Records Management Policy

January 2017

Revised January 2024
Scheduled for review January 2025

Revision History

Version	Date	Summary of Changes	Author
0.1	Sept 2016	Initial draft	Teresa Maley
0.2	Nov 2016	Draft for approval to IGG	TM
0.3	Jan 2017	Remove reference to RM Toolkit	TM
1.0	16 Jan 2017	Final version	TM
1.1	26 July 2018	Revised to reflect Risk Structure and DP Changes	Jaimie Taylor
2.0	17 September 2018	Final approved by IGG	
2.1	16 April 2021	Review of Records Management Policy, inclusion of Managing the Disposal of Records Policy and Disposal of Confidential Waste Management Policy	JW
3.0	1 July 2021	Final approved by IGG	
3.1	18 January 2024	Review	Jenna Paterson
3.2	19 January 2024		Nicola Driver
4.0	8 February 2024	Final approved by IGG	

Table of contents

Contents

Introduction

At Scottish Borders Council (the Council) we recognise that the effective management of our records, regardless of format, is essential to support core functions, comply with legal, statutory and regulatory obligations, and to demonstrate transparency and accountability. Records are a vital information asset and a valuable resource for the Council's decision-making processes, policy creation and operations, and must be managed effectively from the point of their creation until their secure disposal.

Managing information assets as records allows the Council to comply with our statutory duties effectively and timeously, assures us that our information is accurate and up to date, minimises duplication and reduces cost. By agreeing common standards and monitoring adherence to these standards, the Council's Records Management policy conforms to the risk-based approach to business adopted by the Council.

Purpose

The purpose of this policy is to demonstrate the importance of managing records effectively both within the Council, and by those who help to deliver Council functions, to outline key aims and objectives in relation to record keeping, and act as an instruction for the support and delivery of records management policies and procedures across the Council.

This policy supports the Council's Information Governance Policy, approved by the Council's Information Governance Group.

Audience

This policy is relevant to all staff, including those who are mobile working, or working from home, contractors, agents and representatives, volunteers, permanent and temporary staff, those on secondment, work experience placements and all others who process Council information.

Scope

This policy relates to all Council records, whether it is created by Council staff or by someone on the Council's behalf, including information that is shared with the Council. This policy applies to all records regardless of format or medium, paper (including Iron Mountain), electronic (including emails, SharePoint, information held on handheld devices, departmental systems, applications, and cloud), audio, video (including CCTV) and photographic (including biometric data).

This policy will cover

1. What records management is
2. The Council's Information Asset Register
3. Dealing with electronic records
4. Email management
5. Dealing with paper records
6. Version control
7. Vital assets
8. Security classification
9. Records retention periods
10. Iron Mountain

11. Disposal policy
12. What good Records Management is
13. Records Management Plan
14. Staff roles and responsibilities
15. Access to records
16. Risk, policy monitoring and review
17. Policy compliance
18. Related policy and guidance

This policy does not cover the management of historical records and archive collections that have been transferred to The Heritage Hub in Hawick.

Records Management Policy

What is Records Management?

Records Management is defined as an area of management responsible for the efficient and systematic control of the creation, storage, management and disposal of records.

Why is a Records Management Policy important?

A Records Management Policy establishes records management as a corporate function. A Policy is essential to help manage records in an appropriate and suitable manner for as long as they are required for business purposes.

It forms a core part of any records management system, regardless of format.

Information Asset Register

What is an Information Asset Register?

The Information Asset Register is a tool to help staff understand and manage the Council's information assets and risks around those assets.

The Information Asset Register is managed by the Council's Information Management Team. Information Asset Owners within each department are responsible for ensuring entries are included on the register and records are managed effectively to ensure risk is monitored.

Why have an Information Asset Register?

The Information Asset Register is important in order to protect and exploit the information the Council holds; we must understand what it is and who can use it. Identifying the information assets held reduces duplication so that less time is spent searching for information and verifying which version is the reliable record. Understanding what records are held promotes routine and relevant disposal of records so that there is less to manage and there is an audit trail showing that destructions were carried out properly. Records can (by managing the risks) be managed in the same way as other assets in the business planning process and the risk of error (data breach), fines and negative publicity can be controlled.

Effective electronic records

What should be considered when creating a record?

The Council's records must be accurate, authentic, and comprehensive in content in order to provide reliable evidence of Council business.

