SCOTTISH MINISTERS'
CODE OF PRACTICE ON RECORDS MANAGEMENT
BY SCOTTISH PUBLIC AUTHORITIES

UNDER THE
FREEDOM OF INFORMATION (SCOTLAND) ACT 2002

16 December 2011

SG/2011/233

Prepared in consultation with the Keeper of the Records of Scotland and the Scottish Information Commissioner.

Laid before the Scottish Parliament by the Scottish Ministers on 16 December 2011 under section 61(6) of the Freedom of Information (Scotland) Act 2002

Contents

Introduction

Part 1: Records Management

Part 2: Review and transfer of records to public archives

Foreword

The Freedom of Information (Scotland) Act 2002 (‘FOISA’) and the Environmental Information (Scotland) Regulations 2004 (‘EIRs’) enable the public to access information held by Scottish public authorities. These regimes require authorities to either make available the information requested by an applicant or to explain why the information is being withheld. Public authorities subject to FOISA must also have a Publication Scheme which sets out the information that they will routinely publish. The Scottish Information Commissioner is responsible for enforcing and promoting both regimes.

Under section 61 of FOISA, Scottish Ministers may publish a Code of Practice (‘the Code’) which describes the practice which they consider would be desirable for Scottish public authorities to follow in connection with the keeping, management and destruction of the authorities’ records. The Scottish Government has consulted the Keeper of the Records of Scotland (‘the Keeper’) and the Scottish Information Commissioner (‘the Commissioner’) about the content of the Code, which has been laid before the Scottish Parliament. It supersedes the previous Code issued by Scottish Ministers in 2003.

Since the original Code and guidance was issued, the importance of good records management has been brought into sharp focus by the 2007 Historical Abuse Systemic Review of Residential Schools and Children’s Homes in Scotland by Tom Shaw (‘the Shaw Report’). The recommendations of the Shaw Report, and the subsequent 2009 review by the Keeper of Scottish public records legislation, identified problems and highlighted inconsistent and sometimes inadequate management of records across public authorities. These led to the passage of the Public Records (Scotland) Act 2011 (‘the 2011 Act’) in March 2011. While separate and distinct from Freedom of Information legislation, the 2011 Act – which is due to come into force in 2013 – complements FOISA and reflects the need for the provision of good records management by public authorities.

The 2011 Act makes provision about the management of public records by named public authorities. Provisions include the preparation of a records management plan (‘RMP’) setting out proper arrangements for the management of the authority’s public records; submitting the RMP for agreement with the Keeper; and ensuring that the authority’s public records are managed in accordance with the agreed RMP. Though the list of authorities in the schedule of the 2011 Act differs from that of FOISA, reflecting fewer named organisations, the 2011 Act remains complementary to the Code.

In the years since FOISA came into force it has become clear that good records management is essential for the effective and efficient answering of FOI requests. Indeed, the cost of answering a request under FOI in terms of time and resources will often be determined by the quality of information management within an authority. It is ultimately in the interest of an authority to maintain a strong records management practice, as being able to identify and locate stored information allows responses to be answered quickly and with ease. In this regard, the 2011 Act will support better record keeping and improve the quality of information that public authorities can provide.

Further guidance on best practice for public authorities is set out in the Code of Practice on the discharge of functions by Scottish public authorities, issued by the Scottish Ministers under sections 60 and 62 of FOISA.

Introduction

1. Purpose of the Code

The aims of this Code of Practice are:

- To set out practices which relevant authorities should follow in relation to the creation, keeping, management and final disposal of their records; and
- To describe the particular arrangements which apply to authorities which transfer their records to the National Records of Scotland or other public archives.

Part 1 of the Code provides a framework for relevant authorities to manage their records. It sets out recommended good practice for the organisational arrangements, decisions and processes required for effective records and information management.

Part 2 provides a framework for the review and transfer of records that have been selected for permanent preservation in the National Records of Scotland (NRS) or other public archives. It sets out the process by which records due for transfer are assessed to determine whether the information they contain can be designated as open information or, if this is not possible, to identify the exemptions that apply and for how long.

The scope of the Code applies to all records irrespective of the technology used to create and store them or the type of information they contain. It includes, therefore, not only paper file series and digital records management systems but business and information systems (for example case management, finance and geographical information systems) and the contents of websites. The Code's focus is on records and the systems that contain them, but the principles and recommended practice can be applied also to other information held by an authority.

For the purposes of this Code, the term 'records' is defined by the relevant British Standard[1], namely 'information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.' Some specific terms which are not defined in FOISA have been included in the Glossary at Annex A. Other words and expressions used in this Code have the same meaning as the same words and expressions used in FOISA.

This Code is a supplement to the provisions in FOISA and its adoption will help authorities comply with their duties under FOISA. It is not a substitute for legislation nor do its provisions have the force of law. However, part of the role of the Commissioner is to promote observance of the Code (see 'role of the Scottish Information Commissioner' below). Consequently, all relevant authorities are expected to have regard to the guidance in this Code.

Authorities should note that if they fail to comply with the Code, they may also fail to comply with other legislation relating to information and records, [such as the Public Records (Scotland) Act 2011, the Data Protection Act 1998, the Environmental Information Regulations (Scotland) 2004, the INSPIRE (Scotland) Regulations 2009 and the Re-use of Public Sector Information Regulations 2005, and they may consequently be in breach of their statutory obligations].

[1] ISO 15489-1:2001 Records Management

For example, under the 2011 Act, the Keeper must prepare and publish a model RMP and issue guidance to authorities about the form and content of RMPs[2]. The Keeper's statutory guidance will refer to the Code and those authorities who therefore comply with it will make significant steps towards fulfilling their separate obligations under the 2011 Act.

2. Importance of records management

Freedom of information legislation is only as good as the quality of the records and other information to which it provides access. Access rights are of limited value if information cannot be found when requested or, when found, cannot be relied upon as authoritative. Good records and information management benefits those requesting information because it provides some assurance that the information provided will be complete and reliable. It benefits those holding the requested information because it enables them to locate and retrieve it easily within the statutory timescales or to explain why it is not held. It also supports control and delivery of information promised in an authority's Publication Scheme or required to be published by the EIRs.

