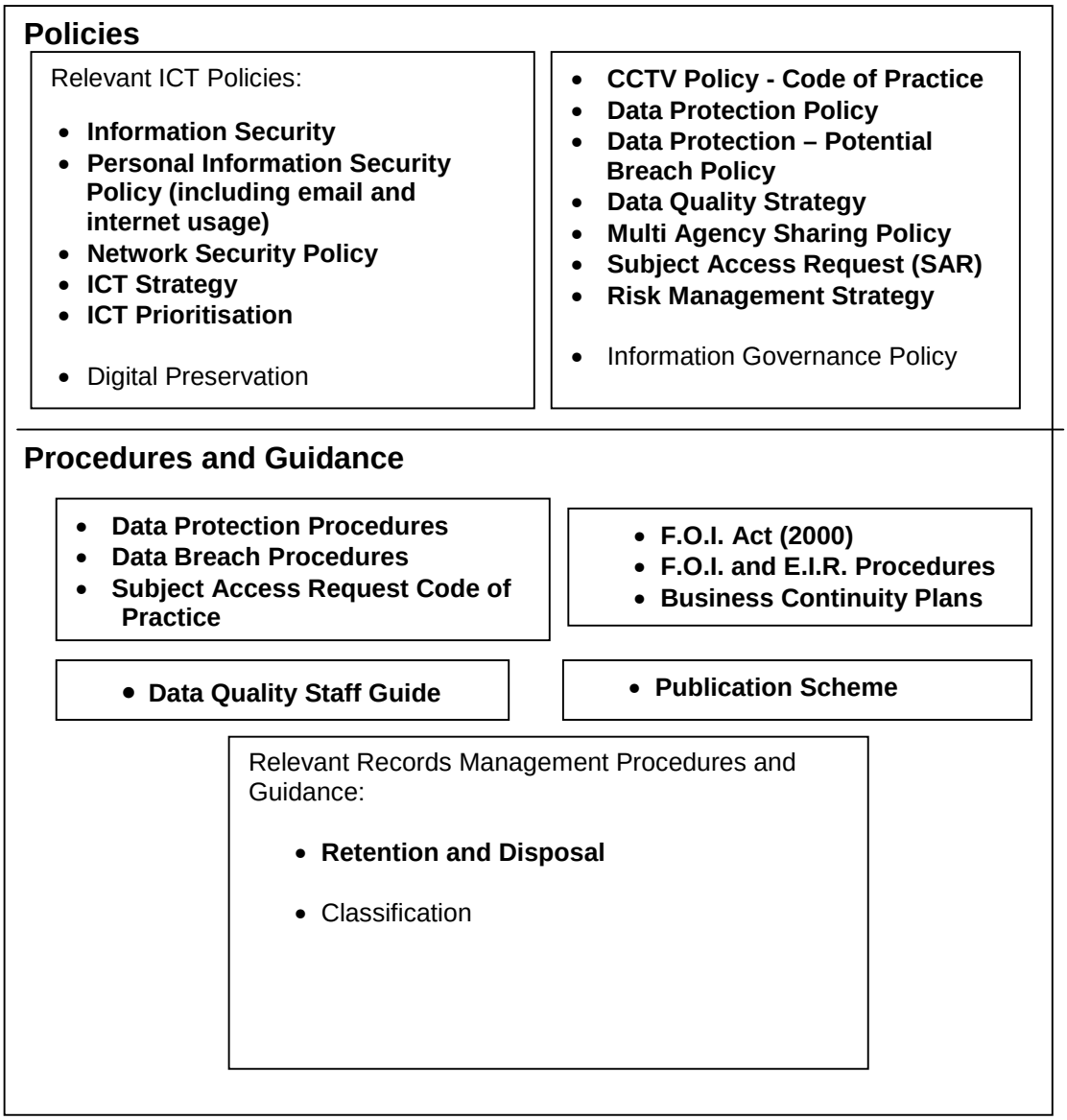
4.2 Records Management is a corporate requirement; hence the policy applies to all groups, services, and employees of the Council. It also links to other key Council documents and policies, in particular Freedom of Information, Data Protection, Information Security, Internet and E-mail procedures.