The Council's records must be adequate for the Council business they support and based on good quality data.

The Council's records must be titled and referenced in a manner consistent and relevant to the business activity to ensure that they can be easily retrieved, understood, and managed. Records must be easily retrievable by relevant staff.

The Council's electronic processes should be able to port, erase or rectify.

The Council must be able to evidence that it has designed its records management processes from the outset with good records management practices.

How electronic records should be stored

The Council's records must be adequately protected and stored securely to prevent unauthorised access.

The Council's records must be stored on the Council's network or in valid electronic record keeping systems.

The Council's records must always be retrievable for business, performance, audit, to allow individuals to exercise their rights and freedoms over their records, and data sharing purposes until such time as records are securely destroyed.

There is a routine risk review of the Information Asset Register. This review is carried out by the Information Asset Owner and Information Management Team which highlights where the Council is not meeting the records management principles.

In order for records to be protected appropriately in terms of information security risk and security classification, the Council should ensure there is a collaborative piece of work between Information Asset Owner, CGI security and where relevant, third party organisation – to identify sensitive assets and then protect accordingly.

How electronic records should be managed

The Council's records must have access controls, audit logging, and business and security classification in place that are appropriate to the sensitivity and risk of their content.

The Council's records must remain accessible and usable for as long as they are required to be retained under the Council's Retention Schedules. This includes versions of a document which may be required to be kept for a different period of time.

The Council's records must not be shared (internally or externally) unless for a specified purpose. If information requires to be shared internally, consideration should be given to providing a link or location rather than a copy of the document. This avoids unnecessary duplication. Where records contain sensitive information staff must ensure the recipient is correct, staff should always expand on distribution lists before sending. Emails containing sensitive information must be transferred by using encryption or password protection before sending to an unsecure email domain.

To minimise duplication, consideration must be given to records held in paper form and electronic format to avoid the Council holding unnecessary copies of information.

Can electronic records be stored for permanent preservation?

Electronic records scheduled for permanent preservation should be discussed with the Councils IT department.

Email management

Why is email management important?

Reducing the volume of emails held allows the Council to be more effective. Regularly going through emails and deleting (from all email folders) emails which you do not require helps you to be more organised, and allows the retrieval of important communications when necessary. Emails relating to specific case records should be stored appropriately, ensuring only relevant and adequate information is kept.

Email management also assists the Council when responding to information requests.

Effective paper records

What should be considered when creating a record?

The Council's records must be accurate, authentic, and comprehensive in content in order to provide reliable evidence of Council business.

The Council's records must be adequate for the Council business they support and based on good quality data.

The Council's records must be titled and referenced in a manner consistent and relevant to the business activity to ensure that they can be easily retrieved, understood, and managed. Records must be easily retrievable by relevant staff.

The Council must be able to evidence that we have designed our records management processes from the outset with good records management practices.

How paper records should be stored

The Council's records must be adequately protected and stored securely to prevent unauthorised access.

Day to day active files which do contain sensitive information must be stored in a secure and restricted location.

Inactive files, which are no longer needed for immediate or routine use should be considered for digitisation in the first instance.

Council records must always be retrievable for business, performance, audit, and data sharing purposes, and to allow individuals to exercise their rights and freedoms over their records, until such time as records are securely destroyed.

Where there is a requirement to retain a paper record, we encourage the use of Iron Mountain,for when records require to be retained for long periods; documents which are high risk or there is a legal obligation for the record to be kept.

There is routine risk review of the Information Asset Register. This review is carried out by the Information Asset Owner and Information Management Team which highlights where the Council is not meeting its records management requirements.

How paper records should be managed

The Council's records must have access controls, audit logging, and business and security classification in place that are appropriate to the sensitivity and risk of their content.

The Council's records must remain accessible and usable for as long as they are required to be retained under the Council's Retention Schedules. This includes versions of a document which may be required to be kept for a shorter or longer period of time.

The Council's records must not be shared (internally or externally) unless for a specified purpose. If information requires to be shared internally, consideration should be given to providing a link or location where there is an electronic copy. When sharing sensitive information ensure it is addressed to the correct recipient and not left unattended.

Can paper records be stored for permanent preservation?

Certain files, that are not active, can be stored for permanent preservation. Staff must refer to the Council's Appraisal of Records for Permanent Preservation Policy for guidance.