Records management is important for many other reasons. Records and information are the lifeblood of any organisation. They are the basis on which decisions are made, services provided, and policies developed and communicated. Effective management of records and other information brings the following additional benefits:

- It supports an authority's business and discharge of its functions, and supports good governance;
- It promotes business efficiency and underpins service delivery by ensuring that authoritative information about past or current activities can be retrieved, used and relied upon in current business;
- It supports compliance with other legislation which requires records and/or information to be kept, controlled and accessible;
- It improves accountability, enabling compliance with legislation and other rules and requirements to be demonstrated to those with a right to audit or otherwise investigate the organisation and its actions;
- It protects the rights and interests of an authority, its staff and its stakeholders;
- It protects the rights and interests of individuals who seek access to information;
- It increases efficiency and cost-effectiveness by ensuring that records are disposed of when they are no longer needed. This enables more effective use of resources, for example space within buildings and information systems, and saves staff time searching for information that may not be there;
- It provides institutional memory.

Poor records and information management create risks for the authority, such as:

- Poor decisions based on inaccurate or incomplete information;
- Inconsistent or poor levels of services;
- Financial or legal loss if information required as evidence is not available or cannot be relied upon;

[2] The Public Records (Scotland) Act 2011, SS.1 & 8

- Non-compliance with statutory or other regulatory requirements, or with standards that apply to the sector to which it belongs;
- Failure to handle confidential information with an appropriate level of security and the possibility of unauthorised access or disposal taking place;
- Failure to protect information that is vital to the continued functioning of the organisation, leading to inadequate business continuity planning;
- Unnecessary costs caused by storing records and other information for longer than they are needed;
- Staff time wasted searching for records;
- Staff time wasted considering issues that have previously been addressed and resolved;
- Loss of reputation as a result of all of the above, with damaging effects on public trust;
- Failure to protect the rights of vulnerable people who are dependent on the direct support provided by an authority;
- Failure to protect the rights of those seeking access to information.

3. Role of the Scottish Information Commissioner

The Scottish Information Commissioner has duties and powers to promote the following of good practice by public authorities. This includes promoting observance of the Code[3]. While the Code's guidance is not statutory, Scottish public authorities are expected to adhere to the Code unless there are good reasons not to do so, which can be justified to the Commissioner. If the Commissioner considers that an authority is failing to take account of the guidance in this Code, he may issue a **practice recommendation** specifying the steps that the authority should, in his opinion, take to conform with it[4].

Before issuing a practice recommendation in relation to conforming with the Code, the Commissioner must consult with the Keeper. The recommendation will set out in writing the particular provisions of the Code with which the authority is failing to comply. A practice recommendation is simply that - a recommendation - designed to help the authority improve its compliance with the legislation. It cannot be directly enforced by the Commissioner. However, a failure to comply with a practice recommendation may lead to a failure to comply with the legislation which can result in an **enforcement notice** being issued by the Commissioner.[5] A failure may also be the subject of specific comment in a report by the Commissioner to Parliament.

If the Commissioner reasonably requires any information to determine whether an authority is complying with the Code (or with the provisions of the regimes) he may issue an **information notice**. This requires an authority to provide the necessary information to him within a stipulated time[6]. The notice will explain why the Commissioner requires the information and give details of the authority's right to appeal to the Court of Session against the decision that resulted in the issue of an information notice.

The Commissioner may also refer to non-compliance with the Code in a **decision notice** issued as a result of a request being appealed to him[7]. If a public authority fails to comply with an information notice, an enforcement notice, or a decision

[3] Under section 43 of FOISA and regulation 18 of EIRs.
[4] Under section 44 of FOISA and regulation 17 of EIRs.
[5] See section 51 of FOISA and regulation 17 of the EIRs.
[6] Under section 50 of FOISA and regulation 17 of the EIRs.
[7] Under section 47 of FOISA and regulation 17 of the EIRs

notice, the Commissioner may certify in writing to the Court of Session that the public authority has failed to comply with the notice.[8] The Court may then inquire into the matter and may deal with the authority as if it were in contempt of court.

4. <u>Role of the Keeper and Reviews under the Public Records (Scotland) Act 2011</u>

Records are crucial to organisations, particularly in this information age. Reliable information depends on good record keeping. The 2011 Act places duties on named public authorities to produce, implement and review a RMP for their particular organisation. A RMP must set out proper arrangements for the management of records created or held by the authority. Where a contractor carries out functions on behalf of an authority the authority's RMP must also cover contractor's records relating to those functions..

An authority must keep its plan under review, and if the Keeper so requires, carry out a review of the plan by such date as the Keeper may determine ('the review date'). The Keeper must not determine a review date earlier than five years after the date on which the authority's RMP was last agreed. An authority may at any time revise its RMP and submit the revised plan to the Keeper for agreement.

The Keeper may carry out a review (a 'records management review') of whether an authority is complying with its RMP, and the authority must provide the Keeper with such assistance as may be required. Following a records management review, the Keeper may make recommendations to the authority and require it to carry out a review of its plan. The Keeper may carry out a records management review in relation to a particular authority, or a group of authorities.

Where the Keeper considers that an authority is failing to comply with its RMP, or any duty imposed on it, the Keeper may issue a notice (an 'action notice') specifying the details of the alleged failure and requiring the authority to take specified action. Where the Keeper is considering issuing an action notice, he must notify the authority; give the authority the opportunity to make representation; and have regard to those representations. If the authority fails to comply with any of the requirements of the action notice, the Keeper may publicise the failure.

