

## **ACCESS TO INFORMATION IN LOCAL GOVERNMENT**

### **1 SUMMARY**

- 1.1 This report suggests a framework of policies and guidelines for the successful implementation of the Freedom of Information Act 2000 coming into force on 1 January 2005.

### **2 INTRODUCTION**

- 2.1 This is the third in a series of reports to this Committee on the progress made towards implementation of the above. Work to date has followed the agreed action plan and Codes of Practice on discharge of functions and management of records issued in accordance with the Act by the Secretary of State and Lord Chancellor respectively. The Lord Chancellor's Code of Practice requires all public authorities to have in place an overall policy statement, endorsed by top management and made readily available to staff at all levels of the organisation, on how it manages its records, including electronic records. To be meaningful, this statement requires a framework of supporting policies and procedures. This report proposes the principal documentation for this framework in a series of appendices covering policy, human resources and procedural guidance to be collated into one comprehensive publication.

### **3 DATA PROTECTION AND RECORDS MANAGEMENT POLICIES**

#### **3.1 Publication Scheme**

A Publication Scheme was the first policy document required under the Act. The Council's Publication Scheme came into force in February 2002 and its operation is being kept under review.

#### **3.2 Data Protection Policy**

The purpose of data protection legislation is to regulate the way in which personal information about individuals, whether held on computer or in a manual filing system, is obtained, stored, used and disclosed. The legislation grants rights to individuals to see the data stored about them and to require modification of the data if it is wrong, and, in certain cases, to compensation. The provisions amount to a right of privacy for the individual. A draft policy is set out at appendix 1.

**3.3 Records Management Policy Statement**

The Records Management Policy Statement is the high level policy that provides a mandate for how records management will be undertaken across the whole organisation. A draft policy statement is set out at appendix 2.

**3.4 Electronic Records Management Policy**

The Electronic Records Management Policy aims to meet the requirements of good records management covering all the electronic records of the Council. This is a growing area and key to dealing efficiently and effectively with Freedom of Information issues. A draft policy is set out at appendix 3.

**3.5 Information Technology Code of Practice**

This code of practice has been developed to provide clear advice on what is and is not acceptable use of the Council's IT systems. An increasing volume of information is disseminated through the Internet and by exchange of email. Email in particular is usually delivered almost instantaneously and in a style less formal than traditional written communication. It is nevertheless subject to the same rules and regulations. While offering considerable advantages in speed, cost, media options and ease of use, it also presents a range of potential problems. It is therefore appropriate to include the IT code of practice for these matters within this documentation. A draft code is annexed at appendix 4.

**3.6 The Essex Trust Charter**

Sharing information between partner organisations is vital to the provision of co-ordinated and seamless services. In addition, the sharing of information can help to meet the requirements of statutory and local initiatives.

While the Council has had a limited data sharing protocol with the police in operation for over a year, an Audit Commission/HMIC review of community safety in Essex identified the need to improve data sharing across key agencies to deal with critical situations and/or vulnerable people. Until now, the uncertainty as to what is and is not legally permissible has inhibited data sharing between authorities throughout the country.

In November 2003 the Department for Constitutional Affairs issued guidance on the legal framework applying to data sharing in an attempt to overcome some of the concerns expressed.

Meanwhile, Essex authorities, including emergency services and various agencies, have developed the Essex Trust Charter, an agreement in principle to share information. The Charter will be supported by specific Information Sharing Protocols, that set out the details of sharing information.

In order to ensure a safe and secure environment for sharing information, organisations signing the Trust Charter agree to;

- Encourage all members to share information, unless it is illegal to share it or permission has not been received.
- Develop good practice for shared information management to help the organisations work together, and support the aims of this Charter through the Essex Information Group.
- Make sure those people giving us information also give us permission to share it.
- Work towards a common set of goals for sharing information.
- Help to develop a brand for the Charter to improve the trust between the organisations involved and the people of Essex.
- Work towards British Standard 7799, the technical standard for information security.

The Charter is being progressed through the Essex Online Partnership and will be considered at the Member e-champions meeting in February. It is proposed that ancillary to the policies set out in this report the Council agrees to become a signatory to the Essex Trust Charter.