What is version control?

Version control allows staff to manage changes to records over time, storing these modifications electronically or physically. Version control involves a process of appropriately naming and distinguishing between a series of draft records which lead to a final (or approved) version. It provides an audit trail for the revision and update of draft and final versions.

Why is version control important?

Version control is important for records that undergo significant revision and redrafting, and it is particularly important for electronic records. This is because they can be easily changed by a number of different users. Knowing the version of a record is important to ensure everyone is working on the latest version. Version control is also important if you are working on a collaborative record with several contributors.

Vital Records

What is a vital record?

Vital records are those that are necessary for the Council to continue to operate in the event of a disaster. The Council's records that are vital to the continuity of Council business must be identified as Vital Records on the Information Asset Register and in the business continuity plan. Categories of vital records may include, records stored in a particular system, legal, financial, commercial and disaster plans (including security, flood, and fire).

Why is identifying vital records important?

It is necessary to identify vital records to ensure that the record remains secure, accessible and can be easily located by relevant staff, even during a disaster. The quickest way to identify the importance of a vital record is to imagine the scenario without access to the information. Vital records form an integral part of disaster recovery and business continuity planning. Extra technical and organisational measures must be in place to protect vital records.

How vital records should be looked after

Electronic records

Electronic records must be stored on servers, ideally in the United Kingdom, to ensure they are protected by appropriate back-ups and emergency recovery. It is important staff do not assume where personal data is transferred to.

It is important that any vital records/systems holding vital records need to be shared with CGI to ensure they are retained for recovery from disaster.

Paper records

Ensure vital records are available in multiple formats in case of an emergency to prevent a single point of failure.

There are a number of ways of doing this:

1. Scan and save a copy of the vital record electronically;
2. Store a copy of the vital record at an off-site storage facility (Iron Mountain); and
3. Store a copy of the vital record in another Council building.

Staff must know the location of the electronic and paper vital records, and access to records should be restricted to relevant individuals. Building and information security measures should be taken into account.

What is security classification?

The Council uses protective marking to mark electronic and paper records based on its content, and the level of security it requires when being shared, handled, and stored. Staff should be aware of what security classification marks mean for when sharing records or when records are shared with the Council:

1. OFFICIAL SENSITIVE - this is information regarding the business of the Council or of an individual which is sensitive. In some instances, an email of this category may be marked as PRIVATE.

2. OFFICIAL - this is information relating to the business of the Council and does not include sensitive information.

3. UNCLASSIFIED – this is not information about the business of the Council.

Why is security classification important?

Information classification is a vital part of managing Council records. If staff do not classify records appropriately, records are at risk of not being managed in line with relevant legislation.

Records Retention Schedule

Why have a records retention schedule

The principles governing the retention and subsequent disposal of records apply regardless of their format (although in practice the procedures used to manage electronic and paper records will differ).

An appropriate records retention schedule helps the Council to comply with a range of statutory and regulatory requirements. It is particularly key for:

- The Public Records (Scotland) Act 2011;
- The Data Protection Act 2018;
- The UK General Data Protection Regulation;
- Freedom of Information (Scotland) Act 2002; and
- Environmental Information (Scotland) Regulation 2004.

A records retention schedule can also provide the basis for different streams of information governance:

- It contributes to the Council's Information Asset Register;
- It provides a structured approach to information risk analysis;
- Security classification and identification of vital records can be applied; and
- In many cases, the schedule will be linked to a business classification scheme which maps out the Council's functions and activities.

The Council needs a records retention schedule to ensure that:

- Records are kept or destroyed consistently, and disposed of in an appropriate manner;
- Records are kept for as long as necessary to meet statutory, regulatory and business requirements;
- Resources are not misused on storing records longer than is necessary;
- The preventive measures are in place to ensure records are stored, managed and handled appropriately;
- The Council can demonstrate accountability for records which are no longer held (for example, in response to a Freedom of Information (FOI) request);
- Staff working with records understand their responsibilities and are given clear information about how long records should be kept and how to destroy records appropriately;
- CGI are aware of the retention period for electronic records to ensure this is built in when implementing or decommissioning a system on behalf of the Council.

Understanding the value of records

Any action in managing records should be based on an understanding of the value of that record to the Council – to the department, service and colleagues.