<u>5. Authorities subject to Public Records legislation (or legislation with record keeping provisions)</u>

The guidance on records management and on the transfer of records to public archives contained in the Code should be read in the context of the prevailing legal framework within which authorities operate. There is a range of legislation on record keeping which may apply to some of the authorities covered by FOISA. Key legislation includes the Public Records (Scotland) Act 1937 (as amended) and the 2011 Act, the Public Registers and Records (Scotland) Act 1948, the Local Government (Access to Information) Act 1985 and the Local Government etc (Scotland) Act 1994 ('the 1994 Act'). The 1994 Act complements the objectives of this Code by requiring local authorities to:

- Make proper arrangements for the preservation and management of their records;
- Consult the Keeper before putting any such arrangements into effect or making any material change to such arrangements; and

[8] See section 53 of FOISA.

- Have regard to any comments which the Keeper may make on their proposed arrangements or changes to such arrangements.

The 1994 Act also permits local authorities to make provision for persons to inspect or obtain copies of their records and for a local authority to carry out an activity with, or on behalf of, another local authority. It is therefore open to local authorities to enter into a mutually beneficial agreement concerning the storage, management or access arrangements for their records.

6. Further guidance

This Code provides high level strategic guidance for authorities. More detailed operational guidance, in the form of a generic Model Action Plan (‘MAP’) is available from the NRS to assist authorities in complying with the Code and FOISA. The generic MAP should be read in conjunction with the Code, but it has not been revised since implementation of FOISA in 2005. It can be used by individual organisations as a guide, and can also be used as the basis for the development of sector-specific codes tailored to the needs and business practices of particular types of public authority.

The NRS also provide a records management workbook to enable authorities to check their records management procedures against the Code.

In addition, under the 2011 Act the Keeper must issue guidance to authorities about the form and content of records management plans, and may issue different guidance in relation to different authorities. Before issuing guidance, the Keeper must consult such authorities as the Keeper considers will be affected by the guidance, and such other persons (if any) as the Keeper considers appropriate, and have regard to any views expressed in response to the consultation. Authorities must have regard to this guidance when preparing their RMP. The Keeper may also issue guidance to authorities about their duties under the 2011 Act which they must also have regard to.

Annex B of the Code contains links to further guidance concerning information and records management.

PART 1: RECORDS MANAGEMENT

Summary of recommended good practice in records management.

Good practice in records management is made up of nine key elements. When considering these, authorities should have regard to the statutory guidance issued by the Keeper under the 2011 Act. This part of the Code describes each records management element in detail.

1. Authorities should have in place organisational arrangements that support records management (see pages 10-11)
2. Authorities should have in place a records management policy, either as a separate policy or as part of a wider information or knowledge management policy (see page 12)
3. Authorities should ensure they keep the records they will need for business, regulatory, legal and accountability purposes (see pages 13-14)
4. Authorities should keep their records in systems that enable records to be stored and retrieved as necessary (see pages 15-16)
5. Authorities should know what records they hold and where they are, and should ensure that they remain usable for as long as they are required (see pages 17-18)
6. Authorities should ensure that records are stored securely and that access to them is controlled (see page 19)
7. Authorities should define how long they need to keep particular records, should dispose of them when they are no longer needed and should be able to explain why records are no longer held (see pages 20-22)
8. Authorities should ensure that records shared with other bodies or held on their behalf by other bodies are managed in accordance with the Code (see page 23)
9. Authorities should monitor compliance with the Code and assess the overall effectiveness of the programme (see page 24)

1. Organisational arrangements to support records management

Authorities should have in place organisational arrangements that support records management.

These arrangements should include:

1.1 Recognition of ***records management as a core corporate function***, either separately or as part of a wider information or knowledge management function. The function should cover records in all formats throughout their lifecycle, from planning and creation through to disposal and should include records managed on behalf of the authority by an external body such as a contractor;

1.2 Recognition of records and information management in the ***corporate risk management framework***. Information and records are a corporate asset and loss of the asset could cause disruption to business. The level of risk will vary according to the strategic and operational value of the asset to the authority and risk management should reflect the probable extent of disruption and resulting damage;

1.3 A governance framework that includes ***defined roles and lines of responsibility.*** This should include allocation of lead responsibility for the records and information management function to a designated member of staff at sufficiently senior level to act as a records management champion, and allocation of operational responsibility to a member of staff with the necessary knowledge and skills. In small authorities it may be more practical to combine these roles. Ideally the same people will be responsible also for compliance with other information legislation, for example the Data Protection Act 1998, the Public Records (Scotland) Act 2011 and the Re-use of Public Sector Information Regulations 2005, or will work closely with those people;

1.4 ***Clearly defined instructions***, applying to staff at all levels of the authority, to create, keep and manage records. In larger organisations the responsibilities of managers, and in particular heads of business units, could be differentiated from the responsibilities of other staff by making it clear that managers are responsible for ensuring that adequate records are kept of the activities for which they are accountable;

1.5 ***Identification of information and business systems*** that hold records and provision of the resources needed to maintain and protect the integrity of those systems and the information they contain;

1.6 Consideration of records management issues when ***planning or implementing ICT systems***, when extending staff access to new technologies and during re-structuring or major changes to the authority;

1.7 ***Induction and other training*** to ensure that all staff are aware of the authority's records management policies, standards, procedures and guidelines and understand their personal responsibilities. This should be extended to temporary staff, contractors and consultants who are undertaking work is to be documented in the authority's records. If the organisation is large enough to employ staff whose work is primarily about records and information management, they should be given opportunities for professional development;

1.8 An ***agreed programme*** for managing records in accordance with this part of the Code;

1.9 ***Provision of the financial and other resources*** required to achieve agreed objectives in the records management programme.

2. Records management policy

Authorities should have in place a records management policy, either as a separate policy or as part of a wider information or knowledge management policy.

2.1 The policy should be endorsed by senior management, for example at board level, and should be readily available to staff at all levels. The policy should identify a person at senior level who has overall strategic responsibility for records management.