#### **4 HUMAN RESOURCES FRAMEWORK**

- 4.1 Practice guidance suggests that responsibility for implementing records management requirements should ideally fall to a professional records manager. However, Central Government is the only part of the public sector until now that has routinely had such posts on its departmental establishments. Other than the County Archive, local government records managers have usually been relatively junior posts managing facilities such as filing systems and “records centres”.
- 4.2 Indications are that qualified records managers are in short supply and most small local authorities will have to consider alternative strategies. The Code of Practice recommends that staff with records management responsibilities should have the appropriate skills and knowledge needed to achieve the aims of the records management programme.
- 4.3 A model competency framework is set out at appendix 5. This is intended as a guide for role specification, identifying training and personal development needs and performance.

4.4 Relying on existing personnel, the minimum requirements for implementing Freedom of Information Act compliant records management in accordance with the Codes of Practice are shown in the following table taken from “Freedom of Information – a practical guide” produced in association with the Information Commissioner. Action taken by the Council to date is indicated in the third column.

<b>Requirement of Code of Practice on Records Management</b>	<b>Recommended action to achieve requirement</b>	<b>Rochford District Council response</b>
Establish Records Management as a corporate programme	Appoint senior officer to take on responsibility for records management as a corporate function	Responsibility delegated to Corporate Director (Law, Planning & Administration)
Formulate and disseminate records management policy	<ul style="list-style-type: none"> <li>▪ Set up Project Group to write up policy</li> <li>▪ Appoint officer responsible for dissemination</li> <li>▪ Establish contact with Records Managers within sector in order to develop associated procedures and guidance</li> <li>▪ Include responsibilities in Job Descriptions</li> </ul>	<ul style="list-style-type: none"> <li>▪ Officers’ Records Management Working Party set up</li> <li>▪ Corporate Director through Operational Management Team</li> <li>▪ Research on internet, practical guidance publications and seminars to produce appended documentation</li> <li>▪ Yet to be considered</li> </ul>
Manage active records effectively	<p>Appoint officer with appropriate skills to;</p> <ul style="list-style-type: none"> <li>▪ produce an authority-wide retention schedule (<i>if at no other point consider appointing a consultant for this task – the authority will fail to comply with FOI in all respects if this is missing</i>)</li> <li>▪ provide continuing guidance</li> <li>▪ provide advice on implementation of systems</li> <li>▪ provide advice on</li> </ul>	<ul style="list-style-type: none"> <li>▪ draft prepared by Corporate Director from “Retention Guidelines for Local Authorities” produced by The Records Management Society of Great Britain.</li> <li>▪ Structure for records management within Administrative &amp; Member Services yet to be addressed</li> <li>▪ Implementation of electronic management</li> </ul>

	<p>whether systems comply with FOI requirements</p> <p>Requires officer with designated records management responsibilities who has been provided with some elements of professional training</p>	<p>system included within IEG strategy</p> <ul style="list-style-type: none"> <li>▪ Supplier to confirm</li> </ul> <p>Will require re-designation of some jobs and provision of adequate training – yet to be addressed</p>
<p>Dispose of records appropriately</p>	<p>Appoint officer to;</p> <ul style="list-style-type: none"> <li>▪ Establish systems for disposal</li> <li>▪ Monitor compliance with the retention schedule</li> <li>▪ Implement physical destruction systems</li> <li>▪ Select and manage the authority's archival record (working with Essex County Records Office)</li> </ul>	<ul style="list-style-type: none"> <li>▪ Yet to be addressed</li> <li>▪ Yet to be addressed</li> <li>▪ Yet to be addressed</li> <li>▪ Yet to be addressed</li> </ul>

4.5 From the above, Members will appreciate that while work is progressing in preparation for January 2005, further consideration needs to be given to the ongoing management and administration of the function and suitable skills training. It is proposed that this will be addressed in a future report on human resources.

## **5 ACTIVE RECORDS MANAGEMENT**

5.1 On 30 October 2003 Council approved the IEG3 statement for submission to the Office of the Deputy Prime Minister. A main thrust of this strategy is the move towards electronic capture of all Council records as far as possible and the realisation of associated benefits from workflow software leading to a comprehensive records management system.