4.3 When staff leaves the organisation the Exit Policy should be followed to ensure safe transfer of all information.

4.4 Records Management is part of a network of policies and procedures which are necessary to ensure that full and accurate records of all activities and decisions of the Council are created, managed and retained or disposed of appropriately (as shown in the diagram above).

4.4 Over time this framework will be populated with a suite of policies, procedures and guidelines that will support an overall Information Governance Policy. Many are already in place, but others still need to be developed.

Key: Policies and Procedures in '**bold**' are already in place, the others are still under development.



5. Aim and Objectives

5.1 To improve the standard of Records Management across all County Council services by moving towards a consistent Council wide approach to the storage, management, sharing, retention and disposal of records.
The policy has five key objectives:

5.2 **Maintain and manage records effectively throughout their lifecycle. (Managing records from birth to death and all the in-between.)**

The Council has to manage and maintain records from when they are created to when they are destroyed or archived. The process has to account for all the Council's actions and decisions. For example, drafts of documents may be requested under Freedom of Information. As such, the Council needs to be aware of the lifecycle of the documents and records it creates so that it can provide transparency of its decisions. At the same time, the lifecycle approach ensures that records are managed and maintained for as long as they are required. In doing so, it provides an audit trail for decisions;

5.3 **High Quality Information. (If you can't trust your records what can you trust?)**

Records have to be complete, accurate, and the information they contain is reliable. The idea of data quality moves beyond its accuracy to include its accessibility in the future. The Council has to be able to demonstrate the authenticity of its records now and in the future. For electronic records, this means that records have to be compatible when access to them is required by future systems.

5.4 **Clear Retention and Disposal Arrangements. (Know when to keep it and when to bin it.)**

The Council needs to know what it has to keep and for how long. In some cases records such as asbestos have retention periods of over 40 years. The retention guidelines that will be agreed within services will address their business needs as well as their service specific statutory requirements. In some cases, the Council has to retain records permanently and these will be transferred to the Durham County Record Office;

5.5 **Accessible Filing. (If you name it, you can file it and then you can find it.)**

When records are filed, they have to be retrievable. To retrieve records, a common approach to filing has to be agreed so that files can be tracked and found.

5.6 **Ensure Security of Data (In how it is stored and shared.)**

The Council need to ensure that data, both in paper and electronic format is stored in a secure environment with appropriate security and backup systems in place. Access and the use of data should be appropriate to the data user and comply with relevant legislation (such as the Data Protection Act 1998).

The National Archives have prepared a guide on Managing Information Risk to highlight specific issues related to the management of information risk. The guide aims to raise awareness of the nature of potential risks.

6. Development of Corporate Procedures

The Council will have a clear inventory of the records they hold. A pro- forma is attached at Appendix D to help services with this. The information gathered should be held in a database.

In the longer term the aim is to develop Council wide standards for storage, management, sharing, retention and disposal of records.

The audit information will be the foundation for services working with the Information Management Team to:

- develop fileplans and the classification of records using the example found at: Local Government Classification Scheme;
- develop a Council wide scheme for the storage of semi-current records and archives.
- consider moving towards an Electronic Document and Records Management System in the longer term.

Service groups will want to consider best practice when they develop their own procedures. A good bench mark of an overall approach to records management is provided by Northumberland County Council found at: Northumberland County Council.

Further guidance and information can also be found on the National Archives website at: National Archives.

6.1 Maintain and manage records effectively throughout their lifecycle

Until you know what you have, it's impossible to establish any type of records lifecycle program. When records have been created, they need to be managed until they can be disposed of.

TIPS - Examples of what to do and what to avoid are:

Do:

- Use the information audit tool at Appendix C to identify major record groups and group them into broad categories for each type of record, such as: Invoices; Purchase Orders, Reports, Minutes etc.;
- Create an inventory of these records, listing their locations and whether they are in paper format, electronic, or both. The records inventory becomes the basis for preparing the retention schedule setting out how long you need to retain records.
- Complete the Records Compliance Health Check at Appendix E to find out how 'healthy' your records are.