2.2 The policy provides a mandate for the records and information management function and a framework for supporting standards, procedures and guidelines. The precise contents will depend on the particular needs and culture of the authority but it should as a minimum:

a) Set out the authority's commitment to create, keep and manage records which document its principal activities;

b) Outline the role of records management and its relationship to the authority's overall business strategy;

c) Identify and make appropriate connections to related policies, such as those dealing with email, information security and data protection;

d) Define roles and responsibilities, including the responsibility of individuals to document their work in the authority's records to the extent that, and in the way that, the authority has decided their work should be documented, and to use those records appropriately;

e) Indicate how compliance with the policy and the supporting standards, procedures and guidelines will be monitored.

2.3 The policy should be kept up to date so that it reflects the current needs of the authority. One way of ensuring this is to review it at agreed intervals, for example every three or five years, and after major organisational or technological changes, in order to assess whether it needs amendment. Authorities should remain aware of their responsibilities to review RMPs under s.5 of the 2011 Act.

2.4 The authority should consider publishing the policy so that members of the public can see the basis on which it manages its records.

3. Keeping records to meet corporate requirements

Authorities should ensure they keep the records they will need for business, regulatory, legal and accountability purposes.

Deciding what records should be kept

3.1 Authorities should consider what records they are likely to need to document their activities, and the risks of not having those records, taking into account the following factors:

a) The legislative and regulatory environment within which they operate. This will be a mixture of generally applicable legislation, such as health and safety legislation and the Data Protection Act 1998, and specific legislation applying to the sector or authority. For example, the Office of the Scottish Charity Regulator is required by its legislation to keep an accurate and up to date register of charities;

b) The need to refer to authoritative information about past actions and decisions for current business purposes. For example, problems such as outbreaks of foot and mouth disease may recur and in order to deal with each new outbreak a local authority needs reliable information about what it did during previous outbreaks and who was responsible for specific measures, such as closing public footpaths;

c) The need to protect legal and other rights of the authority, its staff and its stakeholders. For example, a local authority needs to know what land and buildings it owns in order to ensure proper control of its assets and to protect itself if challenged;

d) The need to explain, and if necessary justify, past actions in the event of an audit, public inquiry or other investigation. For example, Audit Scotland will expect to find accurate records of expenditure of public funds. Or, if an applicant complains to the Commissioner about the handling of or outcome of an FOI request, the Commissioner will expect the authority to provide details of how the request was handled and, if applicable, why it refused to provide the information.

3.2 Having considered these factors, authorities should set business rules identifying:

a) What records should be kept, for example which decisions or actions should be recorded;

b) By whom this should be done, for example by the sender or recipient of an email or voicemail;

c) At what point in the process or transaction this should be done, for example when drafts of a document should be frozen and kept as a record;

d) What those records should contain; and

e) Where and how they should be stored, for example in a case file.

3.3 As part of this process authorities should consider whether any of these records should be subject to particular controls so as to ensure their evidential value can be upheld by demonstrating them to:

a) Be authentic - they are what they say they are;

b) Be reliable - they can be trusted as a full and accurate record;

c) Have integrity - they have not been altered since they were created or filed;

d) Be usable - they can be retrieved, read and used.

Ensuring those records are kept

3.4 All staff should be aware of which records the authority has decided to keep and of their personal responsibility to follow the authority's business rules and keep accurate and complete records as part of their daily work. Managers of business units, programmes and projects should take responsibility for ensuring that the agreed records of the unit, programme or project's work are kept and are available for corporate use.

3.5 Authorities should ensure that staff creating or filing records are aware of the need to give those records titles that reflect their specific nature and contents so as to facilitate retrieval.

3.6 Staff should also be aware of the need to dispose of ephemeral material on a routine basis. For example, print-outs of electronic documents should not be kept after the meeting for which they were printed, trivial emails should be deleted after being read, and keeping multiple or personal copies of documents should be discouraged.

4. Records systems

Authorities should keep their records in systems that enable records to be stored and retrieved as necessary.

Choosing, implementing and using records systems

4.1 Authorities should decide the format in which their records are to be stored. There is no requirement in this Code for records and information to be created and held electronically, but if the authority is operating electronically, for example using email for internal and external communications or creating documents through word processing software, it is good practice to hold the resulting records electronically. In addition, authorities should note that the EIRs require them progressively to make environmental information available to the public by electronic means[9].

4.2 Authorities are likely to hold records and other information in a number of different systems. These systems could include a dedicated electronic document and records management system, business systems such as a case management, finance or geographical information system, a website, online storage, shared workspaces, audio-visual material and sets of paper files with related registers. In some cases related records of the same business activities may be held in different formats, for example digital files and supporting paper material.

4.3 Records systems should be designed to meet the authority's operational needs and using them should be an integral part of business operations and processes. Records systems should have the following characteristics:

a) They should be easy to understand and use so as to reduce the effort required of those who create and use the records within them. Ease of use is an important consideration when developing or selecting a system;

b) They should enable quick and easy retrieval of information. With digital systems this should include the capacity to search for information requested under FOISA;

c) They should be set up in a way that enables routine records management processes to take place. For example, digital systems should be able to delete specified information in accordance with agreed disposal dates and leave the rest intact;

d) They should enable the context of each record and its relationship to other records to be understood. In a records management system this can be achieved by classifying and indexing records within a file plan or business classification scheme to bring together related records and enable the sequence of actions and context of each document to be understood. This approach has the added benefit of enabling handling decisions, for example relating to access or disposal, to be applied to groups of records instead of to individual records;

[9] Regulation 4(1) of the EIRs.

e) They should contain both information and metadata. Metadata enables the system to be understood and operated efficiently, the records within the system to be managed and the information within the records to be interpreted;

f) They should protect records in digital systems from accidental or unauthorised alteration, copying, movement or deletion;

g) They should provide secure storage to the level of protection required by the nature, contents and value of the information in them. For digital systems this includes a capacity to control access to particular information if necessary, for example by limiting access to named individuals or by requiring passwords. With paper files this includes a capacity to lock storage cupboards or areas and to log access to them and any withdrawal of records from them;

h) They should enable an audit trail to be produced of occasions on which selected records have been seen, used, amended and deleted.

4.3 Records systems should be documented to facilitate staff training, maintenance of the system and its reconstruction in the event of an emergency.