5.2 Public interface to electronic systems is already available in a number of areas. To maximise the benefit of work undertaken to date, the phased implementation of electronic document management will commence with planning and building control, followed by housing benefits and council tax. Having considered a number of software options, the system that is affordable within grant funding limits and most compatible with existing corporate systems is Comino's "Universal Government". Comino plc are

currently installing this system at Maldon and Chelmsford Borough Councils following thorough evaluation, comparison and tendering exercises by those authorities.

- 5.3 Relying on the information provided by the company and the evaluation work done at Maldon and Chelmsford, it is proposed to use the Office of Government Commerce GCat scheme to acquire this software and avoid the lengthy EU tendering procedure. GCat is a catalogue based procurement scheme designed to provide public sector organisations with a simplified means of procuring a range of IT and telecommunications products and related services. GCat reduces the time and costs associated with procurement by offering a pre-tendered call off facility that is EU compliant.
- 5.4 Development of the system in planning and building control will assist to determine the corporate protocols and procedures for active data records management and Members will be advised of progress in further reports.
- 5.5 In the meantime, a pressing requirement is to reduce the amount of duplicate and unnecessary paper records currently held by the Council. There are over 40,000 files in the central filing system alone. For this purpose, Records Disposal Guidelines have been prepared based on "Retention Guidelines for Local Government" published by the Records Management Society of Great Britain. These are annexed at appendix 6.
- 5.6 An important element of active records management is performance monitoring. Recommended performance indicators include information on the quantity of records created, response times to data requests, quantities of records appraised, destroyed or transferred to archive and user satisfaction. A performance management scheme will be prepared for approval and implementation by January 2005.

## **6 RISK IMPLICATIONS**

- 6.1 Failure to have proper policies and procedures in place, prior to the commencement of the Freedom of Information Act 2000, are likely to lead to claims of maladministration for failure to follow the Codes of Practice and increase the risk of breach of statutory duties and responsibilities.
- 6.2 Failure to introduce an electronic records management system will compound the difficulties of achieving a FOIA compliant system and reduce the benefits to be derived from work undertaken to date on the implementation of electronic government and the Council's ability to achieve its IEG aims.

## **7 RESOURCE IMPLICATIONS**

- 7.1 The most significant financial implication will relate to human resources and introduction of an electronic system for data capture, workflow and record management. There are likely to be considerable benefits in improved service delivery, effective communications, productivity and streamlined and automated business processes. However, the efficiency saving to the authority over the longer term is difficult to quantify at this stage.
- 7.2 In the short term there is a requirement for additional resources to undertake weeding of existing files, reducing the number of records held in line with the retention schedule. There is also a need to review organisational and management arrangements to maximise the benefits of an electronic records management system. This is likely to lead to some level of reorganisation.
- 7.3 The cost of introducing the first two phases of Comino Universal Government can be met from the current IEG grant. Proposals in the IS/ICT Strategy and IEG3 Statement to introduce a corporate records management system across the whole authority depend on further grant funding. The level of IEG funding for the coming year is not known at the time of writing this report. There will be an annual maintenance cost of approximately £20,000 when the complete system is installed. This cost is likely to be recovered in efficiency savings over the longer term.
- 7.4 In December 2003 the Policy and Finance Committee included a sum of £30,000 towards implementing this legislation within the Council's budget strategy for the coming financial year.

## **8 LEGAL IMPLICATIONS**

- 8.1 There is a statutory duty to provide access to information under the Freedom of Information Act 2000 from January 2005. Enforcement action can be taken by the Information Commissioner. It is a criminal offence to destroy or alter in any way any record that is the subject of a request for information after the above date.

## **9 PARISH IMPLICATIONS**

- 9.1 The Freedom of Information Act is applicable to parish councils.

## **10 RECOMMENDATION**

- 10.1 It is proposed that the Committee **RECOMMENDS**

---

That the Policy & Finance Committee agrees to

- (1) adopt the following policies and guidelines;
  - Data Protection Policy
  - Records Management Policy Statement
  - Electronic Record Management Policy
  - Information Technology Code of Practice
  - Essex Trust Charter and
- (2) the use of the Government Office of Commerce GCat procedure to acquire the Comino Universal Government corporate document management and workflow system.

and further **RESOLVES**

- (1) to endorse the following guidelines:
  - Model Competencies Framework
  - Record Disposal Guidelines
- (2) to consider further reports on the human resources implications of records management and active records procedures in due course.