- Records that need to be kept by law: certain pieces of legislation set out types of information that should be kept and how long they should be kept for, for example, the Health and Safety at Work Act.
- Records that have ongoing business value: information of business value is that which is needed to carry out business functions or to provide evidence of a business activity. It is important to identify, if you regularly work with another service, whether you hold a key part of their records and agree and document how those partial records will be managed compliantly and cost effectively.
- Records that have re-use value: it is important to consider whether Council records might have value from a re-use perspective and publish accordingly. The Freedom of Information (Scotland) Act 2002, the Environmental Information (Scotland) Regulations 2004, the Re-use of Public Sector Information Regulations 2015 and the INSPIRE Regulations 2009 require the Council to publish as much information as possible so that, for example, datasets and the records they contain can be used by the general public in innovative ways.

- Records that are of historical value: Information of historical value should be selected for permanent preservation at the Council Archives that are managed by Live Borders Heritage Hub. Decisions about the value of records should be based on the content and context rather than on format. This includes significant policy documents, records of significant decisions, and records about notable events persons or public issues.

How long records should be retained for

The Council has adopted the Scottish Council Archives Records Retention Schedules (SCARRS) business classification scheme. Business classification describes the Council's functions and activities. These retention schedules are published on the intranet under Information Management broken down by each business classification such as Human Resources and Finance.

Within Scottish Council Archives Records Retention Schedules staff may expect to find a clear legal requirement setting out the retention requirement for most records. There are very few record types governed by statutory retention periods. In most cases, it is necessary to consider how long a document is required and balance that against the costs and risks of keeping it, to arrive at an appropriate retention period.

For that reason, it may be entirely appropriate for two Local Authorities to have different retention periods for the same or similar records. Another Local Authority may have a different approach to risk or a different analysis of the business requirement.

Iron Mountain

What is Iron Mountain?

Iron Mountain is an off-site storage facility used by Council departments to store records. Iron Mountain protects these records on the Council's behalf and is contracted to destroy records when requested to do so. Iron Mountain sub-contracts Shred-It to carry out physical destruction.

There is a cost to the department to store files at Iron Mountain. It is important that the department determines whether Iron Mountain is the appropriate place to store inactive files.

Can I store records at Iron Mountain?

Staff should contact the Information Management Team to discuss storage at Iron Mountain.

Disposal Policy

What is a Disposal Policy?

A Disposal Policy is concerned with managing the secure permanent disposal of records owned by the Council that are no longer required. Records containing sensitive data (personal and commercial) must be protected and disposed of correctly.

Why is a Disposal Policy important?

Understanding which records are no longer requiredis an important part of effective records management. Disposal of records must be done responsibly through a clear understanding of the Council's business functions and with consideration of:

- The value of the record to the whole Council – not just the service that created it;
- Legislative retention requirements; and
- The technology that supports the record.

The Council must be able to demonstrate:

- How long it is required to keep particular records;
- That records have been disposed of following the Council's process when they are no longer needed;
- Why records are no longer held.

Keeping records for longer than is required exposes the Council to risks, including:

- Reputation: under the Data Protection Act 2018 and the UK General Data Protection Regulation, personal data should be held for no longer than necessary and must be up to date. The Regulator – Information Commissioner Office – can investigate and make public the Council's failings that lead to a complaint or data breach. On the other hand, failure to provide information – at all, in part or on time – could lead to bad publicity under the Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004.
- Efficiency: the more records held the slower the search when responding to an information request from the public. Reviewing and disposing of records routinely means the Council can be sure that what the Council holds is complete, available and accessible to permitted users for as long as it is needed.
- Cost: storing paper records that have no business purpose, for example, in Iron Mountain (the Council's off-site storage facility) is expensive as is the cost of maintaining, preserving and providing on request digital records that are no longer required. Non-compliance with legislation can lead to financial penalties.

How electronic records should be disposed of

Planned disposal of records is important for digital records. Consideration of records retention and destruction when first adopting new systems of technologies is essential for good records management. For some technology it will be possible to have disposal built-in and to provide for automatic deletion of records, and for others it is not possible, and it has to be managed separately. This could include manual deletion or ensuring that a third party – the owner of the product – destroys Council records in agreement with the contract.

