



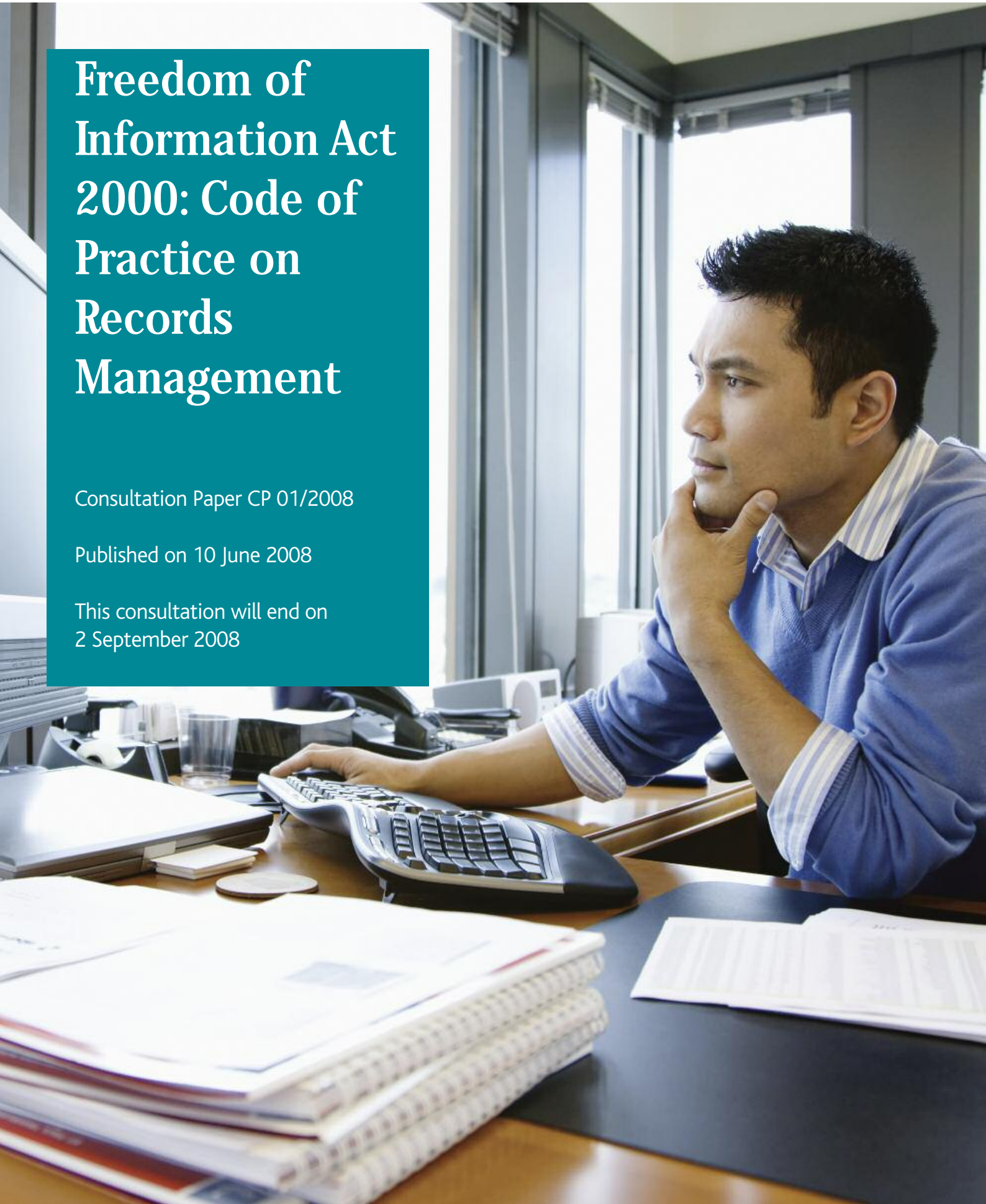
The National Archives

Freedom of Information Act 2000: Code of Practice on Records Management

Consultation Paper CP 01/2008

Published on 10 June 2008

This consultation will end on 2 September 2008





The National Archives

Freedom of Information Act 2000: Code of Practice on Records Management

Consultation Paper CP 01/2008
Published on 10 June 2008
This consultation will end on 2 September 2008

Contents

Executive Summary	5
Introduction	6
The proposals	7
Questionnaire	13
About you	15
How to respond	16
The Code of Practice	17
The consultation criteria	44
Consultation co-ordinator contact details	44

Executive summary

Section 46 of the Freedom of Information Act 2000 requires the Lord Chancellor to issue a Code of Practice on 'the keeping, management and destruction of their records' by public authorities and by other bodies that are subject to the Public Records Act 1958 or the Public Records Act (Northern Ireland) 1923.

The Code of Practice on Records Management was issued in November 2002 on the basis that it would be reviewed and, if necessary, revised five years after publication. With the approval of Ministers a review was initiated in February 2007 when members of the information and records management community were invited, through letters and publicity, to send comments on the present text of the Code and suggestions for its amendment. The proposed amendments to the Code draw directly on the responses received. They also reflect ongoing consultation with representatives of government departments, local government, the police, higher education and the NHS.

The changes in the Code are primarily to reflect new and emerging practice in the management of records and information and to clarify and, where possible, simplify its provisions. A guiding principle has been that the revised Code should not be perceived as imposing additional burdens on any authority. The Code sets out recommended, not required, good practice; conformance to its provisions is not mandatory.

Introduction

This is a consultation on the revised Code of Practice on Records Management. This revised Code is, subject to the outcome of this consultation, intended to replace the Code issued by the Lord Chancellor, under section 46 of the Freedom of Information Act 2000, in November 2002¹.

The paper invites views on the revised Code. The consultation is aimed at interested parties and in particular at those who would be affected by its provisions, namely those responsible for managing the records of bodies that are subject to the Freedom of Information Act 2000, the Public Records Act 1958 and the Public Records Act (Northern Ireland) 1923.

Revision of the Code of Practice follows consultation on the 2002 Code during which comments and suggestions for its amendment were sought. This consultation took place in Spring 2007 and a report on it was published in July 2007².

This consultation is being conducted in line with the Code of Practice on Consultation issued by the Cabinet Office and falls within the scope of that Code. The consultation criteria set out on page 44 have been followed.