John Honey

Corporate Director (Law, Planning & Administration)

---

**Background Papers:**

None

For further information please contact John Honey on:-

Tel:- 01702 318004  
E-Mail:- john.honey@rochford.gov.uk



**APPENDIX 1**

**DATA PROTECTION POLICY**

This document sets out Rochford District Council's policy regarding data protection. The Data Protection Acts 1984 and 1998 and the EC Data Protection Directive form the background to the document. The Policy is drafted using the terms of the Data Protection Act 1998, although there are transitional arrangements in respect of certain parts of the Act. The Freedom of Information Act also affects the Council's use of non-personal information and the operation of this policy. The Human Rights Act 1998 will enhance the protection and individual rights given under the Data Protection legislation.

**Table of Contents**

		Page No
<b>1. Introduction</b>		<b>3</b>
<b>2. Definitions</b>	Data	<b>3</b>
	Data Controller	<b>3</b>
	Data Process	<b>3</b>
	Data Subject	<b>3</b>
	Personal Data	<b>3</b>
	Sensitive Personal Data	<b>4</b>
	Processing	<b>4</b>
	Relevant Filing System	<b>4</b>
<b>3. Principles</b>		<b>4</b>
<b>4. Policy</b>	External and Internal Registration / Notification	<b>5</b>
	Amount of data to be held	<b>6</b>
	Subject Access	<b>6</b>
	Public Registers	<b>6</b>
	Disclosures	<b>6</b>
	System Design	<b>6</b>
	Training	<b>6</b>
	Disciplinary Action	<b>7</b>
<b>5. Responsibilities</b>		<b>7</b>

## **1. INTRODUCTION**

The purpose of the data protection legislation is to regulate the way in which personal information about individuals, whether held on computer or in a manual filing system, is obtained, stored, used and disclosed. The legislation grants rights to individuals to see the data stored about them, to require modification of the data if it is wrong and, in certain cases, to compensation. The provisions amount to a right of privacy for the individual.

The Data Protection Act 1998 presents a number of significant challenges for local authorities. There is the extension of the scope of data protection from purely automated records to certain types of paper and other manual records. There are new rules that require that data controllers establish a legitimate basis for the processing of personal data. There are significant changes to the system of registration that existed previously and the impact of the Freedom of Information Act 2000 which comes into force in full in January 2005.

The 1998 Act requires all processing of personal data to be notified to the Information Commissioner and to be kept and used in accordance with the provisions of the Act.

## **2. DEFINITIONS**

To aid the understanding of this document and the provisions of the Data Protection Act, the following definitions are provided for assistance:

**Data** is information that is:

- being processed by means of equipment operating automatically in response to instructions
- given for that purpose (e.g. payroll system)
- recorded with the intention that it should be processed by means of such equipment
- recorded as part of a manual filing system or with the intention that it should form part of a **relevant filing system** (see definition below)
- one of a number of records to which public access is allowed.

**Data Controller** means the Council as the organisation who determines how data is processed.

**Data Processor** means any person, other than an employee of the Council, who processes data on behalf of the data controller (e.g. someone contracted to the Council to print documents containing personal data).

**Data Subject** is the individual about whom personal data is held.

**Personal Data** means data about a living individual who can be identified from that information (or from that and other information in the possession of the data controller). This includes an expression of opinion about the individual, and any indication of the intentions of the data controller or any other in respect of that individual.

---

**Sensitive Personal Data** means personal data consisting of information as to:-

- racial or ethnic origin of the data subject
- his/her political opinion
- his or her religious beliefs or other beliefs of a similar nature
- whether he or she is a member of a trade union
- his or her physical or mental health or condition
- his or her sexual life
- the commission or alleged commission by him or her of an offence
- any proceedings for any offence committed by him or her, the disposal of such proceedings or the sentence of any court in such proceedings.

**Processing** is very widely drawn and means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data including:

- organisation, adaptation or alteration
- retrieval, consultation or use
- disclosure
- destruction of the information or data.

**Relevant Filing System** means any data that is recorded as part of a manual filing system or with the intention that it should form part of a relevant filing system (e.g. "any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible").