Limiting the active life of records within record systems

4.4 Folders, files and similar record assemblies should not remain live indefinitely with a capacity for new records to be added to them. They should be closed, that is, have their contents frozen, at an appropriate time.

4.5 The trigger for closure will vary according to the nature and function of the records, the extent to which they reflect ongoing business and the technology used to store them. For example, completion of the annual accounting process could be a trigger for closing financial records, completion of a project could be a trigger for closing project records, and completion of formalities following the death of a patient could be a trigger for closing that person's health record. Size is a factor and a folder should not be too big to be handled or scrutinised easily. For digital records a trigger could be migration to a new system. Authorities should decide the appropriate trigger for each records system and put arrangements in place to apply the trigger.

4.6 New continuation or part files should be opened if necessary. It should be clear to anyone looking at a record where the story continues, if applicable.

5. Storage and maintenance of records

Authorities should know what records they hold and where they are, and should ensure that they remain usable for as long as they are required.

Knowing what records are held

5.1 The effectiveness of records systems depends on knowledge of what records are held, what information they contain, in what form they are made accessible, what value they have to the organisation and how they relate to organisational functions. Without this knowledge an authority will find it difficult to:

a) Locate and retrieve information required for business purposes or to respond to an information request;

b) Produce a Publication Scheme[10] or a reliable list of information assets available for re-use;

c) Apply the controls required to manage risks associated with the records;

d) Ensure records are disposed of when no longer needed.

5.2 Authorities should gather and maintain data on records and information assets. This can be done in various ways, for example through surveys or audits of the records and information held by the authority. It should be held in an accessible format and should be kept up to date.

5.3 Authorities should consider publishing details of the types of records they hold to help members of the public planning to make a request for information under FOISA.

Storing records

5.4 Storage should provide protection to the level required by the nature, contents and value of the information in them. Records and information will vary in their strategic and operational value to the authority, and in their residual value for historical research, and storage and preservation arrangements reflecting their value should be put in place.

5.5 Authorities should be aware of any specific requirements for records storage that apply to them. For example, BS 5454:2000 makes recommendations for the storage and exhibition of archival documents, mainly those on paper and parchment.

5.6 Storage should follow accepted standards in respect of the storage environment, fire precautions, health and safety and, if applicable, physical organisation. It should allow easy and efficient retrieval of information but also minimise the risk of damage, loss or unauthorised access.

5.7 Records that are no longer required for frequent reference can be removed from current systems to off-line or near off-line (for digital media) or to off-site (for

[10] As required under s.23 of FOISA.

paper) storage where this is a more economical and efficient way to store them. They should continue to be subject to normal records management controls and procedures. The accessibility of these records should not be compromised.

5.8 The whereabouts of records should be known at all times and movement of files and other physical records between storage areas and office areas should be logged.

Ensuring records remain usable

5.9 Records should remain usable for as long as they are required. This means that it should continue to be possible to retrieve, use and rely on them.

5.10 Records in digital systems will not remain usable unless actions are taken. Authorities should put in place a strategy for their continued maintenance designed to ensure that information remains intact, reliable and usable for as long as it is required. The strategy should provide at a minimum for updating of the storage media and migration of the software format within which the information and metadata are held, and for regular monitoring of integrity and usability.

5.11 Records in digital systems are particularly vulnerable to accidental or unauthorised alteration, copying, movement or deletion which can happen without trace. This puts at risk the reliability of the records which could damage the authority's interests. Authorities should assess these risks and put appropriate safeguards in place.

5.12 Back-up copies of records in digital systems should be kept and stored securely in a separate location. They should be checked regularly to ensure that the storage medium has not degraded and the information remains intact and capable of being restored to operational use. Back-ups should be managed in a way that enables disposal decisions to be applied securely without compromising the authority's capacity to recover from system failures and major disasters.

5.13 Physical records such as paper files may also require regular monitoring. For example, formats such as early photocopies may be at risk of fading, and regular checks should be made of any information in such formats that is of continuing value to the authority.

5.14 Metadata for records in any format should be kept in such a way that it remains reliable and accessible for as long as it is required, which will be at least for the life of the records.

Business continuity plans

5.15 Business continuity plans should identify and safeguard records considered vital to the organisation, that is:

a) Records that would be essential to the continued functioning or reconstitution of the organisation in the event of a disaster;

b) Records that are essential to ongoing protection of the organisation's legal and financial rights.

The plans should include actions to protect and recover these records in particular.

6. Security and access

Authorities should ensure that records are stored securely and that access to them is controlled.

6.1 Authorities should ensure that their storage arrangements, handling procedures and arrangements for transmission of records reflect accepted standards and good practice in information security. It is good practice to have an information security policy addressing these points.

6.2 Ease of internal access will depend on the nature and sensitivity of the records. Access restrictions should be applied when necessary to protect the information concerned and should be kept up to date. Particular care should be taken with personal information about living individuals in order to comply with the 7th data protection principle, which requires precautions against unauthorised or unlawful processing, damage, loss or destruction. Within central Government, particular care should be taken with information bearing a protective marking. Other information, such as information obtained on a confidential basis, may also require particular protection.

6.3 Transmission of records, especially outside the authority's premises, should require authorisation. The method of transmission should be subject to risk assessment before a decision is made.

6.4 External access should be provided in accordance with relevant legislation.

6.5 An audit trail should be kept of provision of access, especially to people outside the immediate work area.

7. Disposal of records

Authorities should define how long they need to keep particular records, should dispose of them when they are no longer needed and should be able to explain why records are no longer held.

7.1 For the purpose of this Code, disposal means the decision as to whether the record should be destroyed or transferred to an archives service for permanent preservation, and the putting into effect of that decision.

General principle

7.2 As a general principle, records should be kept for as long as they are needed by the authority: for reference or accountability purposes, to comply with regulatory requirements or to protect legal and other rights and interests. Destruction at the end of this period ensures that office and server space are not used and costs are not incurred in maintaining records that are no longer required. For records containing personal information it also ensures compliance with the fifth data protection principle[11].