The consultation paper is being widely distributed to public bodies which would be affected by, or otherwise have an interest in, the revised Code. We welcome responses from everyone with views on the subject covered in this paper.

¹ The 2002 Code is available on the Ministry of Justice website <http://www.foi.gov.uk/reference/statCodesOfPractice.htm>

² The report was published on The National Archives website <http://www.nationalarchives.gov.uk/recordsmanagement/code/review.htm>

The proposals

In the five years since the Code of Practice was first issued there have been major changes to records and information management. Many of those changes have been driven by technological developments. Electronic document and records management systems have been implemented by many authorities; general administrative functions such as Finance and Human Resources are supported and enabled by specialised information systems; case management systems have been introduced for delivery of public services; websites are used not only to communicate with the public but also to provide services on an interactive basis; and new ways of collaborative working are appearing all the time, within and between authorities.

The 2002 Code dates from an earlier era. New technology was accepted and being introduced but it co-existed with traditional paper files and registers. This is reflected in the structure of the 2002 Code, in which electronic records were given separate, and quite general, treatment in section 10.

Updating is essential if the Code is to retain its relevance. The challenge this task presented has been to carry forward the content that remains valid and synthesise it with the new content considered necessary.

The National Archives started the review and revision of the Code with some assumptions of its own as to changes that needed to be made. Other themes and issues emerged from the consultation undertaken in 2007³. This part of the consultation paper explains how these aspects and issues have been addressed and seeks views on whether the approach has been successful.

The Foreword

The Foreword is not part of the Code but provides useful background information.

During the review of the 2002 Code it became apparent that there was some overlap between the Foreword (which precedes the Code) and the Introduction (which is part of the Code). It became apparent also that parts of the Foreword related to the Freedom of Information Act as a whole and could be considered redundant in a Code of Practice on Records Management. Text falling into this category and obvious duplication have been identified and removed from the Foreword.

Q1: Do you think the revised Foreword contains sufficient and relevant information?

³ These assumptions and issues are set out in the report on the 2007 consultation, for which see Footnote 2

Part 1: Records Management

This part of the Code applies not only to all bodies subject to the Freedom of Information Act 2000 but also to other bodies that are subject to either the Public Records Act 1958 or the Public Records Act (Northern Ireland) 1923. (Collectively these bodies are referred to as 'relevant authorities' in section 46 of the Freedom of Information Act.) Part 1 of the Code sets out recommended good practice in the 'keeping, management and destruction' of records.

In addition to general updating, some structural and presentational changes have been introduced, for example:

- Sections 5 and 7 of the 2002 Code have been grouped together in a new section 6 called 'Organisational arrangements to support records management';
- New sections have been introduced for collaborative working and performance monitoring;
- Each section now starts with a brief statement summarising the recommendations in the rest of the section;
- Bullet points have been used as a device to break up blocks of text where possible.

Some of these changes are reflected in the text, and questions, that follow.

Q2: Do you think the layout of the revised Code is helpful? Please specify any changes you would recommend.

One of the themes emerging from the 2007 consultation was the need for a clearer explanation of the importance of records management and the benefits of conforming to the Code. Although the 2002 Code explained how good records management supported the Freedom of Information Act, other business benefits which would be equally persuasive to senior managers were not identified. In addition, a greater emphasis on risk management was needed. The revised Code takes account of these points and has included text about benefits and risk at section 5 in particular.

Q3: Do you think the revised Code contains adequate explanations of the importance of good records management and the risks presented by poor records management? Please specify any changes you would recommend.

There was general agreement that the content relating to electronic records – or, as they are more commonly known now, digital records – should be updated and integrated with recommended good practice for other record formats. This raised two issues:

- Could the Code be truly format-neutral or would it be necessary to deal explicitly with the differing requirements of particular formats;
- Could the revised Code be drafted in such a way that it would not be overtaken by new technology shortly after it had been issued.

The approach we have taken is to state general principles and insert some format-specific guidance where necessary, but to avoid references to current media. For example, at section 11, Storage and preservation of records, the specific needs of digital records, in terms of ensuring they continue to remain an accessible and reliable source of information, have been described, but without reference to, for example, magnetic tape.

Q4: Do you agree with the approach taken in the revised Code to records in different formats? Please specify any changes you would recommend.

Q5: Do you think the revised Code gives sufficient guidance on the storage and preservation of digital records? Please specify any changes you would recommend.

There was general agreement that although the 2002 Code provided comprehensive guidance on traditional file systems, it was not always possible to apply its recommendations to the wide range of information and business systems now in use. In addition to paper files (still used by some authorities) and electronic document and records management systems (introduced by some authorities), there may be a variety of databases, case management systems, websites and shared workspaces for carrying out and recording the authority's work. The revised Code recognises this complexity, for example in section 10, and has been drafted with the aim of ensuring that the good practice it describes can be applied to a wide variety of systems.

Q6: Do you think the revised Code deals adequately with the multiple records and information systems likely to be in use at any one time? Please specify any changes you would recommend.

One issue that required careful consideration was the amount of detail to include in the revised Code. One of the initial assumptions made by The National Archives was that the revised Code should focus on principles and outcomes and that some of the process-level detail in the 2002 Code should be removed. This approach would have two benefits:

- Individual authorities would have greater scope to decide for themselves the most appropriate means by which a particular outcome could be achieved;
- It would reduce the risk of the revised Code becoming out of date as technology developed.

However, it was also recognised that some detail would need to be included if the Code was to remain useful and capable of assessment of conformance. The approach adopted has been to include some detail but primarily as illustrative examples of the principles and outcomes.

Q7: Do you think the revised Code has struck the correct balance in terms of level of detail? Have useful details been omitted or should some details that have been included be removed? Please specify any changes you would recommend.

The Code of Practice on Records Management originated as a necessary adjunct to the Freedom of Information Act 2000, in recognition of the fact that the rights of access provided by the Act would be of limited value if records were not created, kept and organised so as to facilitate retrieval of the information they contained. However, following good practice in records and information management promotes compliance with other legislation also, in particular the Data Protection Act 1998. The revised Code seeks to make more explicit the connections between the good practice it recommends and the requirements of other information legislation, for example by referring to the 7th Data Protection Principle in section 9, Security and access.