Avoid:

- Keep records within folders called 'My Stuff' etc.;
- Store paper or electronic records in un-named files;
- Keep records for any longer than they are needed;
- Store electronic records on your desktop, this makes them inaccessible for other staff, also they are not backed up on the network if they are saved there;
- Dispose of records which are involved in any type of investigation, even if they are out of their retention period;
- Make copies of records that are sent into storage.

6.2 High Quality Information

The Council recognises that there are a number of key characteristics of good quality data. The data on which we report and make decisions on should be:

- Accurate – Data should be sufficiently correct for its intended purposes;
- Valid – Data should be recorded in an agreed format and used in compliance with recognised Council and national standards;
- Reliable – Data should reflect stable and consistent data collection processes across the Council;
- Timely – Data should be available within a reasonable time period, quickly and frequently enough to support information needs;
- Relevant – Data captured should be relevant to the purpose for which it is used;
- Complete – All data should be captured based on the information needs of the Council;
- Secure - Data should be stored securely and confidentially;
- Accessible – Data should be easily available by those who need it.

TIPS - Examples of what to do and what to avoid are:

Do:

- Make sure that records are kept complete and accurate. If something is removed, for example, because it's out of retention, add a reference to it in the file;
- Make sure that records are kept in a format that will continue to be readable in the future;
- Arrange periodic audits/reviews of record quality for key records in line with the Council Data Quality Policy available at: Data Quality Policy.

Avoid:

- Retain duplicates or drafts of records longer than the official version of the records.

6.3 Clear Retention and Disposal Arrangements

The development of retention guidelines by services is required so that records can be disposed of in a documented and controlled way. This is necessary for records in both paper and electronic format and will minimise the amount of information we keep. Using the pro forma found at Appendix D will help you to identify the major groups of records you use. You will then be able to determine the correct retention by using the available guidance or advice from the Information Management Team.

Confidential and sensitive records must be disposed of by using the blue confidential waste bins. When large clearances of records, which contain a series of records are carried out, a log of the disposal should be created.

Other records created in the normal course of business may be disposed of by recycling. This may be information that is duplicated, unimportant or only of short-term business value such as: 'with compliments' slips, telephone message slips, messages or notes not related to a business transaction.

Guidance on the retention of records is available at:
Retention Guidelines for Local Authorities.

TIPS - Examples of what to do and what to avoid are:

Do:

- Include Records Management as part of your internal audit process to ensure that consistency, compliance and legal requirements are met;
- Try and reduce the number of records which no longer have on-going business value in order to reduce the risk and cost of storage;
- Keep a log of the confidential records you have disposed of to create an audit trail.
- Always dispose of confidential information by shredding.

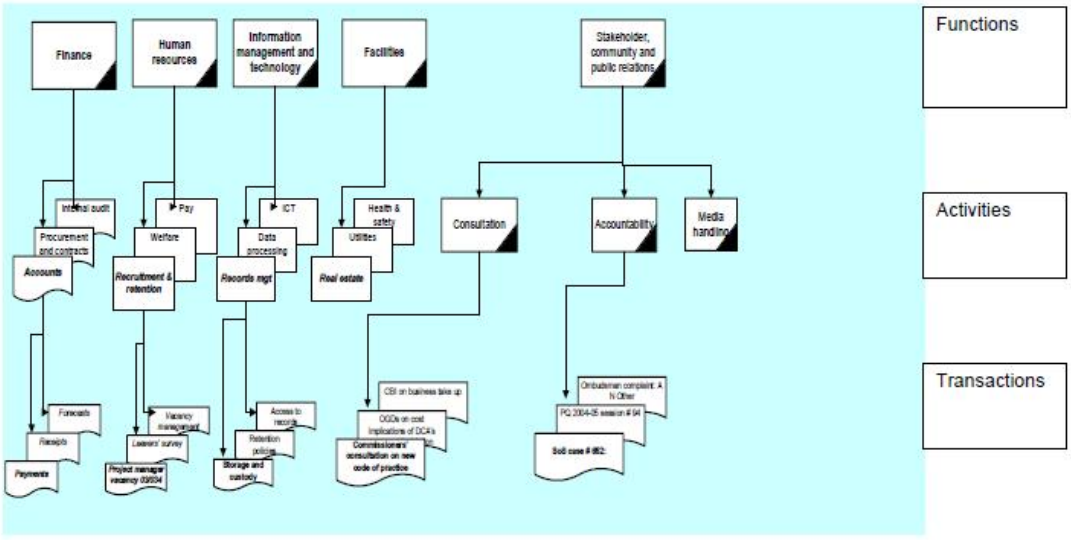
Avoid:

- Destroying records if there is a possibility of litigation, the records and information that are likely to be affected should not be amended or disposed of until the threat of litigation has been removed.
- Retain information 'just in case', set a retention period using the guidelines provided or advice from the Information Management Team;
- Place confidential information in normal rubbish bins.

6.4 Accessible Filing

At present there are a huge range of varied file formats across the Council including SharePoint. Our long term aim is to develop a Council wide approach to filing classification and move towards an Electronic Document Records Management System (EDRMS). The starting point is to complete an information audit for all areas to find out what groups of records are held and take action to improve accessibility in the shorter term. Records are created, received or maintained as evidence of a business transaction. Therefore a classification scheme should be designed to directly reflect the hierarchical relationship of functions, activities and transactions of the Council.

Figure 3: administrative functions



Arranging records in a functional filing system ensures that the business context of records is clearly identifiable. It becomes much easier to exercise security, audit, efficiency-saving or other exercises if business records are filed in a way that mirrors the ways in which the organisation operates.

Guidance on the functional naming criteria can be found at: Local Government Classification Scheme.

TIPS - Examples of what to do and what to avoid are:

Do:

- Use the same naming criteria for both paper and electronic records.
- Limit access of individuals to records, unless it is necessary for them to conduct authorised business.

Avoid:

- Store records which may need to be shared with others on your own drive.

6.5 **Ensure Security of Data**

In accordance with the Data Protection Act (1998) the Council has an obligation to protect the information it collects. The Information Commissioner's Office state that the eight principles are as follows:

Personal information must:

- Be fairly and lawfully processed;
- Be processed for limited purposes;
- Be adequate, relevant and not excessive;
- Be accurate and up to date;
- Not be kept for longer than is necessary;
- Be processed in line with the data subjects' rights;
- Be secure;
- Not be transferred to countries outside of the EU without adequate protection.

To enable the Council to do this services need to put measures in place to ensure that information is held safely and only shared with those who have a business right to it.

Information should be stored in a secure location whether in paper or electronic format, with access controls in place.

Sharing of personal or sensitive data needs to be done within the framework of a formal information sharing agreement. Paper records containing personal data which are rarely accessed and need to be retained should be moved to a suitable secure storage area until they can be disposed of in line with retention guidelines.

Confidential and sensitive electronic records which need to be shared with partners outside of the Council should be shared by using a secure network, for example, the Public Service Network (PSN). A secure network will enable interactions between connected local authorities and other connected organisations such as the National Health Service and the Police with minimal risk.

7. Benefits from this Policy

7.1 The policy will help the Council to manage its records effectively. It will ensure that the Council:

a) Safeguards and preserves vital information so that it is readily accessible;

b) Optimises the use of office space;

c) Complies with statutory requirements;

d) Improves joint working, information sharing and integrated records;

e) Makes all staff aware of their record-keeping responsibilities through

specific training programmes and guidance;

f) Carries out periodic audits to measure compliance and improves standards wherever possible;

g) Risks are minimized;

h) Makes savings based on less storage and office space.

8. Roles and Responsibilities: Who does what?

8.1 Corporate Management Team are responsible for:

a) Approving the corporate framework for the management of records within the Council as set out in this policy to create, keep and manage records which document its principal activities.

b) Developing the Records Management culture which will demonstrate the Councils commitment to accountability and promotion of good governance.