### **3. PRINCIPLES**

The Data Protection Act 1998 contains 8 governing Principles relating to the collection, use, processing and disclosure of data, and the rights of data subjects to have access to personal data concerning themselves. These Principles are:

- Personal data shall be **processed fairly and lawfully** and, in particular, shall not be processed unless one of the conditions in Schedule 2 is met. These can be summarised as consent, contract, legal obligation, vital interests, public interest and balance of interest. In the case of sensitive personal data at least one of the conditions in Schedule 3 must also be met, which can be summarised as explicit consent, employment law, vital interests, non-profit associations, manifestly made public, legal claims, justice/statute Crown, medical purposes, ethnic monitoring.
- Personal data shall be obtained only for **one or more specified and lawful purpose** and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be **adequate, relevant and not excessive** in relation to the purpose or purposes for which they are processed.
- Personal data shall be **accurate** and, where necessary, kept up to date.

- 
- Personal data processed for any purpose or purposes **shall not be kept for longer than is necessary** for that purpose or purposes.
  - Personal data shall be processed **in accordance with the rights of the data subject** under this act (this includes the rights of subjects to access the data and to correct it).
  - Appropriate **technical and organisational measures** shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (this relates to data security).
  - Personal data **shall not be transferred to a country or territory outside the European Economic Area** unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

These principles are required as the minimum standards of practice for any organisation with respect to personal data.

#### **4. POLICY**

Rochford District Council supports the objectives of the Data Protection Act 1998. This policy is intended to maintain the confidentiality of personal data held or processed, either on computer or in manual files, and to increase the access given to individuals to information relating to them.

The Policy links to the other council policies including:

- Access to Information Procedure Rules
- Complaints Procedure
- Records Management Policy Statement
- Electronic Records Policy
- Information Technology Code of Practice

Data may also be shared with certain other public authorities in accordance with statutory and other requirements including the Essex Trust Charter (see **Disclosures**). For further information on the legal framework for data sharing see “Public Sector Data Sharing – Guidance on the Law” published by the Department of Constitutional Affairs – November 2003. <http://www.dca.gov.uk>

#### **External and Internal Registration / Notification**

The Council has an external registration/notification with the Information Commissioner. The Register can be searched at <http://www.dpr.gov.uk>. The Rochford District Council Registration references are:

- **Z6617133 Rochford District Council** (5 April 2002)
- **Z5162315 Electoral Registrar of Rochford District Council** (15 December 2000)

The Register Entry gives general descriptions of the type of data processing activities carried out by Local Government. The Register Entry is therefore

supplemented by an internal register of data repositories, maintained by the IT Client Manager.

### **Amount of data to be held**

The Council will hold the minimum personal data necessary to enable it to perform its functions. The data will be erased once the need to hold it has passed. Every effort will be made to ensure that data is accurate and up-to-date, and that inaccuracies are corrected quickly.

### **Subject Access**

The Council will provide to any individual who requests it, in a specified manner, a reply stating whether or not the Council holds personal data about that individual. A written copy, in clear language, of the current data held, will be given. A fee will not be levied for this service. However, there are certain exemptions from the right of subject access, which relate largely to a test of prejudice. For example, personal data that are held for the purpose of the prevention or detection of crime are exempt, to the extent that providing access would be likely to prejudice that purpose. In addition, data may be withheld if it is not possible to release information without disclosure of personal data about other people.

### **Public Registers**

The Council maintains a number of public registers that contain personal data or data that could be used to identify individuals. Strict compliance with the legislation giving rights of access will be used in all cases.

### **Disclosures**

Disclosures of information must be in accordance with the provisions of the Act and the Council's registration/notification. Where the Council has a duty to disclose certain data to public authorities (such as the Inland Revenue, Customs and Excise, Benefits agency), this will be done in accordance with statutory and other requirements. Legal and internal rules limit disclosure within the authority either to council officers or elected members. When a request for information is made, the minimum of personal data will be made available on a need to know basis.

### **System Design**

The Council intends that personal data must be treated as confidential. Computer systems will be designed to comply with the Principles of the Data Protection Act so that access to personal data should be restricted to identifiable system users.

### **Training**

It is the aim of the Council that all staff will be fully informed of their obligations under the Data Protection Acts and aware of their personal liabilities, and where appropriate further training will be given.

### **Disciplinary Action**

The Council expects all of its staff and members to comply fully with this Policy and the Principles of the Data Protection legislation. Disciplinary action may be taken against any employee who breaches any of the instructions or procedures following from this policy.

