



Records Management Policy

V1.0

Information Governance Framework

IGF/CDPAL3

Document owner	Roger Kershaw, Strategic Director Resources
Document author	Richard Boneham, Head of Governance & Assurance
Approved by and when	
Date of document	December 2013
Version	1.0
Document classification	Internal
Document distribution	Internal
Document retention period	Until date of next review
Location	TBA
Review date of document	December 2016

If you require this document in large print, on audio tape, computer disc or in Braille please contact the document manager.

Date Issued	Version	Status	Reason for change
June 2013	0.1	Draft	New Policy document
November 2013	1.0	Final	Approved by IGB

To make sure you are using the current version of this policy please check on iDerby under **Governance/Information Governance** or contact the Information Governance Manager when using printed copies

Equality impact assessment record	
Date of assessment	
Summary of actions from EIA	

Contents

Introduction and purpose..... 4

Scope..... 4

Related Council strategies, policies, and procedures..... 4

Legislation, guidance and standards 4

Policy statement..... 5

1. Aims of our Records Management System..... 6

2. Roles and responsibilities 7

3. Accuracy of personal records and data..... 7

4. Access to records (Statutory public access) 7

5. Standards for the storage of paper records..... 8

6. Standards for managing electronic records and email 8

7. Retention and disposal schedules 9

8. Offsite Storage Procedure and Guidance 9

9. Corporate Records Destruction Procedure 9

Compliance and monitoring of the Records Management Policy 10

Information 10

Evaluation and review 10

Help messages..... 10

Appendix 1 10

Introduction and purpose

This Policy forms part of the Council's Information Governance Framework and sits at Level 3 under Information Security Assurance. See Appendix 1.

This Policy establishes the Council's expectations and rules in respect of records management.

Records Management is governed by a number of laws and regulations, several of which are related to Data Protection and Freedom of Information.

Records management is the practice of maintaining records from the time they are created up to their eventual disposal. This may include classifying, storing, securing, and destruction (or in some cases, archival preservation) of records.

A record can be on paper, a physical object or digital records, for example, customer records, birth certificates, office documents, prosecution evidence, electronic systems and e-mail. Records management is primarily concerned with retaining records produced from the Council's business activities.

Scope

This Policy applies to all Council employees, including Councillors, consultants and temporary contractors who have authorised access to Council IT systems who work with and produce official records on behalf of the Council.

This policy relates to records held in any format by the Council that do not form part of the corporate Electronic Document Record Management System - EDRMS.

Related Council strategies, policies, and procedures

- [Information Security Policy](#)
- [Data Protection Act Policy](#)
- Caldicott Principles
- Protective Marking Scheme
- Document Retention Schedule
- [Desktop and Laptop Computer Security Policy](#)
- Serious Incident Reporting Policy

Legislation, guidance and standards

The Council is required by law to comply with all relevant legislation or statutory guidance. All employees including temporary employees and agency staff, Elected Members, partners and external contractors must comply with the relevant legislation when acting on behalf of the Council.

The Council will comply with the following legislation and guidance, and any other legislation as appropriate:

- Data Protection Act 1998

- The Freedom of Information Act 2000
- Public Records Act 1958
- Re-use of Public Sector Information Regulations 2005
- Employment legislation
- Health and safety legislation

If you are not sure of your responsibilities under any of these laws, contact the Council's Information Governance Manager for further information

Policy statement

This Policy has been developed to promote and establish good record keeping processes and procedures within the Council.

Derby City Council (the Council) has a commitment to maintain and improve the way in which information and records are created, maintained and destroyed.

Records will be managed in relevant management systems and organised accordingly, for example alphabetically, numerically, in date order. Reference numbers and/or version control must be applied. This will assist with identifying records which need to be accessed in the future, and for storing of records prior to destruction.

The Council has in place a Record Retention Schedule that will be followed to make sure appropriate retention periods are maintained prior to destructions of records so the Council complies with relevant legislation and regulations.

Training is provided for employees and Elected Members on the importance of managing records effectively. Relevant Policies, procedure and guidance must be used in conjunction with the Council's retention and disposal schedules and regular audits will be scheduled to monitor compliance for the safe management of records.