7.3 Records should not be kept after they have ceased to be of use to the authority unless:

a) They are known to be the subject of litigation or a request for information. If so, destruction should be delayed until the litigation is complete or, in the case of a request for information, all relevant complaint and appeal provisions have been exhausted;

b) They have long-term value for historical or other research and have been or should be selected for permanent preservation. (Note that records containing personal information can be kept indefinitely for historical research purposes because they thereby become exempt from the 5th data protection principle.)

c) They contain or relate to information recently released in response to a request under FOISA. This may indicate historical value and destruction should be delayed while this is re-assessed.

Making disposal decisions

7.4 Disposal of records should be undertaken only in accordance with clearly established policies that:

a) Reflect the authority’s continuing need for access to the information or the potential value of the records for historical or other research;

b) Are based on consultation between records management staff, staff of the relevant business unit and, where appropriate, others such as legal advisers, archivists or external experts;

[11] “Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.” Schedule 1 of the Data Protection Act 1998.

c) Have been formally adopted by the authority;

d) Are applied by properly authorised staff;

e) Take account of security and confidentiality needs.

7.5 The policies should take the form of:

a) An overall policy, stating in broad terms the types of records likely to be selected for permanent preservation. The policy could be a separate policy, part of the records management policy or a preamble to a disposal schedule;

b) Disposal schedules which identify and describe records to which a pre-defined disposal action can be applied, for example destroy x years after [trigger event]; review after y years, transfer to archives for permanent preservation after z years.

7.6 Disposal schedules should contain sufficient details about the records to enable the records to be easily identified and the disposal action applied to them on a routine and timely basis. The amount of detail in disposal schedules will depend on the authority's needs but they should at least:

a) Describe the records, including any relevant reference numbers;

b) Identify the function to which the records relate and the business unit for that function (if that is not clear);

c) Specify the retention period, i.e. how long they are to be kept;

d) Specify what is to happen to them at the end of that period, i.e. the disposal action;

e) Note the legal, regulatory or other reason for the disposal period and action, for example a statutory provision.

7.7 Disposal schedules should be arranged in the way that best meets the authority's needs.

7.8 Disposal schedules should be kept up to date and should be amended if a relevant statutory provision changes. However, authorities should consider keeping information about previous provisions so that the basis on which records were previously destroyed can be explained.

7.9 If any records are not included in disposal schedules, special arrangements should be made to review them and decide whether they can be destroyed or should be selected for permanent preservation. Decisions of this nature should be documented and kept to provide evidence of which records have been identified for destruction, when the decision was made, and the reasons for the decision, where this is not apparent from the overall policy.

Implementing disposal decisions

7.10 Disposal schedules and disposal decisions should be implemented by properly authorised staff. Implementation arrangements should take account of variations caused by, for example, outstanding requests for information or litigation.

7.11 Records scheduled for destruction should be destroyed in as secure a manner as required by the level of confidentiality or security markings they bear. For example, records containing personal information about living individuals should be destroyed in a way that prevents unauthorised access (this is required to comply with the 7th data protection principle). With digital records it may be necessary to do more than overwrite the data to ensure the information is destroyed.

7.12 When destruction is carried out by an external contractor, the contract should stipulate that the security and access arrangements established for the records will continue to be applied until destruction has taken place.

7.13 In some cases there will be more than one copy of a record. For example, there are likely to be back-up copies of digital records, or there may be digital copies of paper records. A record cannot be considered to have been completely destroyed until all copies, including back-up copies, have been destroyed, if there is a possibility that the data could be recovered.

Documenting the destruction of records

7.14 Details of destruction of records should be kept, either as part of the audit trail metadata or separately. Ideally, some evidence of destruction should be kept indefinitely because the previous existence of records may be relevant information. However, the level of detail and for how long it should be kept will depend on an assessment of the costs and the risks to the authority if detailed information cannot be produced on request.

7.15 At the very least it should be possible to provide evidence that as part of routine records management processes destruction of a specified type of record of a specified age range took place in accordance with a specified provision of the disposal schedule. Evidence of this nature will enable an authority and its staff to explain why records specified in a court order cannot be provided or to defend themselves against a charge under section 65 of FOISA that records were destroyed in order to prevent their disclosure in response to a request for information.

Records for permanent preservation

7.16 Records selected for permanent preservation and no longer required by the authority should be transferred to an archives service that has adequate storage and public access facilities. Transfer should take place in an orderly manner and with a level of security appropriate to the confidentiality of the records.

Part 2 of the Code sets out the arrangements that apply to the review and transfer of records to public archives.

8. Records created in the course of collaborative working or through out-sourcing

Authorities should ensure that records shared with other bodies or held on their behalf by other bodies are managed in accordance with the Code.

8.1 When authorities are working in partnership with other organisations, sharing information and contributing to a joint records system, they should ensure that all parties agree protocols that specify:

a) What information should be contributed and kept, and by whom;

b) What level of information security should be applied;

c) Who should have access to the records;

d) What disposal arrangements should be in place;

e) Which body holds the information for the purposes of FOISA.

8.2 Instructions and training should be provided to staff involved in such collaborative working.

8.3 Records management controls should be applied to information being shared with or passed to other bodies. Particular protection should be given to confidential or personal information. Protocols should specify when, and under what conditions, information will be shared or passed, and details should be kept of when this information has been shared or passed. Details should be kept also of how undertakings given to the original source of the information have been respected.

8.4 Some of an authority’s records may be held on its behalf by another body, for example a body carrying out work for the authority under contract. The authority on whose behalf the records are held is responsible for ensuring that the provisions of the Code are applied to those records. Under the 2011 Act, an authority’s public records includes records created by or on behalf of a contractor in carrying out the authority’s functions where the records relate to those functions. The authority’s RMP must set out the arrangements for the management of those records created or held by the contractors who carry out those functions. The contract between the public authority and the contracted organisation will detail the records management responsibilities and the processes for proper care of the records created under the contract.