## **5. RESPONSIBILITIES**

**Overall responsibility** for the efficient **administration** of the Data Protection legislation lies with the Council and is exercised by the **Corporate Director (Law, Planning & Administration)**.

**Day to day responsibility** for administration and compliance with the act is delegated to **Directors and Heads of Service**, for compliance with the Act's provisions within their respective areas of authority. In some cases, this may involve a joint responsibility (for example, where one Division carries out work on behalf of another Division).

All **Officers** and **Members (Councillors)** have a duty to observe the Principles of the Act and the procedures referred to in this document.

Please note: **Councillors** could be regarded as data controllers if they process personal data either manually or by computer, whether on their own equipment or on equipment provided to them by their local authority. Just as any other individual holding and processing personal information about others, Councillors need to comply with the Data Protection Act, and need to notify the Information Commissioner of all purposes for which they hold and process personal data.

However, where holding and processing personal data about individuals *in the course of undertaking council business*, the elected member will be covered by the authority's notification, and have the same responsibilities in respect of data protection as an employee of the authority.

Further guidance on **Data Protection for Councillors** can be found in the document of that name which has been published by the Improvement & Development Agency (I&DeA). Their website can be found at [www.idea-infoage.gov.uk](http://www.idea-infoage.gov.uk).

**Individuals who do not handle data** as part of their normal work have a responsibility to ensure that any personal data they see or hear goes no further. This includes personal data and information extracted from such data,

thus, for example, unauthorised disclosure of data might occur by passing information over the telephone, communicating information contained on a computer print-out or even inadvertently by reading a computer screen.

---

**APPENDIX 2**

**RECORDS MANAGEMENT POLICY STATEMENT**

Rochford District Council recognises that the efficient management of its records is necessary, to support its core functions, to comply with its legal and regulatory obligations and to contribute to the effective overall management of the authority. This document provides the policy framework through which this effective management can be achieved and audited. It covers

1. Scope of the policy
2. Responsibilities
3. Relationship with existing policies
4. Available guidance for implementation of the policy
5. Contacts

**1. SCOPE OF THE POLICY**

- 1.1 This policy applies to all records created, received or maintained by officers of the Council in the course of carrying out their duties including provision of services and corporate functions.
- 1.2 Records are defined as all those documents which facilitate the business carried out by the Council and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically.
- 1.3 Records management is defined as a field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.
- 1.4 A small percentage of the Council's records will be selected for permanent preservation as part of the County's archives, for historical purposes and as an enduring record of the conduct of business.

**2. RESPONSIBILITIES**

- 2.1 The Council has a corporate responsibility to maintain its records and record-keeping systems in accordance with the regulatory environment. The Corporate Management Board member with overall responsibility for this policy is the Corporate Director (Law, Planning & Administration).
- 2.2 The Head of Administrative and Member Services is responsible for drawing up guidance for good records management practice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of information.



2.3 Heads of Service have responsibility for ensuring records management practice and procedures within their divisions comply with this policy and guidelines.

2.4 Individual employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the Council's records management guidelines

### **3. RELATIONSHIP WITH EXISTING POLICIES**

This policy has been formulated within the context of the following Council documents

- Information Strategy
  - Freedom of Information policy
  - Data Protection policy
  - Electronic Records Management Policy
- (available at [www.rochford.gov.uk](http://www.rochford.gov.uk))

Compliance with this policy will in turn facilitate compliance not only with information-related legislation but also with all other legislation or regulations (including audit, equal opportunities and the Council's Constitution) affecting the authority.

### **4. GUIDANCE**

Guidance on the procedures necessary to comply with this Policy is available at [www.rochford.gov.uk](http://www.rochford.gov.uk) or from the Central Services Manager. This guidance covers;

- records creation
- business classification (for filing schemes)
- retention periods for records
- storage options for records
- destruction options for records
- archival records: selection and management
- external codes of practice and relevant legislation

### **5. CONTACTS**

Central Services Manager: Dawn Tribe x3828

---

**APPENDIX 3**

**ELECTRONIC RECORDS POLICY**

**1 PURPOSE**

This policy aims to meet the requirements of good records management to cover all the electronic record collections and planned electronic records of Rochford District Council.