This policy document should also be read in conjunction with the Council's Records Management Strategy which sets out how the policy requirements will be delivered

Definitions

Records Management is a discipline which utilises an administrative system to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is administratively and legally sound, whilst at the same time serving the operational needs of the Council and preserving an appropriate historical record. The key components of records management are:

- record creation
- record keeping, including classification
- record maintenance, including tracking of record movements
- access and disclosure

- closure and transfer
- appraisal
- archiving
- disposal.

The term **Records Life Cycle** describes the life of a record from its creation/receipt through the period of its 'active' use, then into a period of 'inactive' retention (such as closed files which may still be referred to occasionally) and finally either confidential disposal or archival preservation.

In this policy, **Records** are defined as 'recorded information, in any form, created or received and maintained by the Council in the transaction of its business or conduct of affairs and kept as evidence of such activity'.

Information is a corporate asset. The Council's records are important sources of administrative, evidential and historical information. They are vital to the Council to support its current and future operations (including meeting the requirements of Freedom of Information legislation), for the purpose of accountability, and for an awareness and understanding of its history and procedures.

1. Aims of our Records Management System

The aims of our Records Management System are to make sure that:

- **records are available when needed** - from which the Council is able to form a reconstruction of activities or events that have taken place;
- **records can be accessed** - records and the information within them can be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist;
- **records can be interpreted** - the context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records;
- **records can be trusted** – the record reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated;
- **records can be maintained through time** – the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format;
- **records are secure** - from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled and audit trails will track all use and changes. To make sure that records are held in a robust format which remains readable for as long as records are required;

- **records are retained and disposed of appropriately** - using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value; and
- **employees are trained** - so that all employees are made aware of their responsibilities for record-keeping and record management.

2. Roles and responsibilities

The Information Governance Manager is responsible for developing records management processes and procedures on behalf of the Head of Governance & Assurance.

All employees and Elected Members are responsible for the records they hold on behalf of the Council. All relevant policies, procedures, guidance and the retention and disposal schedules approved by the Chief Officer Group must be followed.

All records created by Council employees and elected members will remain the property of the Council.

The creation, maintenance and destruction of records are the responsibility of the department providing the service. Each department must manage records in accordance with this policy and associated policies and procedures. It is essential records are stored securely and the location of files is up to date at all times.

3. Accuracy of personal records and data

The Council must make sure all personal information is processed in accordance with the Data Protection Act 1998. The Council's [Data Protection Policy](#) explains how employees are expected to comply with the Act when creating and maintaining records on behalf of the Council.

All records must be accurate, up to date and not excessive. Any corrections, amendments or additions to a record are to be made in accordance with departmental procedures and a record of changes retained for audit purposes.

4. Access to records (Statutory public access)

i Subject Access Requests

The Data Protection Act 1998 gives individuals the right to access their personal information held by the Council. Policy, procedure and guidance can be found on the Information Governance pages of iDerby in relation to subject access requests.

ii. Freedom of Information

The Freedom of Information Act 2000 gives people a right to know what decisions are taken on their behalf by the Council on how services are run. The Council has published a [Publication Scheme](#) which shows what information is already in the public domain. Any information which is not part of the Publication Scheme can be requested under the Freedom of Information Act. There may be exceptions where statutory exemptions to publishing information apply. Further guidance and contact information can be found on the [Information Governance](#) pages on iDerby.

iii. Environmental Information Regulations

The Government have issued regulations to local Government which make it easy for people to access information about the state of the elements of the environment (air, atmosphere, water, soil, landscape, natural sites and ecology, biological diversity, and genetically modified organisms). Some information related to this is contained within the Council's Publication Scheme. Requests that fall under the Environmental Information Regulations are treated much the same as requests under the Freedom of Information Act 2000 except when we wish to rely on an statutory exception to disclosure. Further guidance and contact information can be found on the [Information Governance](#) pages.

5. Standards for the storage of paper records

The Council must make sure records are protected from damaging elements such as water, light, temperature, humidity, fire and infestation.

The security of the information must also be protected by keeping storage units and rooms locked when not in use. Access to keys must be restricted to the responsible service area employees.