Q8: Do you think the revised Code has explained sufficiently how following its guidance can support compliance with other information legislation? Have you any suggestions as to where additional connections with other information legislation could be made?

The Code will be read by a wide range of people with varying knowledge and experience of records and information management – not only qualified records managers but also managers and administrators. Terminology is key to a general understanding of the contents of the Code. As far as possible the Code has avoided specialist terminology. Where it has been felt necessary to use it, an explanation has been provided where a term is first used (for example, the term 'metadata' is explained at paragraph 10.3). We considered including a Glossary, as was done in the equivalent Code of Practice under the Freedom of Information (Scotland) Act 2002⁴. Our conclusion was that a Glossary was not necessary and it would be more helpful to readers of the Code if terms they might not understand were explained in the context in which they are first used.

Q9: Do you agree that a separate Glossary is not needed? Should any further terms be explained?

The 2002 Code contained no guidance on monitoring of performance or compliance other than a brief reference in the context of the records management policy, at paragraph 6.2. The revised Code addresses this to a certain extent. It recommends that authorities have in place arrangements for monitoring compliance and for assessing the effectiveness of their records management programme but is not prescriptive as to the performance measures that should be adopted. This is because we consider that individual authorities are likely to have audit and performance monitoring arrangements in place already and should be encouraged to build upon those arrangements in a way that best meets their needs.

Q10: Do you agree with the approach to compliance and performance monitoring in the revised Code? If you do not agree with this approach, please provide examples of performance measures you believe should be specified.

⁴ This Code can be seen at <http://www.scotland.gov.uk/Resource/Doc/1066/0003775.pdf>

When and in what circumstances requested records were destroyed has been an issue in some decisions of the Information Commissioner and the Information Tribunal. The implication is that authorities should keep some records of their destruction of records. How detailed those records should be, in what form they should be kept and for long they should be kept needs to be considered. The revised Code makes some general recommendations in section 13 but is not prescriptive. Instead, it recommends that authorities should make their own risk-based decisions

Q11: Do you agree with the approach taken in the Code with regard to documenting the destruction of records? If you do not agree, please suggest an alternative approach.

Part 2: Review and transfer of public records

This part of the Code applies only to public records, that is to records of, or in the possession of, bodies that are subject to the Public Records Act 1958 or the Public Records Act (Northern Ireland) 1923⁵. It sets out the practice to be followed in the review and transfer of public records to The National Archives⁶, places of deposit for public records appointed under section 4 of the Public Records Act 1958, or the Public Record Office of Northern Ireland.

It is clear from the 2007 consultation that Part 2 of the Code has not dated to the same extent as Part 1. While technology has had its effect – in the earlier transfer of digital records for example – the processes described in Part 2 remain applicable and it is supporting guidance that is more likely to need keeping up to date than the Code itself.

Revision of the Code has provided an opportunity to do some minor restructuring of this Part and to improve its presentation by introducing some headings and bullet points where appropriate. (Note that Question 2 relates to layout and presentation of the revised Code as a whole.)

Once records covered by the Public Records Act 1958 have been selected for permanent preservation the authority must consider not only when the information they contain can be disclosed but also whether there is any reason for them not to be transferred to The National Archives or a place of deposit for public records by the due date⁷. The 1958 Act provides for records to be retained by the department after the due date with the Lord Chancellor's approval⁸. Applications from departments are currently assessed against a set

⁵ These Acts can be seen at <http://www.nationalarchives.gov.uk/documents/public-records-act1958.rtf> and http://www.proni.gov.uk/public_records_act_1923.pdf respectively

⁶ The legal entity to which this provision applies is the Public Record Office. Since April 2003 the Public Record Office has functioned as part of The National Archives and is known by that name. For that reason the name 'The National Archives' is used here.

⁷ At present records that fall under the Public Records Act 1958 are required to be transferred by the time they are 30 years old. This date is currently being reviewed by an independent team which is expected to report to the Prime Minister in Summer 2008. The Code will be amended to reflect any changes introduced as a consequence.

⁸ The position in Northern Ireland is slightly different. Under section 3 of the Public Records Act (Northern Ireland) 1923, records are transferred after 20 years and may be retained for a further period if the principal officer of the department, or a judge if court records are involved, certifies to the Minister of Culture, Arts and Leisure that they should be retained.

of criteria that originated in chapter 9 of the White Paper Open Government (Cm 2290, 1993). This consultation proposes that these criteria be annexed to the Code as Annex B.

Q12: Do you agree that it would be useful to annex to the Code the criteria used to assess applications from departments to retain rather than transfer records?

One of the issues identified in the 2007 consultation was whether Part 2 should provide more detailed guidance on the transfer of digital records, given that such records may require slightly different approaches, for example in the method of transfer (particularly when confidential information is involved) and in determining public access. Having considered the issue we have concluded that the Code should focus on principles and processes that can be applied to any record formats, and leave it to supporting guidance to provide the detailed information and advice that authorities will need.

Q13: Do you agree that detailed guidance for the transfer of digital records should continue to be published separately on The National Archives website and not form part of the Code? If you do not agree, please suggest additional elements you believe should be included in the Code.

One of the lessons learned from experience of the Act is that difficult access decisions benefit from consultation, both internally within the authority and externally with, for example, other authorities that originated the information or whose interests might be affected by premature disclosure. Provision for this consultation has been inserted in the revised Code at section 19.

Q14: Do you agree that the Code should recommend adequate consultation when reviewing the access status of records being prepared for transfer?

One proposal that emerged from the 2007 consultation was that the Code should contain guidance on exemptions, including details of the exemptions that expire after a prescribed period (currently 30 years)⁹. We have considered this suggestion and concluded that it would be preferable to refer people to guidance on exemptions issued by the Ministry of Justice and the Department of the Environment, Food and Rural Affairs, available on their websites and cited in Annex A.

Q15: Have you any other comments on the revised Code, or any suggestions for its amendment? Please give details.

⁹ The exemptions to which this suggestion referred are those in the Act. There are similar exemptions in the separate Environmental Information Regulations which are called 'exceptions' but no expiry periods are specified for them. For simplicity we have used the term 'exemption' in this consultation paper.