Third parties are sometimes required to keep the necessary amount of Council records for their own purpose such as to comply with legislation applicable to them and audit purposes. It is important that staff are aware of what they hold and the retention date for Council records (including back-ups held). It is important to ensure retention is clearly documented to ensure this can be followed up with all relevant parties at that time.

Delete does not always mean delete in a digital world and it is often possible to recover digital records after they have been deleted. For example, storing records in the Cloud means that it is impossible to remove in entirety and the Council must take a risk-based approach. Where possible, records must be permanently removed from all electronic means where a record is no longer required.

Where records stored on media, including CD and USB, appropriate destruction methods must be used such as ensuring records are permanently deleted from all files, including the recycling bin (on the desktop), or the media is securely disposed of.

How paper records should be disposed of

Records containing sensitive data, including personal and commercial, should be disposed of using confidential waste. This applies to all staff, and anyone handling this type of record on the Council's behalf.

Staff homeworking and working off-site must be careful when they are disposing of Council records and must ensure this is done securely. Staff must not use home waste disposal or public bins/recycling units to dispose of sensitive data. Staff must bring all Council records that are no longer required back to Council offices to dispose of securely.

What steps can be taken to ensure good Records Management?

There are several actions that can be taken to ensure Records Management is complied with across the Council.

- It is suggested that staff identify a time of the week when they can focus on Records Management – make it a team task and give it a name such as, Tidy Friday!
- Ensure the record is documented on the Council's Information Asset Register – this includes the sections on business classification, retention and destruction – non-compliance means that the asset will be risk rated as Amber or Red
- Understand what records you hold, including the purpose it is held for, who can have access, how long it should be retained and how it should be disposed of
- Identify records scheduled for destruction using the Council's retention schedule and create a destruction record. Some digital systems automatically capture this information, for others, when destructions are complete protect the destruction record from amendment
- Understand what is considered sensitive data, including personal and commercial, and dispose of it using the Council's confidential waste
- Publish as much as possible on the Council's internet – be open and transparent
- Retain only what is necessary - any records you hold should be removed and destroyed appropriately so the Council retains only what is required for business purposes
- Think before sending – consider picking up the phone rather than creating a written record
- Think before sharing records – provide a link where possible
- Build records management into digital systems and applications – consult with the Information Management Team before purchasing new systems, applications or signing up to free websites. A Data Protection Impact Assessment may be required where personal data is involved.
- Think about records management before moving offices or decommissioning a service
- When removing paper records from filing cabinets and storage, check the record contents to ensure they are what they say they are, and destroy securely

Confidential Waste

What is Confidential Waste?

Confidential waste is defined as any sensitive data that can be used to identify individuals (including staff), including their name, address, contact numbers or any financial data. Examples of financial data may include invoices and quotes that is not already in the public domain.

How do I destroy Confidential Waste?

Confidential Waste at Council Headquarters

Confidential waste disposal bins have been placed throughout Council Headquarters. These bins must be used to dispose of records that contain sensitive data that are no longer required.

These bins are emptied by a third party on a scheduled basis. This third party takes all records placed in these bins to dispose of securely off premise.

Confidential Waste at all other Council properties

This is a service provided by the Cleaning and Facilities department, Assets and Infrastructure. The process is to identify records for destruction and request confidential shredding bags from Facilities Management. Once the bag is full and sealed a collection can be arranged through the completion of the form on the intranet. Sealed bags must be stored in a secure area within the property and will be collected by Cleaning and Facilities staff.

Cleaning and Facilities staff will remove the confidential waste and transport it to a secure area at Council Headquarters for collection by the contractor of the confidential waste.

How Confidential Waste should be stored before collection

- Do not leave sensitive data in Confidential Waste bags in public areas;
- Confidential Waste bags must be always stored in a secure and restricted area; Do not put Confidential Waste in black bags – there is a high risk of it ending up in general waste.

How Confidential Waste should be disposed of

Confidential Waste collection must be arranged through Cleaning and Facilities, Assets and Infrastructure.

Records Management Plan

The Public Records (Scotland) Act 2011 places an obligation on the Council to produce a Records Management Plan which sets out the Council's arrangements for the effective management of all records.

A joint Records Management Plan for Scottish Borders Council and Scottish Borders Council Licensing Board has received approval by the Keeper of the Records of Scotland.