The policy covers:

- The requirements that must be met for the records themselves to be considered as a proper record of the activity of the Council
- The requirements for systems and processes that deal with records, maintaining quality and reliability, to provide a valuable information and knowledge resource for the whole organisation
- Its place within the strategic and policy framework of the organisation
- The implementation plan across the organisation
- The use of approved technical solutions
- The resources needed to preserve the record intact
- The policy governing Registration process
- The policy governing access
- The policy governing security
- The policy for reviewing the policy and checking the quality of implementation.

These will be updated according to a development plan issued within the policy-making areas of the Council.

**2 REQUIREMENTS**

Electronic records within the authority are to be clearly identified following a pattern of treatment similar to that previously given to paper records. They must be able to be preserved and stored for the required period within the Council. They will be selected using defined selection criteria and can be transferred to other organisations for future preservation, or destroyed once they are no longer of operational use. In order to ensure that the information constitutes a record the Council is required and endeavours at all times to ensure that:

- The record is present
- The information needed to reconstruct activities and transactions that have taken place is recorded.
- The record can be accessed
- It is possible to locate and access the information and present it in a way that is true to the original presentation of the information

- 
- The record can be interpreted
  - A context for the information can be established showing when, where and who created it, how it was used and how it is related to other information
  - The record can be trusted
  - The information and its representation exactly matches that which was actually created and used, and its integrity and authenticity can be demonstrated beyond reasonable doubt
  - The record can be maintained
  - The record can be deemed to be present and can be accessed, interpreted and trusted for as long as necessary and on transfer to other approved locations, systems and technologies.

### **3 PROCESS REQUIREMENTS**

The Council deems that electronic records are assets that require careful control and the diligent application of standards to all systems and processes within the Council. The systems and processes will be required to:

- Identify whether they deal with records, electronic records or potential electronic records
- Provide information on the records or potential records as required for inclusion as part of a collection in the inventory of record collections
- Provide the records for registration, transfer or disposal according to the records management guidance
- Keep the records secure and monitor access in accordance with records management guidance
- Have regard for legal requirements such as Data Protection, Freedom of Information and copyright legislation.

If they do deal with such records, the system or process must maintain them so that the record nature remains intact.

### **4 TRANSITIONAL REQUIREMENTS**

The Council will monitor electronic records and potential electronic records to ensure that:

- Records that should be captured are being processed electronically if they do not appear in the paper record
- There is no unwarranted duplication between the paper and electronic record collections
- There is a distinction made between the electronic documents which are printed, printed records that reside in the paper record systems and other original documents that are retained as electronic records (possibly to be passed to an electronic record keeping system)
- An inventory of record collections will be created to ascertain the nature and type of records and potential records within collections. Care must be taken to ensure a good level of control of the record creating systems and that the record's nature is preserved appropriately in the transitional period.

- 
- The implementation of any Record Management System should clearly show where the record is located and in which form it is held.

## **5 LINKED POLICIES**

There will be requirements in other policies that electronic records must meet. The following are made explicit by reference:

- **Following best practice**  
Electronic records should be managed in accordance with relevant codes of practice for records management – in particular, the forthcoming ISO/CD 18489-1 which provides an overall guide to best practice in records management
- **The Council's e-government strategy**  
Electronic records will underpin e-government, providing records for business use, corporate knowledge management and evidence-based policy making, evidence for accountability and historical use.
- **Freedom of Information**  
*Electronic records will have to adhere to procedures under the Freedom of Information legislation and the associated Lord Chancellor's Code of Practice on the Management of Records*
- **Data Protection**  
Electronic records will have to adhere to procedures under the Data Protection Act 1998.
- **Existing records policy** (that is, paper-based policies)
- **Audit policy**  
Electronic records will have to meet audit requirements.

## **6 TECHNICAL CRITERIA**

The Council applies technical criteria to the technologies that process electronic records. This ensures that:

- It is technically possible for the electronic records to meet record requirements starting from when they are created and for as long as they are needed
- Systems will be selected on the basis of how well they will cope with electronic records, to prevent any loss of the record because of incompatibility or insufficient safeguards being used
- Records management systems adhere to the minimum functional requirements as stated in the PRO publication Functional Requirements for Electronic Records Management Systems.
- The systems designed for records management are capable of and useful for record keeping activities
- Metadata is captured and can be used for referencing the information by using defined terms that are user-friendly and accurate.