Questionnaire

We would welcome responses to the following questions.

- Q1 Do you think the revised Foreword contains sufficient and relevant information?
- Q2 Do you think the layout of the revised Code is helpful? Please specify any changes you would recommend.
- Q3 Do you think the revised Code contains clear explanations of the importance of good records management and the risks presented by poor records management? Please specify any changes you would recommend.
- Q4 Do you agree with the approach taken in the revised Code to records in different formats? Please specify any changes you would recommend.
- Q5 Do you think the revised Code gives sufficient guidance on the storage and preservation of digital records? Please specify any changes you would recommend.
- Q6 Do you think the revised Code deals adequately with the multiple records and information systems likely to be in use at any one time? Please specify any changes you would recommend.
- Q7 Do you think the revised Code has struck the correct balance in terms of level of detail? Have useful details been omitted or should some details that have been included be removed?
- Q8 Do you think the revised Code has explained sufficiently how following its guidance can support compliance with other information legislation? Have you any suggestions as to where additional connections with other information legislation could be made?
- Q9 Do you agree that a separate Glossary is not needed? Should any further terms be explained?
- Q10 Do you agree with the approach to compliance and performance monitoring in the revised Code? If you do not agree with this approach, please provide examples of performance measures you believe should be specified.
- Q11 Do you agree with the approach taken in the Code to documenting the destruction of records? If you do not agree, please suggest an alternative approach.
- Q12 Do you agree that it would be useful to annex to the Code the criteria used to assess applications from departments to retain rather than transfer records?

- Q13 Do you agree that detailed guidance for digital records should continue to be published separately on The National Archives website and not form part of the Code? If you do not agree, please suggest additional elements you believe should be included in the Code.
- Q14 Do you agree that the Code should recommend adequate consultation when reviewing the access status of records being prepared for transfer?
- Q15 Have you any other comments on the revised Code, or any suggestions for its amendment? Please give details.

About you

Please use this section to tell us about yourself

Full name	
Job title or capacity in which you are responding to this consultation exercise (e.g. member of the public)	
Date	
Company/organisation name (if applicable)	
Address (postal or email)	
Postcode	
If you would us to acknowledge receipt of your response please tick here	
Address to which response should be sent if different from above	

If you are a representative of a group, please tell us the name of the group and give a summary of the people or organisations that you represent

How to respond

Please send your response by 2 September 2008 to:

Susan Healy
The National Archives
Kew
Surrey TW9 4DU
Tel: +44 (0)20 8392 5330 ext 2305
Fax: +44 (0)20 8487 9203
Email: codeconsultation@nationalarchives.gov.uk

Extra copies

This consultation paper is available online at
<http://www.nationalarchives.gov.uk/recordsmanagement/code/review.htm> .

A limited number of paper copies is available and can be obtained from the above address

Publication of responses

A paper summarising the responses will be published. It will be available online from the same web page as this paper.

Representative groups

Representative groups are asked to give a summary of the people and organisations they represent when they respond.

Confidentiality

Information provided in response to this consultation, including personal information, may be published or disclosed in accordance with the access to information regimes (these are primarily the Freedom of Information Act 2000, the Data Protection Act 1998 and the Environmental Information Regulations 2004).

If you want the information you provide to be treated as confidential, please be aware that, under the Freedom of Information Act, there is a statutory Code of Practice with which public authorities must comply and which deals, among other things, with obligations of confidence. In view of this, it would be helpful if you could explain to us why you regard the information you have provided as confidential. If we receive a request for disclosure of the information we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding on The National Archives.

The National Archives will process your personal data in accordance with the Data Protection Act and in the majority of circumstances this will mean that your personal data will not be disclosed to third parties.

The Code of Practice

Contents

Foreword	18
General	18
Role of the Information Commissioner	19
Authorities subject to the Public Records Act	19
Role of the Lord Chancellor’s Advisory National Records and Archives	20
Code of Practice	21
Introduction	21
Part 1 Records management	23
Why records management is important	23
Organisational arrangements to support records management	24
Records management programme	25
Records management policy	25
Creation of records to meet corporate requirements	26
Records systems	28
Storage and preservation of records	30
Security and access	31
Disposal of records	31
Records created in the course of collaborative working or through out-sourcing	34
Monitoring and reporting on records and information management	34
Part 2 Review and transfer of public records	35
Annex A Standards and guidance supporting the Code of Practice	39
Annex B Criteria for the retention of public records	42

Foreword

General

- (i) The Code of Practice which follows fulfils the duty of the Lord Chancellor under section 46 of the Freedom of Information Act 2000 (the Act). This foreword provides background but does not form part of the Code itself.
- (ii) The Code provides guidance (in Part 1) to all public authorities as to the practice which it would, in the opinion of the Lord Chancellor, be desirable for them to follow in connection with the keeping, management and destruction of their records. It also describes (in Part 2) the procedure to be followed for timely and effective review and transfer of public records¹⁰ to The National Archives¹¹ or to places of deposit (as defined in section 4 of the Public Records Act 1958) or to the Public Record Office of Northern Ireland under the Public Records Act 1958 or the Public Records Act (Northern Ireland) 1923¹².
- (iii) The Code applies not only to public authorities but also to other bodies that are subject to the Public Records Act 1958 and the Public Records Act (Northern Ireland) 1923. Collectively they are called relevant authorities.
- (iv) Freedom of information legislation is only as good as the quality of the records and other information to which it provides access. Such rights are of little use if reliable records are not created in the first place, if they cannot be found when needed or if the arrangements for their eventual destruction or transfer to an archives service are inadequate. Consequently, all relevant authorities are strongly encouraged to pay heed to the guidance in the Code.
- (v) The Code is a supplement to the provisions in the Act and its adoption will help authorities comply with their duties under the Act. Public authorities should seek legal advice as appropriate on general issues relating to the implementation of the Act or its application to individual cases. The Code is complemented by the Code of Practice under section 45 of the Act and by the Code of Practice under Regulation 16 of the Environmental Information Regulations 2004 (the EIR).
- (vi) Authorities should note that if they fail to comply with the Code, they may also fail to comply with legislation relating to the creation, management, disposal, use and re-use of records and information, for example the Public Records Act 1958, the Data Protection Act 1998, and the Re-use of Public Sector Information Regulations 2005, and they may consequently be in breach of their statutory obligations.