9. Monitoring and reporting on records and information management

Authorities should monitor compliance with the Code and assess the overall effectiveness of the programme.

9.1 Authorities should identify performance measures that reflect their information management needs and arrangements and the risks that non-compliance with the Code would present to the authority, including the impact on risks identified in the overall risk management framework.

9.2 The performance measures could be general in nature, for example that a policy has been issued, or could refer to processes, such as the application of disposal schedules to relevant records with due authorisation of destruction, or could use metrics such as retrieval times for paper records held off-site that have been requested under FOISA.

9.3 Authorities should put in place the means by which performance can be measured. For example, if metrics are to be used, the data from which statistics will be generated must be kept. Qualitative indicators, for example whether guidance is being followed, can be measured by spot checks or by interviews.

9.4 Monitoring should be undertaken on a regular basis and the results reported to the person with lead responsibility for records management so that risks can be assessed and appropriate action taken.

9.5 Assessing whether the records management programme meets the needs of the organisation is a more complex task and requires consideration of what the programme is intended to achieve and how successful it is in delivering its objectives. This requires consideration of business benefits in relation to corporate objectives as well as risks and should include consultation throughout the authority.

PART 2: REVIEW AND TRANSFER OF RECORDS TO PUBLIC ARCHIVES

1. Purpose of Part 2

1.1 This part of the Code applies to authorities which transfer records either:

- to the Keeper of the Records of Scotland at the National Records of Scotland (NRS) under the Public Records (Scotland) Act 1937 and 2011; and the Public Registers and Records (Scotland) Act 1948; or
- to a public archive other than NRS (such as a public archive service operated by the same authority or by another Scottish public authority).

1.2 The purpose of this part of the Code is to assist the transferring authority in exercising their functions under FOISA. It sets out the arrangements which authorities should follow to ensure the timely and effective review and transfer of public records. In reviewing records for public access, authorities should ensure that records become available at the earliest possible time in accordance with FOISA and the EIRs.

1.3 For the purposes of this part, 'public archive' means an archive service which holds records of, or on behalf of, a Scottish public authority[12], regardless of whether the service is operated by a Scottish public authority or by another person such as a private company.

1.4 Many Scottish public authorities operate their own public archive service, and so the transferring authority and the public archive are part of the same authority. In such circumstances, unless the context requires otherwise, the references in this Part to 'transferring authority' should be read as meaning the part of the authority from which the records originated or which has responsibility for the subject matter of the records.

2. Selection of public records for permanent preservation

2.1 Section 7 of Part 1 of this Code describes the arrangements that authorities should follow for the disposal of records. In this context, disposal means the decision as to whether the record should be destroyed or transferred to an archive service for permanent preservation and the putting into effect of that decision.

2.2 Authorities that have created or are otherwise responsible for public records should ensure that they operate effective arrangements to determine which records should be selected for permanent preservation in accordance with the guidance in section 7.

2.3 Authorities which transfer records to NRS (although these points are equally applicable to other archives) should observe the following:

- Review and transfer to NRS should normally take place before records reach 30 years old and become 'historical records'[13].

[12] s.3(1) of FOISA
[13] s.57 of FOISA

- The long term preservation of electronic records presents particular problems and effective action should be taken as early as possible. As a result transfer of electronic records should take place well before the records are 30 years old. Ideally decisions on transfer timings should be agreed with NRS when the records are created. The review of electronic records should therefore occur before the records reach the age at which it is agreed they should be transferred, preferably also at the point of creation.

3. Determining the access status of records before transfer

3.1 Authorities which transfer records to NRS or a public archive should establish arrangements for regularly reviewing their records to ensure that they become available to the public at the earliest possible time. When preparing records for transfer, authorities should review the access status of those records. The purpose of this review is to:

a) Consider which information must be available to the public (ie made 'open') on transfer because no exemptions under FOISA or the EIRs apply;

b) Consider which information should be withheld from public access through the application of an exemption under FOISA or an exception under the EIRs;

c) Consider whether the information must be released in the public interest, notwithstanding the application of an exemption under FOISA or an exception under the EIRS.

3.2 Those undertaking the review should ensure that adequate consultation takes place, both within the authority and with other authorities that might be affected by the decision, for example authorities that originally supplied the information. (It is for the transferring authority however to conclude whether, for example, exemptions may apply to the information.)

4. Records to be transferred as 'open'

4.1 If the outcome of the review is that records are to be transferred as open, the transferring authority should designate the records as open.

5. Records to be transferred as subject to an exemption

5.1 If the outcome of the review is identification of specified information which the authority considers ought not to be released under the terms of FOISA or the EIRs, the authority should prepare a schedule that:

a) Identifies the information precisely;

b) Cites the relevant exemption(s) or exception(s);

c) Explains why the information may not be released;

d) Identifies a date at which either release would be appropriate or the case for release should be reconsidered.

5.2 Authorities should consider whether parts of records might be released if the sensitive information were redacted, i.e. rendered invisible or blanked out. Any method of redaction should not, however, damage the document and must be fully reversible. Information that has been redacted should be stored securely and should be returned to the parent records when the exemption has ceased to apply.

5.3 The archive will use the schedules received to identify those records which might be exempt. If circumstances change the content of a schedule, the transferring authority should submit a revised schedule to the archive, highlighting the adjustments. They should also update their publication scheme as appropriate if additional information is to be made accessible to the public.

6. Transmission of records to archives

6.1 It is the responsibility of authorities transferring records to ensure that those records are prepared in a manner agreed with NRS or the receiving public archive and are transferred with the level of security appropriate to the confidentiality of the information they contain.

7. Access after transfer of records – Freedom of Information requests

7.1 For the avoidance of doubt, none of the actions described in this Code affects the statutory rights of access established under FOISA or the EIRs. Requests for exempt information in records transferred to archives will be dealt with on a case by case basis in accordance with the provisions of FOISA or the EIRs.