8.2 Information Governance Group responsibilities are to:

a) Advise services and departments on developing service specific procedures and applying the Records Management Policy;

b) Ensure that staff have access to support in terms of training and development in adhering to the Records Management Policy and Procedures;

c) Review and update the Corporate Policy and procedures when changes occur.

8.3 Corporate Directors are responsible for:

a) Developing service guidance for the management of records to meet their respective needs and best practice;

b) Ensuring the aims of this policy are implemented within their own department/service;

c) Each service grouping will update their retention guidelines following the Corporate Policy, supported by the Information Governance Group. (for example, how long to retain a record such as an invoice?);

d) Ensuring that appropriate staff are appointed as Records Champions as they are required to assist with the implementation of Records Management procedures within their own department/service (see Appendix B);

8.4 Heads of Services are responsible for Records Management in their service, their responsibilities are to:

a) Develop and operate records management procedures, covering both electronic and hard copy records, to comply with corporate records management policy and standards;

b) Ensure employees, including contractors, consultants and volunteers employed to undertake Council business follow procedures for the management and storage of electronic and hard copy records. This will include developing verification procedures for monitoring compliance with procedures;

c) Ensure appropriate resources are in place to enable compliance with records management policy and standards;

d) Communicate records management procedures.

8.5 Individual Employees: (See Appendix B for types of records)

a) Individual employees are responsible for the records they create (type a and b records, as shown on Appendix B);

b) The Council owns the information that individual employees create;

c) Employees will create records in accordance with the relevant service guidelines (for example when you create a purchase order, you follow the appropriate guidance);

d) Are responsible for making sure that records are disposed of in accordance with the service guidelines as framed by the corporate policy;

e) Are responsible for ensuring that the most appropriate method of disposal is used dependant of the confidentiality of the records to be destroyed;

8.6 Archivist (Type c records, as shown on Appendix B)

a) The Archivist is responsible for the long-term management and preservation of the records of the Council selected for permanent retention and deposited at the County Record Office.

b) The Archivist provides professional expertise on the maintenance and preservation of records in all formats across the authority.

8.7 Members

Members need to be aware of their own records management requirements as part of their Council work. Advice and guidance on the policy will be issued to elected Members of the Council.

9 Partnership Working

Where **joint** records are created as a result of partnership working there needs to be clearly defined responsibilities between the Council and the partner organisation for the creation and management of records.

The ICO has prepared some guidance on Data Controllers. This will explain the differences which need to be considered between data controllers and data processors.

Further guidance can also be found here: Article 29 Working Party Opinion 1/2010 on the concepts of 'controller' and 'processor'.

- Where the Council is the lead partner:

  - The Council's Records Management Policy will be applicable;
  - The Council will be responsible for the custody and ownership of the records;
  - The Council's records management procedures including retention policy will be followed.

In integrated Council/partner teams, ensure that these teams develop their own records management procedures which comply with the policies of both the Council and partner organisations, with each partner responsible for their own records.

9. Training and Awareness

9.1 All employees of the Council are involved in creating, maintaining and using records, it is vital that everyone understands their records management responsibilities as set out in this policy.

9.2 Heads of services will ensure that staff responsible for managing records are appropriately trained or experienced and that all staff understands the need for records management and the difference between the types of records created (See Appendix B).

9.3 Induction training for all staff, whether permanent or temporary, should include an awareness of records issues and practices, including an introduction to the Data Protection Act 1998, Freedom of Information Act 2000 and the Environmental Information Regulations 2004.

10. Performance Management

10.1 The Information Management Team will monitor performance with regard to the management of records. Indicators to monitor the performance on records management are set out on the table below a will be reported as part of Corporate and Service Grouping performance management frameworks.

Performance Measurement	Target	When?
Internal Audit of service records and Information Management.	All reports show a moderate level of assurance or better.	In line with annual audit programme.
Response times: o F.O.I. o E.I.R. o Subject Access Request	 20 working days 20 working days 40 calendar days	Quarterly Corporate Report.
No adverse judgements from the Information Commissioner's Office linked to Records Management issues.	Nil	Annually.