¹⁰ For the avoidance of doubt, the term 'public records' includes Welsh public records as defined by section 148 of the Government of Wales Act 2006.

¹¹ The legal entity to which this provision applies is the Public Record Office. Since April 2003 the Public Record Office has functioned as part of The National Archives and is known by that name. For that reason the name 'The National Archives' is used in this Code.

¹² The Public Records Acts can be seen at <http://www.nationalarchives.gov.uk/documents/public-records-act1958.rtf> and http://www.proni.gov.uk/public_records_act_1923.pdf respectively

Role of the Information Commissioner

- (vii) The Information Commissioner will promote the observance of the Code by relevant authorities, acting as required by the Act. If it appears to the Information Commissioner that the practice of an authority in relation to the exercise of its functions under the Act does not conform to that set out in the Code, he may issue a practice recommendation under section 48 of the Act. A practice recommendation will be in writing and will specify the provisions of the Code that have not been met and the steps that should, in his opinion, be taken to promote conformity with the Code.
- (viii) If the Information Commissioner reasonably requires any information in order to determine whether the practice of an authority conforms with that recommended in this Code, he may serve on the authority a notice (known as an 'information notice') under section 51 of the Act. An information notice will be in writing and will require the authority to provide the Information Commissioner with specified information relating to conformity with the Code. It will also contain particulars of the rights of appeal conferred by section 57 of the Act.
- (ix) Under section 54 of the Act, if an authority fails to comply with an information notice, the Information Commissioner may certify in writing to the court that the authority has failed to comply. The court may then inquire into the matter and, after hearing any witnesses who may be produced against or on behalf of the authority, and after hearing any statement that may be offered in defence, deal with the authority as if it had committed a contempt of court.

Authorities subject to the Public Records Act

- (x) The guidance on records management and the transfer of public records in the Code should be read in the context of existing legislation affecting the management of records. In particular, the Public Records Act 1958 (as amended) gives duties to public record bodies in respect of the records they create or hold. It also requires the chief executive of The National Archives¹³ to supervise the discharge of those duties.
- (xi) The Public Records Act (Northern Ireland) 1923 sets out the duties of public record bodies in Northern Ireland in respect of the records they create and requires that records should be transferred to, and preserved by, the Public Record Office of Northern Ireland.
- (xii) The Information Commissioner will promote the observance of the Code in consultation with the chief executive of The National Archives when dealing with bodies which are subject to the Public Records Act 1958 and with the Deputy Keeper of the Records of Northern Ireland for bodies subject to the Public Records Act (Northern Ireland) 1923. Before issuing a practice recommendation under section 48 of the Act to a body subject to

¹³ The title 'Keeper of Public Records' is used in the Public Records Act 1958 and the Freedom of Information Act 2000. This is one of the titles of the chief executive of The National Archives. The title 'chief executive of The National Archives' is used in this Code in recognition of the fact that it is the title used for operational purposes.

either of the Public Records Acts, the Information Commissioner will consult the chief executive of The National Archives or the Deputy Keeper of the Records of Northern Ireland as appropriate.

Role of the Lord Chancellor's Advisory Council on National Records and Archives

- (xiii)** The Advisory Council on National Records and Archives¹⁴ (hereafter 'the Advisory Council') has a statutory role to advise the Lord Chancellor on matters concerning public records in general and on the application of the Act to information in public records that are historical records. Having received the advice of his Advisory Council, the Lord Chancellor, may prepare and issue guidance. The guidance may include advice on the review of public records and on the periods of time for which the Advisory Council considers it appropriate to withhold categories of sensitive records after they have become historical records.¹⁵
- (xiv)** The National Archives provides support as appropriate to the Advisory Council in its consideration of applications from authorities relating to retention or access to public records and in its preparation of guidance to authorities.
- (xv)** In Northern Ireland the Sensitivity Review Group, consisting of representatives of Northern Ireland departments, provides advice on the release of public records. The Public Record Office of Northern Ireland provides support to the Group. Guidance may be issued by the Deputy Keeper of the Records of Northern Ireland following consultation with the Departments responsible for the records affected by the guidance.

¹⁴ The legal entity to which this provision applies is the Advisory Council on Public Records. Since April 2003 the Council has functioned as The Advisory Council on National Records and Archives and so that name is used in this Code.

¹⁵ The term 'historical record' is defined at section 62 of the Act.

Code Of Practice on (1) The Management of Records by Relevant Authorities and (2) The Review and Transfer of Public Records under the Freedom of Information Act 2000

The Lord Chancellor, after consulting the Information Commissioner and the appropriate Northern Ireland Minister, issues the following Code of Practice pursuant to section 46 of the Freedom of Information Act 2000.

Laid before Parliament on [date not yet known] pursuant to section 46(6) of the Freedom of Information Act 2000.

Introduction

1 The aims of the Code are:

- 1 To set out the practices which relevant authorities¹⁶ should follow in relation to the creation, keeping, management and destruction of their records (Part 1 of the Code); and
- 2 To describe the arrangements which public record bodies should follow in reviewing public records and transferring them to The National Archives or to a place of deposit for public records, or to the Public Record Office of Northern Ireland (Part 2 of the Code).

¹⁶ Relevant authorities is the collective term used in the Act for bodies that are public authorities under the Freedom of Information Act and bodies that are not subject to that Act but are subject to the Public Records Act 1958 or the Public Records Act (Northern Ireland) 1923

- 2 Part 1 of the Code provides a framework for the management of their records by relevant authorities. 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 to The National Archives¹⁷, a place of deposit for public records or the Public Record Office of Northern Ireland. 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 indicate for how long they should apply. More detailed guidance on both themes has been published separately. Standards and guidance which support the objectives of this Code most directly are listed at Annex A.
- 3 For the purposes of this Code, 'records' are defined as in the relevant British Standard¹⁸, namely 'information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business'. Some other specific terms which are not defined in the Act have been defined in the context in which they first appear, for example metadata (10.3) and disposal (13.1). Other words and expressions used in this Code have the same meaning as the same words and expressions used in the Act.
- 4 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 records management systems but also 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.