Locations such as basements are not suitable for long term storage so alternative arrangements must be made. Utilisation of the Cintas off-site storage facility must be explored if paper records must be retained. Please contact Business Support for more information on 642314.

Access to the basement in the Council House is restricted by Facilities Management. If access is required to the basement for storage on a short term basis then reasons must be provided and agreement reached with FM. Please contact Facilities Management for more information on 642142. Records must be managed in line with the Council's [retention and disposal](#) schedules and destruction and offsite storage procedures which are available on the [Information Governance](#) pages.

6. Standards for managing electronic records and email

It is essential that regular housekeeping is completed to make sure records stored are saved for the appropriate length of time in line with retention and disposal

schedules. Records from services that are not yet included in the corporate rollout of the EDRMS system must be saved into the relevant business system or shared work areas.

The [Network, email and Internet User Policy](#) has further information on appropriate management of electronic records and email which is available on the Information Governance pages.

7. Retention and disposal schedules

The Council's [retention and disposal schedules](#) identify the types of records that we may hold and length of time each document or electronic record is retained, and when it should be destroyed. In some cases records are retained permanently.

Directorates are consulted on the types of records held and agreement reached on the appropriate length of time set for retention of those records. Some retention periods are governed by statutory legislation so it is important retention periods are applied correctly when deciding how long to keep or destroy a record. Requests can be made to change retention periods but there must be a valid business reason and agreement with the Information Governance team.

All records have different retention periods, for example the destruction date may be from last involvement (closed record/last action entry) or from date of birth depending on which service generates the record and if it is covered by a statutory retention period.. This must be checked on the corporate retention and disposal schedules.

The retention schedules can be found on the [Information Governance](#) pages.

8. Offsite Storage Procedure and Guidance

The Council is required to keep records for specified periods of time after involvements have ended. The length of time for keeping closed records varies dependent upon the nature of the involvement the Council had with the customer.

The retention period for each type of record is specified in the Council's retention and disposal schedules.

The Offsite storage procedure and guidance contains guidance in relation to the processes for preparing records prior to sending offsite and for retrieving closed records. Please contact Business Support for more information on 642314.

9. Corporate Records Destruction Procedure

The Council has a statutory duty under Data Protection legislation to make sure records are not kept for an excessive amount of time. Where records are outside of the documented retention period these must be destroyed unless there is a valid

reason for retaining. If the responsible department have a business need to retain information after the destruction date set the Information Governance team must be notified and an agreement reached to change.

Compliance and monitoring of the Records Management Policy

The Head of Governance & Assurance is responsible for monitoring compliance with this policy.

If employees knowingly do not comply with Council policies, procedures or guidelines, the Council may take appropriate action under the Disciplinary Procedure

Information

Further information and the most up to date policies and procedures on information management, risk management, information security and information governance can be found on iDerby/Governance/Information Governance.

Evaluation and review

This Policy will be review by December 2016.

Help messages

If you require this document in large print, on audio tape, computer disc or in Braille please contact the document manager.

L2 Information Governance Management

- L3 IG Strategy document
- Information Governance Board TOR
- Information Asset Register
- Serious incident Reporting Policy

L2 Confidentiality & Data Protection Assurance

- L3 Principles & Obligations
 - [Data Protection Act Policy](#)
 - L4 [Data Protection operational guidance](#)
 - Accessing & Storing Data
 - [Records Retention schedule](#)
 - Records management policy/strategy
 - [Protective marking scheme/Classification](#)
 - DPA/Caldicott Guidance
 - Confidential waste disposal
 - Business Impact Levels
 - Register of Information Sharing Agreements
 - Privacy impact assessments new systems

L2 Information Security Assurance

- L3 [Information security policy](#)
 - Password policy
 - Network, Email & Internet User policy/electronic mail
 - Mail handling procedures
 - Monitoring policy
 - IT Security
 - L4 Anti-Virus Policy
 - Desktop and Laptop computer security policy
 - Starters & Leavers
 - Rules
 - Home & remote working policy
 - [Mobile computing](#)
 - Code of Connect compliance documentation
 - User access management policies

L2 Action Plan