11. Policy Review

This policy will be reviewed on a regular basis at least once every three years and if appropriate, amended to maintain its relevance.

12. Contacts

The Information Management Team or guidance via the Intranet available at: Information Management Team.

The Information Governance Group Representative for each service.

Appendix A

Checklist for Assessing Risk to Paper and Electronic Records

Have we assessed the importance of paper and electronic records to our business?

We know what records we hold and handle. ☐

We know the relative security, sensitivity and importance of each set of records. ☐

We understand which record systems support the management of key paper and electronic records. ☐

We know how critical the records are for the management of our business. ☐

Do all staff understand their roles and responsibilities in managing these risks?

All our staff understand their role in managing information, and the risks it poses. ☐

All staff are clear on what's mandatory, and where they can make decisions. ☐

All staff are clear about to whom they report concerns and 'near misses', so we can learn from incidents and mistakes. ☐

We have built this into our culture through training, performance management and governance structures. ☐

All staff understand the consequences of not following the rules. ☐

Have we assessed our information risks?

We have developed a risk assessment of our paper and electronic records. ☐

This risk assessment looks at all of our key risks and how critical they are to our business. ☐

This assessment follows the approach we have taken overall to risk management, and embeds information risk management within our overall business risk model. ☐

Do we have a plan for managing these risks?

We have identified what we need to do to mitigate risks to an acceptable level. ☐

We consider paper and electronic records as one of many business process, and business risks. ☐

Records Management is seen as a core skill, and is built into training and assessment. ☐

If this policy is not followed then the following consequences are likely:

1 You lose records;
2 You spend time and money finding records;
3 You spend time re-creating records;
4 Failure in complying with the Data Protection Act 1998, resulting in a fine for the Council;
5 Legal challenge – unable to provide documentary evidence.

If you require any further assistance in completing the checklist please contact the Corporate Risk Management Team or visit the Corporate Risk page on the Intranet. Other relevant guidance includes the Local Public Services Data Handling Guidelines.

There are many types and size of information systems. Consequently, the level and nature of the associated risk also varies. The table below should help you decide whether or not you need to undertake a formal, risk analysis.

Each factor is allocated a score of between 1 and 3. Depending on the score it may not be necessary to undertake a formal, detailed risk analysis. This decision lies with the manager responsible for the information system. If there is any doubt it is recommended that a formal risk management approach is taken.

	1 Point	**2 Points**	**3 Points**	**Score (1 – 3)**
Business Impact Note (1)	Minor	Moderate	Major	
Sensitivity of Data Note (2)	Minor	Moderate	Major	
Potential Fine for Legal Breach	< £0.5m	£0.5m - £5m	> £5m	
Accessibility Requirement	> 1 working week	< 1 working week	< 1 working day	
Business Impact	Minor	Moderate	Major	
Number of System Records	< 5,000	5,000 – 99,999	100,000	
Number of System Users	1	1-100	100 +	
Scope of Usage	Service Only	Corporate	Internal and External	
System Complexity	Straight-forward	Moderately Complex	Highly Complex	
Replacement Cost	£1,000	£1,001 - £10,000	£10,000 +	
Total Score				

Notes

1. Refer to Business Impact Assessments
2. Data can fall into three categories:
   i. Personal Data;
   ii. Personal Data containing financial or confidential information;
   iii. Sensitive Personal Data, means personal data consisting of information as to;
   a) the racial or ethnic origin of the data subject,
   b) his/her political opinions,
   c) his/her religious beliefs or other beliefs of a similar nature,
   d) whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
   e) his/her physical or mental health or condition,
   f) his/her sexual life,
   g) the commission or alleged commission by him/her of any offence, or
   h) any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