¹⁷ See footnote 11

¹⁸ BS ISO 15489-1:2001 Information and documentation – Records management – Part 1: General

Part 1 Records management

5 Why records management is important

5.1 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 is important for a number of reasons:

- It supports compliance with the Act. Access rights are of limited value if records and other information cannot be found when requested or, when found, cannot be relied upon as an authoritative source of evidence and information. Good records and information management benefits those requesting information because it provides some assurance that the information provided will be complete and accurate. 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, if it is information that they might be expected to hold. It also supports control and delivery of information promised in the authority's Publication Scheme or required to be published by the Environmental Information Regulations 2004 (the EIR);
- It supports the authority's business and discharge of its functions, promotes business efficiency and underpins service delivery by ensuring that authoritative information about past activities can be retrieved, used and relied upon in current business;
- It supports compliance with other legislation which requires records and information to be kept, controlled and accessible, such as the Data Protection Act 1998, employment legislation and health and safety legislation;
- 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;
- It enables protection of the rights and interests of the authority, its staff and its stakeholders;
- It increases efficiency and cost-effectiveness by ensuring that records are disposed of when 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.

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

- Poor decisions based on inaccurate or incomplete information;
- Inconsistent levels of service;
- Financial or legal loss if information required as evidence is not available;
- Non-compliance with statutory or other regulatory requirements;
- Failure to handle confidential information with an appropriate level of security and the possibility of unauthorised access or disposal taking place;

- 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.

6 Organisational arrangements to support records management

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

6.1 These arrangements should include:

- Recognition of records management as a core corporate function, either separately or as a clearly identified 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;
- Inclusion 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;
- 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 champion, for example a board member, and allocation of operational responsibility to a member of staff with the necessary knowledge and skills. In small authorities it may be more practicable 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 and the Re-use of Public Sector Information Regulations 2005, or will work closely with those people;
- Clearly defined responsibilities, applying to staff at all levels, for creating, keeping and managing records throughout the authority. 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;
- 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. Examples of these systems are records management systems, datasets, function-specific systems such as case management, finance and geographical information systems, websites and shared workspaces;

- Consideration of records management issues when planning or implementing IT systems;
- Induction and other training to ensure that all staff are aware of the authority's records management policies, standards, procedures and guidelines and that they understand their personal responsibilities. This should be extended to temporary staff, contractors and consultants who are undertaking work that it has been decided should 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;
- An agreed programme for managing records in accordance with this part of the Code;
- Provision of the financial and other resources required to achieve agreed objectives in the records management programme.

7 Records management programme

Authorities should have in place a programme for managing their records and other information.

7.1 The programme should cover all records held by the authority and should include the following elements:

- A records management policy;
- Provisions for identifying the authority's requirements for records and for creating those records;
- Provisions for the storage and maintenance of records;
- Provisions for security and access;
- Provisions for the disposal of records;
- Provisions for records created in the course of collaborative working or through out-sourcing;
- Provisions for monitoring, auditing and reporting on compliance and the effectiveness of the programme.

7.2 Recommended good practice for each of these elements is set out in the remaining sections of this part of the Code.

8 Records management policy

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

- 8.1** The policy should be endorsed by senior management, for example at board level, and should be readily available to staff at all levels.
- 8.2** 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:
- Set out the authority's commitment to create, keep and manage records which document its principal activities;
 - Outline the role of records management and its relationship to the authority's overall business strategy;
 - Identify and make appropriate connections to related policies, such as those dealing with information security and data protection;
 - 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 it should be documented and to use those records appropriately;
 - Indicate how compliance with the policy and the supporting standards, procedures and guidelines will be monitored.
- 8.3** 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 changes, in order to assess whether it needs amendment.

9 Creation of records to meet corporate requirements

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

Deciding what records should be created

- 9.1** Authorities should consider what records they are likely to need about their activities, and the risks of not having them, taking into account the following factors:
- 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 Charity Commission is required by its legislation to keep an accurate and up-to-date register of charities. It also includes standards applying to the sector or authority;
 - 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 information about what it did during previous outbreaks and who was responsible for specific measures, such as closing public footpaths;

- 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 protect itself if challenged;
- The need to explain, and if necessary justify, past actions in the event of an audit or other investigation. For example, the Audit Commission will expect to find accurate records of expenditure of public funds. Or, if an applicant complains to the Information Commissioner's Office (ICO) about the handling or outcome of an FOI request, the ICO will expect the authority to provide details of how the request was handled and, if applicable, why it refused to provide the information.

9.2 Having considered these factors, authorities should set business rules for the creation of records, identifying what records should be created, by whom, at what point in the process or transaction, what those records should contain and where and how they should be stored.

9.3 Authorities should assess whether they may need to rely on certain records as particularly authoritative, so that they can be shown to:

- Be authentic, that is, they are what they say they are;
- Be reliable, that is, they can be trusted as a full and accurate record;
- Have integrity, that is, they have not been altered;
- Be usable, that is, they can be retrieved, read and used.

Authorities should put in place controls to ensure that records on which particular evidential weight may be placed can be shown to meet these criteria. For example, when there are multiple versions of a document such as guidance, it should be clear which version was issued for use.

Ensuring those records are created

9.4 All staff should be aware of which records the authority has decided to create and of their personal responsibility to create 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 as evidence for corporate use.

9.5 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.

9.6 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 multiple or personal copies of documents should be discouraged.

Knowing what records are held

9.7 The effectiveness of records systems depends on knowledge of what records and other information are held, 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:

- Locate and retrieve information required for business purposes or to respond to an information request;
- Produce a Publication Scheme or a reliable list of information assets available for re-use;
- Apply the controls required to manage risks associated with the records;
- Ensure records are disposed of when no longer needed.

9.8 Authorities therefore need to gather and maintain data on information and record assets. This can be gathered 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.

10 Records systems

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

10.1 Authorities should decide in what format their records are to be stored, based on their needs. 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, creating documents through word processing software or using case management systems, then it is good practice to hold the resulting records electronically.

10.2 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, shared workspaces and systems containing records that are physical objects, such as a set of files or registers. Systems should be designed to meet the authority's operational needs and using them should be an integral part of business operations and processes.