7.2 Public archives which receive records from authorities are, under FOISA and EIRs, holding those records ‘on behalf of’ the authority. The transferring authority is therefore responsible for considering access requests made for information contained in them. Where information is already ‘open’ however and is made available in accordance with the authority’s publication scheme[14], it may be regarded as being reasonably obtainable under section 25 of FOISA and so is exempt from the access requirements of FOISA.

7.3 When an archive receives a request for access to information which the transferring authority has identified as being exempt:

- if the archive and transferring authority are part of the same Scottish public authority, the archive should forward the request as soon as possible to the transferring authority for their consideration. The time within which the authority must comply with the request will start from the day on which it was received by the public archive, not the authority.

- if the archive and transferring authority are not part of the same Scottish public authority the archive should redirect the applicant to apply direct to the transferring authority.

7.4 When an exemption has ceased to apply under section 58 of FOISA the information in question will become automatically available to the public.

[14] As required by section 23 of the Act

Annex A: Glossary

Disposal – the decision as to whether the record should be destroyed, transferred to an archive service for permanent preservation, or presented and the putting into effect of that decision.

Disposal schedules – schedules that identify types of records and specify how long they will be kept before they are destroyed, designated for permanent preservation or subject to further review.

Keeping records – in the context of this Code, keeping records includes recording the authority's activities by creating documents and other types of records as well as handling material received.

Metadata – information about the context within which records were created, their structure and how they have been managed over time. Metadata can refer to records within digital systems, for example event log data. It can also refer to systems such as paper files that are controlled either from a digital system or by a register or card index, for example the title and location.

Public records – records that are subject to the Public Records (Scotland) Act 1937 and 2011 and the Public Registers and Records (Scotland) Act 1948.

Records – information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.

Records system – the term used for an information or process system that contains records and other information. It can be either a paper-based system or a digital system. Examples are correspondence file series, digital records management systems, case management systems, function-specific systems such as finance systems, etc.

Annex B: Standards and guidance supporting the Code

Note: external weblinks are provided for reference purposes only and are correct at time of printing.

PART 1: RECORDS MANAGEMENT

1. British Standards (BSI)

Relevant Standards issued by the British Standards Institution include:

BS ISO 15489-1:2001 - *Information and documentation. Records management*
BS ISO/IEC 27001:2005, *Information technology. Security techniques. Information security management systems. Requirements*
BS ISO/IEC 27002:2005, *Information technology. Security techniques. Information security management systems. Code of practice for information security management*
BS 4783-8:1994 - *Storage, transportation and maintenance of media for use in data processing and information storage*
BS 5454:2000 - *Recommendations for the storage and exhibition of archival documents*
BS 10008:2008 - *Evidential weight and legal admissibility of electronic information.*
BS EN 15713:2009 – *Secure destruction of confidential material. Code of practice.*

2. Standards and guidance produced by The National Archives for the management of public sector records

The Chief Executive of The National Archives, as head of profession for the knowledge and information function across Government, sets standards for the management of records in all formats, covering their entire life cycle. The standards are supported by guidance and toolkits. Advice for government departments can also be applied by other parts of the public sector. They are available on The National Archives website at:
http://www.nationalarchives.gov.uk/information-management/projects-and-work/information-records-management.htm

3. Sector-specific guidance

Guidance is available for specific sectors as follows:

(a) Central government
Cabinet Office has produced resources and information on the procedures and reviews of data handling within UK Government including the final report on data handling procedures across government – these are available at:
http://www.cabinetoffice.gov.uk/resource-library/data-handling-procedures-government

(b) Local government
The Information and Records Management Society has issued guidelines on disposal and information audits for local government at:
http://www.irms.org.uk/resources

The Local Government Association and Welsh Local Government Association have issued data handling guidance for protected records – see http://www.idea.gov.uk/idk/aio/9048091

(c) Further and higher education
JISC (Joint Information Systems Committee) Infonet has produced an information management Infokit at:
http://www.jiscinfonet.ac.uk/information-management

(d) Schools
The Information and Records Management Society has issued a records management toolkit for schools – see http://www.irms.org.uk/resources/848

(e) The police
A code of practice on the use of the new Police National Database is available from the National Policing Improvement Agency at:
http://www.npia.police.uk/en/15483.htm

The Association of Chief Police Officers (ACPO) has produced guidance on the management of police information at:
http://www.acpo.police.uk/ProfessionalPractice/InformationManagement.aspx

The Association of Chief Police Officers in Scotland (ACPOS) has guidance on information management at:
http://www.acpos.police.uk/Policies.html#information%20management

(f) The National Health Service
A Code of Practice on Records Management for NHS Scotland is available at:
http://www.scotland.gov.uk/Publications/2010/04/20142935/0

PART 2: REVIEW AND TRANSFER OF RECORDS TO PUBLIC ARCHIVES

1. Transfer of records to public archives

UK references:
The National Archives has published guidance on determining whether records should be transferred to The National Archives or a place of deposit for public records – see the *Acquisition and Disposition Strategy* and supporting guidance at http://www.nationalarchives.gov.uk/information-management/projects-and-work/acquisition-disposition-strategy.htm and http://www.nationalarchives.gov.uk/information-management/projects-and-work/disposition-guidance.htm

For guidance on the preparation of records for transfer to the National Archives, including cataloguing, see http://www.nationalarchives.gov.uk/recordsmanagement/advice/standards.htm and http://www.nationalarchives.gov.uk/recordsmanagement/advice/cataloguing.htm
For guidance on the transfer of records to places of deposit see http://www.nationalarchives.gov.uk/documents/information-management/foi_guide.pdf

2. Determining whether exemptions apply
Guidance on FOI exemptions has been issued by the Scottish Information Commissioner's Office, the regulator of both FOISA and the EIRs, at:

http://www.itspublicknowledge.info/Law/FOISA-EIRsGuidance/Briefings.asp#exemptions

Guidance has also been issued by The National Archives on how the UK Freedom of Information Act has affected the management of public records and how to handle access requests at http://www.nationalarchives.gov.uk/information-management/projects-and-work/foi.htm