Appendix B

Types of Records

If the record or data it contains is required for further processing then this should be copied and a new record created. There are four basic types of records:

a) **Current** - records needed to efficiently and effectively conduct current business, including vital records (e.g. ongoing projects and case files);

b) **Semi-current** - records not needed to support current business, but which need to be retained for defined periods for operational, regulatory or legal reasons (e.g. completed projects and closed case files);

c) **Archival** - records retained permanently because of their value as evidence. Records no longer required for administrative use should be offered to the archivist for permanent preservation in the County Record Office (e.g. Committee Minutes);

d) **Redundant** - records that are no longer required and which are not archival. Redundant records should be destroyed by appropriate means. If the records contain sensitive information they should be destroyed by shredding and a disposition log kept for audit purposes (e.g. records older than the time limit set by the retention guidelines or best practice).

Appendix C

The Role of the Records Champion

Each Head of Service will designate a Records Champion or Champions for their service. The Records Champion(s) will be the key contact for the Information Management Team.

The Information Management Team will provide guidance for each administrative procedure for Records Management.

The Information Management Team will provide advice regarding Records Management.

The Head of Service will:

- Appoint Records Management Champion(s);
- Identify and designate from within their service, the administrative support needed to fulfil the Records Management needs;
- Know the statutory requirements for the retention of records for their own service area.

The Records Champion will:

- Identify what is a record both in paper and electronic format;
- Identify which records need to be retained for business use and are no longer accessed regularly;
- Ensure the service have robust processes in place for filling archive boxes in preparation for moving them to the archive storage area;
- Ensure the service have robust processes in place for creating records listings in electronic format and retaining them for reference;
- Ensure the service have robust processes in place for identifying records which are to be offered to the County Record Office for appraisal;
- Request/retrieve information from the archive storage area;
- Record information which is to be destroyed onto Disposition Logs to create an audit trail;
- Attend meetings as needed on behalf of the service to discuss issues with regard to Records Management;
- Cascade information to other staff members within the service area when necessary.

Appendix D

Information Audit Pro Forma for Services/Service Groupings

Record Type	Location and Owner	Format	Quality Control Arrangements	Retention and Disposal	Accessibility of filing	Security
For example: Service user files, Personnel files, Contracts, Minutes, Reports, Applications etc.	For example: Filing Cabinets, Cupboard, Shelves etc.	For example: Paper, Electronic or both, Video, Microfiche, other etc.	Do you audit the quality of information? Will its format continue to be readable (watch out for obsolete formats such as Microfiche and old IT systems.	Do you know the retention of the record and how it should be disposed of? For example: Current year plus six, then shred. (CY+6 = S)	Are you able to retrieve the records easily?	1. Are records stored in a secure manner? 2. Are the records shared easily with the staff that has access rights? 3. When shared outside of the Council, is an information sharing agreement in place?

Appendix E **Proposed Records Compliance Health Check for Services - 2014**

	Task	Yes	No	Under Development/Comments
1.	Have you distributed the Records Champion's Manual to relevant officers managing the records in your service?			
2.	Do you have a file plan for your services?			
3.	Do you have an agreed file naming and file categorisation in your service?			
4.	Do you have a retention guideline for your service?			
5.	What are your security systems for your paper and electronic records depending on the content such as financial or personal data?			
6.	Has the file plan been circulated to all officers to follow?			
7.	Are your disposal logs up to date?			
8.	Do you have a check out system to track the location of your records as an audit trail?			
9.	What date did your service last review its approach to records management?			

Action Plan for Improving Records Management

Area for Improvement	Action to be taken
Retention and Disposal	
Accessibility	
Quality	
Security	

For advice go to: Information Management Team Page

Appendix F

Metadata

Title:	Corporate Records Management Policy
Purpose:	To assist services in the management of their records and protect the Council from fines and negative publicity due to inappropriate use.
Scope:	The scope of this Policy applies to all DCC personnel, including members who create records on behalf of the Council.
Version:	3.0 - Web Version
Author:	Records Management Officer
Owner:	HOS Planning and Performance
Approval:	IGG – September 2014
Issue Date:	Feb 2015
Next Review:	Feb 2018
Location:	DCC Intranet: Information Management Team