10.3 Records systems should have the following characteristics:

- 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;
- They should enable quick and easy retrieval of information;
- They should have the functionality required for records management processes, for example deletion of information in accordance with agreed disposal dates;

- They should enable the context of each record and its relationship to other records to be understood. This can be achieved by classifying and indexing records within a file plan or business classification scheme that brings together related records and enables 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;
- They should contain both information and metadata. (Metadata here is information about the context within which records were created, their structure and how they have been managed over time. For records that are physical objects it includes their location.) 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. Metadata can refer to records within an electronic records system or to records that are physical objects but are controlled either from such a system or by a paper register or card index. With records that are physical objects, metadata can be as simple as a file title, date range and the name of the originating body on the file cover;
- They should provide secure storage to the level of protection required by the nature, contents and value of the information in them. For records held in an electronic system this includes a capacity to control access to particular information if necessary, for example by limiting access to named individuals or requiring passwords. For records that are physical objects this includes a capacity to lock storage cupboards or areas and to log access to them and any withdrawal of records from them;
- They should enable an audit trail to be produced of all occasions on which a record has been seen, used, amended and deleted.

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

10.5 Records should not remain live indefinitely with a capacity for new information to be added to them, for example another document added to a folder. They should be closed, that is, have their contents frozen, at an appropriate time.

10.6 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 a health record. Size is a factor with physical records in particular and a folder should not be too big to be handled easily. For records held electronically 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.

10.7 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.

11 Storage and preservation of records

Storage should be designed to ensure that records can be retrieved and used for as long as access to them is required.

- 11.1 Storage accommodation 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.
- 11.2 Storage should follow accepted standards in respect of the storage environment, fire precautions, health and safety and, for records that are physical objects, physical organisation. It should allow easy and efficient retrieval of information but also prevent damage, loss or unauthorised access.
- 11.3 The whereabouts of records that are physical objects should be known at all times and removal from and return to storage areas should be logged.
- 11.4 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 paper) storage which may be a more economical and efficient way to store them.
- 11.5 Records should remain usable for as long as they are required. With records that are physical objects, 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.
- 11.6 Records held electronically will not remain usable unless precautions are taken. Authorities should put in place a strategy for their continued maintenance designed to ensure that information remains intact and usable for as long as it is required. The strategy should provide for migration at regular intervals of both the storage media and the software within which the information and metadata are held and for regular tests during the intervening period.
- 11.7 Back-up copies of records held electronically should be kept and should be checked 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 without compromising the authority's need for access to reliable back-ups if required.
- 11.8 Metadata 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. Metadata for records that are physical objects, such as registers or indexes in either electronic or physical format, should also be kept for as long as the records and should continue to be capable of being accessed and used.

- 11.9** Business continuity plans should identify and safeguard records considered vital to the organisation, that is records that would be essential to the continued functioning or reconstitution of the organisation in the event of a disaster and records that are essential to protection of the organisation's legal and financial rights. The plans should include actions to protect and recover these vital records.

12 Security and access

Authorities should have in place arrangements for controlling access to their records and for keeping adequate records of such access.

- 12.1** Authorities should ensure that their storage arrangements, handling procedures and arrangements for transmission of records reflect good practice in information security.
- 12.2** 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. 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.
- 12.3** External access should be provided in accordance with relevant legislation.
- 12.4** An audit trail should be kept of provision of access, especially to people outside the immediate work area.

13 Disposal of records

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

- 13.1** For the purpose of this Code, disposal is defined as the point in a record's lifecycle at which the record is either destroyed or transferred to an archives service for permanent preservation.
- 13.2** As a general principle, records should be destroyed as soon as they have ceased to be needed by the authority for reference purposes, to comply with regulatory requirements or to protect legal and other rights and interests. This ensures that office and server space are not taken up by records of no further use to the authority. For records containing personal information it also ensures compliance with the 5th data protection principle which requires that personal data is retained only for as long as it is needed.

13.3 Records should be retained after they have ceased to be of use to the authority only in the following circumstances:

- 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;
- They have long-term historical value 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.)

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

- Reflect the authority's continuing need for access to the information or the potential value of the records for historical research;
- Are based on consultation between records management staff, staff of the relevant business unit and legal advisers;
- Have been formally adopted by the authority;
- Are applied by properly authorised staff;
- Take account of security and confidentiality needs.

13.5 The policies should take the form of:

- An overall policy, stating in broad terms the functions from which records are likely to be selected for permanent preservation or the types of records likely to be selected for permanent preservation. The policy could be either a separate policy, part of the records management policy or a preamble to disposal schedules;
- 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.

13.6 Disposal schedules should contain sufficient details about the records to enable them to be easily identified and the disposal action applied to them on a routine basis. These details should include:

- The function to which the records relate (if that is not clear from background papers);
- The authority for the disposal action (such as a statutory provision or specific guidance);
- The business unit if applicable;

- The dates of the records;
- Any relevant reference numbers that might aid identification of the records;
- The whereabouts of the records;
- The retention period and disposal action.

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

- 13.7** 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.
- 13.8** 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. 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.
- 13.9** In some cases there will be more than one copy of a record. For example, there are likely to be back-up copies of records held electronically. A record cannot be considered to have been completely destroyed until all back-up copies have been destroyed, if there is any possibility that the data could be recovered.
- 13.10** 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 as the previous existence of records may be relevant information. However, the level of detail and for how long it should be retained will depend on an assessment of the risks to the authority if detailed information cannot be produced on request. 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 defend themselves against a charge under section 77 of the Act that records were destroyed in order to prevent their disclosure in response to an access request. Where server space makes this difficult one option is to extract destruction audit trail metadata and store it off-line.
- 13.11** 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 this Code sets out the arrangements that apply to the review and transfer of public records. The approach set out in Part 2 may be relevant to the review and transfer of other types of records also.

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

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

- 14.1** When authorities are working in partnership with other organisations, sharing information and contributing to a joint records system, they should ensure that all parties have agreed formally what information should be contributed and kept and by whom, who should have access to the records, what disposal arrangements are in place and which body holds the information for the purposes of the Act. Instructions and training should be provided to staff involved in such collaborative working.
- 14.2** 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, and details should be kept of when and under what conditions information has been shared, and how undertakings given to the original source of the information have been respected.
- 14.3** 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 should ensure that the provisions of this Code are applied to those records.