## **7 REGISTRATION**

The approach the authority has to registration involves:

- Classifying of the records into series that have meaningful titles and a consistent reference code
- Setting a responsibility on individuals forming record items to allocate them to a series and if necessary a sub-series or sub-sub-series
- Saving sequences of reference numbers that can cover series with both electronic and paper records
- Checking that the correct records have been allocated to the sequence and that meaningful titles are used
- Auditing lists of the references used so that the registration system makes sense and records can be found in appropriate search sequences.

## **8 ACCESS**

The authority will use access controls to allow the records to be viewed by all relevant parties, and offer a mechanism for opening up some of the information for use outside the Council. The actual controls will depend on many factors but the general principles can be summarised as:

- Electronic records will be made available for continuity of actions. The creators and managing individuals or groups should have access to relevant information
- Roles or bodies within the Council which have been identified as being able to make an accurate judgement will decide on the sensitivity of the record. This judgement may be on a whole series or simply cover individual items. It will identify any restrictions on the records and it will highlight any groups or individuals within the organisation who should have access
- Any judgements, including any background reasons for withholding or masking information within the record or record series, are to be recorded. The resulting record will be kept for at least as long as the records in question; however it may not have the same access status as the main record
- The Council will not seek to put blanket restrictions on a record series if only some of the individual records are judged sensitive
- Information taken from the records or record metadata may be subject to legislation requiring it to be either withheld or made more widely available outside normal business needs (or even outside the Council itself). For example there may be a need for compliance with data protection or Freedom of Information legislation
- All records are part of the corporate memory. Unless restricted, due to legislation or as a result of a judgement, they will be made readily available within the Council. This may be subject to volume restrictions because of technical limitations or copyright reasons
- Any access arrangements will be made for a specified duration and these will be reviewed according to a schedule identified during appraisal.

## **9 SECURITY**

The authority takes all reasonable steps to ensure that the electronic records and processes dealing with them are secure. Once recorded and registered in the system, they will be safe from alteration, misinterpretation or loss.

The steps include:

- Informing staff and complying with records management best practice
- Using a corporate policy and organisational procedures, where they exist, and helping to determine new policy and procedures where they do not
- Training staff to use the records management systems for an accurate representation of the records using only relevant metadata, thereby ensuring consistency in record registration and metadata without loss of context and control
- Auditing the systems to trace any deviation from procedure
- Offering solutions to rectify mistakes or altering the procedures to accommodate better ways of working
- Setting up business continuity plans to ensure a constant service is maintained in spite of any technical or strategic hitches that may occur
- Enforcing access restrictions with user IDs and passwords, setting user lockouts
- Maintaining disaster recovery plans that include replicating electronic records on a physically secure back-up and safeguarding the information from technical failures.
- Implementing strict back-up cycles with updates for new records and metadata, ensuring that any destroyed or transferred records are also promptly physically cleaned from the back-ups
- Labelling the replicated records as a replica set and making sure these cannot be used as the master set, unless the original has been destroyed accidentally or following a disaster

## **10 PLANNED REVIEW**

The authority will endeavour to follow the policy within all relevant procedures and guidance used for operational activities. Interpretation of the policy will be monitored and there will be a regular planned audit to assess how the policy is being put into practice.

The audit will seek to:

- Identify areas of operation that are covered or not covered by the policy and to identify which procedures and/or guidance should adhere to the policy
- Follow a mechanism for adapting the policy to cover missing areas if these are critical to the creation and use of electronic records and use a subsidiary development plan if there are major changes to be made

- Set requirements by implementing new procedures, including obtaining feedback where the procedures do not match the desired activity
- Highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment to related procedures such as security and access.

## **11 PRESERVATION POLICY**

The Council will seek to preserve electronic records during any change in the infrastructure so that they can still satisfy the original policy requirements.

Preservation needs must be satisfied when there are changes in:

- The technology that processes the electronic records
- How this affects the way records are processed throughout the records' existence
- Organisational structures and how these are interpreted and give the records context
- The definition of terms used in the metadata and within the records themselves
- The classification of the electronic records including how the records are grouped and described so that they can be presented in a way consistent with the original understanding of the subject when the record was created.