The Chief Executive of the Council and Clerk to the Scottish Borders Licensing Board are the senior officers responsible for the Plan. The Senior Information Risk Owner (SIRO) is responsible for the overall management of Scottish Border's Council and Scottish Borders

Licensing Board public records. The Information Asset Owner of the Records Management Plan is the Council's Information Manager.

Each new Records Management Plan requested by the Keeper of the Records of Scotland will be approved by the Council's Corporate Management Team and signed off by the Chief Executive and Clerk to the Licensing Board before submitting to the Keeper for approval.

Roles and responsibilities

The Council takes a risk-based approach to information management and the Records Management function is managed in this context. The SIRO convenes an Information Governance Group with representation from all parts of the business. The Information Governance Group reviews, monitors and approves all information management policies through quarterly meetings. The meetings are themed – once a year the theme is Records Management.

The Council's Information Management Team duties include creation and implementation of policy, guidance and training and awareness on records management. The Information Asset Register is an effective records management tool that helps ensure compliance with the Policy.

Within the Council, there are Strategic Information Asset Co-ordinators and Operational Information Asset Owners who manage the information assets, cascade training and measure risk on the assets that belong to their business.

All Council staff must undertake mandatory training (e-learning) on information management and security.

All Council staff have the responsibility to manage records effectively, through the documentation of all decisions and actions made by the Council.

All Council staff have the responsibility to ensure effective maintenance of records throughout their lifecycle, including access, tracking and storage of records, the timely review of records and their ultimate disposal - whether this be transfer to archive for permanent preservation, or confidential destruction.

All Council staff have the responsibility in communicating this information to CGI to ensure records are accessed, tracked, stored, and disposed of in accordance with the Councils requirements.

<u>What training is available?</u>

Training is provided to all staff in order to highlight and increase awareness of their responsibilities in relation to information governance, records management, data protection, information access and information security. E-Learning training is mandatory for all staff. Bespoke training and awareness sessions can be requested from the Information Management Team.

Staff with operational responsibility for records management must ensure they understand their roles and responsibilities and remain proactive in their management of record keeping.

Access to Council records

The Council follows guidance from the UK Information Commissioner in creating policies, guidance and training about Data Protection legislation and acknowledges that good records management (along with technical and organisational measures) supports the public's rights to access their personal data held by the Council as well as reducing the burden on staff in administering Subject Access Requests made under the legislation.

The Council follows guidance from the Scottish Information Commissioner in creating policies, guidance, and training on requests for information made in respect of the Freedom of Information (Scotland) Act 2002 (FOISA), the Environmental Information Regulations (Scotland) 2004 and other relevant information regulations. In particular, the Council recognises the value of the FOISA s61 Code of Practice on the Management of Records in promoting good record keeping as a way of complying effectively with the Act and lowering administrative costs to the Council.

Departments are encouraged to routinely publish Information on the Council Website, if that information is regularly requested by members of the public through information requests.

Risk, policy monitoring and review

The Information Governance Group is responsible for monitoring information risk. This group reviews and monitors policy. There is one theme per quarter: Records Management, Data Protection and Information Access, Information Security, Information Governance.

This policy and associated guidance are scheduled for review by the Information Governance Group annually when Records Management is the review theme.

The Information Governance group reports to the Corporate Management Team to ensure information management is monitored and adhered to, and, where applicable, endorsed at executive level in the Council.

Records Management Policy Compliance

Exceptions to policy

Any deviations and/or exceptions to this policy must be risk assessed and approved in advance by the Council's Senior Information Risk Owner (SIRO). For advice and assistance please contact the Information Management Team.

Non-compliance

Any member of Council staff, contractors, sub-contractors, and all other Council designated agents found to have violated or misused the recording functions and policy requirements, may be subject to disciplinary action.

Always speak to your line manager in the first instance or contact the Information Management Team.

Related policies and guidance

Related policies and guidance are on the intranet pages for Information Management and Information Technology.

Mandatory information management and Information security e-learning modules are available on SBLearn for individuals and groups to complete. Other training modules are also available on the site.

Information about the Public Records (Scotland) Act, Records Management Plans and Proper Arrangements under the Local Government Scotland Act can be found on the National Records of Scotland website.

Information on Data Protection legislation can be found on the website of the UK Information Commissioner.

Information on the Freedom of Information (Scotland) Act and associated regulations and codes of practice is on the website of the Scottish Information Commissioner.