15 Monitoring and reporting on records and information management

Authorities should put in place arrangements for monitoring compliance with agreed policies and procedures and for assessing the overall effectiveness of the programme.

- 15.1** Authorities should identify performance indicators that reflect their information management needs and arrangements and the risks that non-compliance would present to the authority. They should then put in place the means by which performance can be measured. For example, if quantitative indicators such as statistics are to be used, the data from which they will be generated must be kept. Qualitative indicators, for example whether guidance is being followed, can be measured by spot checks of files or by interviews.
- 15.2** 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 being. 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 public records

16 Purpose of Part 2

- 16.1** This part of the Code applies only to authorities which are subject to the Public Records Act 1958 or the Public Records Act (Northern Ireland) 1923. Under those Acts, authorities are required to identify records worthy of permanent preservation and transfer them to The National Archives¹⁹, a place of deposit for public records or the Public Record Office of Northern Ireland as appropriate. This part of the Code sets out the arrangements which those authorities should follow to ensure the timely and effective review and transfer of public records. Arrangements should be established and operated under the supervision of The National Archives or, in Northern Ireland, in conjunction with the Public Record Office of Northern Ireland.
- 16.2** The general purpose of this part of the Code is to facilitate the performance by the authorities, The National Archives, the Public Record Office of Northern Ireland and other archives services of their functions under the Act. In reviewing records for public access, authorities should ensure that public records become available at the earliest possible time in accordance with the Act and the EIR.

17 Selection of records for permanent preservation

- 17.1** Section 13 of this Code describes the arrangements that authorities should follow for the disposal of records. In this context, disposal includes the decision to transfer records to an archives service for permanent preservation.
- 17.2** 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 13.

18 Transfer or retention of records

- 18.1** Under the Public Records Act 1958, records selected for preservation may be transferred either to The National Archives or to a place of deposit for public records appointed by the Lord Chancellor²⁰ under section 4 of that Act. For guidance on which records may be transferred to which archives service, and on the disposition of UK public records relating to Northern Ireland, see Annex A. For the avoidance of doubt, Part 2 of this Code applies to all such transfers.
- 18.2** The Public Records Act 1958 also provides for public records selected for preservation to be transferred to The National Archives or another archives service by the time they are 30

¹⁹ See Footnote 11 for an explanation of why this name has been used in this Code.

²⁰ The Lord Chancellor has delegated the power to appoint places of deposit to the chief executive of The National Archives or another officer of appropriate authority.

years old²¹ unless the Lord Chancellor gives authorisation for them to be retained in the department for a longer period of time under section 3(4) of the Public Records Act 1958. By agreement with The National Archives, transfer may take place before 30 years.

- 18.3** Applications to retain records should be submitted to The National Archives for review and advice. The Lord Chancellor's Advisory Council will then consider the case in favour of retention beyond the 30 year period. The Advisory Council will consider the case for retaining individual records, or coherent batches of records, on the basis of the guidance in chapter 9 of the White Paper *Open Government* (Cm 2290, 1993) or subsequent revisions of Government policy. Some categories of records are covered by a standard authorisation by the Lord Chancellor (known as 'blanket retentions') which are reviewed every 10 years. (See Annex B for the retention criteria and a description of the categories covered by the 'blanket'.)
- 18.4** In Northern Ireland, transfer under the Public Records Act (Northern Ireland) 1923 to the Public Record Office of Northern Ireland takes place normally at 20 years. Under section 3 of that Act, records may be retained for a further period if the principal officer of the department, or a judge if court records are involved, certifies to the Minister of Culture, Arts and Leisure that they should be retained.
- 18.5** It is the responsibility of authorities transferring records to ensure that those records are adequately prepared and are transferred with the level of security appropriate to the confidentiality of the information they contain.

19 Reviewing the access status of records for transfer

- 19.1** Authorities preparing public records for transfer to The National Archives, a place of deposit for public records or the Public Record Office of Northern Ireland should review the access status of those records. The purpose of this review is to:
- Consider which information must be available to the public on transfer because no exemptions under the Act or the EIR apply²²;
 - Consider whether the information must be released in the public interest, notwithstanding the application of an exemption under the Act or the EIR;
 - Consider which information must be available to the public at 30 years because relevant exemptions in the Act have ceased to apply²³;
 - Consider which information merits continued protection in accordance with the provisions of the Act or the EIR.

²¹ The date by which records must be transferred is currently being reviewed by an independent team which is expected to report to the Prime Minister in Summer 2008. This Code will be amended to reflect any changes introduced as a consequence.

²² In the EIR, exemptions are called exceptions. For simplicity the term exemption is used throughout the Code and should be taken to apply also to exceptions in the EIR

²³ At present some exemptions in the Act fall away after 30 years. Their duration is currently being reviewed by an independent team which is expected to report to the Prime Minister in Summer 2008. The Code will be amended to reflect any changes introduced as a consequence.

- 19.2** 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. This is particularly advisable for records that are less than 30 years old.
- 19.3** If the review results in identification of specified information which the authority considers ought not to be released under the terms of the Act or the EIR, the authority should prepare a schedule that:
- Identifies the information precisely;
 - Cites the relevant exemption(s);
 - Explains why the information may not be released;
 - Identifies a date at which either release would be appropriate or the case for release should be reconsidered.
- 19.4** Authorities should consider whether parts of records might be released if the sensitive information were redacted, i.e. rendered invisible or blanked out. Information that has been redacted should be stored securely and should be returned to the parent record when the exemption has ceased to apply.
- 19.5** This schedule should be submitted to The National Archives or, in Northern Ireland, to the Public Record Office of Northern Ireland prior to transfer.

20 Outcome of the access review

20.1 Transfer of open records

The transferring department should designate records as open if no exempt information is identified. There will be no formal review of this designation by The National Archives.

20.2 Transfer of closed records to The National Archives

In the first instance, the schedule described above should be submitted to The National Archives for review and advice. If the outcome of the review is that some or all of the information in the records should be closed after it is 30 years old, the schedule will be considered by the Advisory Council. The Advisory Council may respond as follows

- By accepting that the information may be withheld for longer than 30 years and earmarking the records for release or re-review at the date identified by the authority;
- By accepting that the information may be withheld for longer than 30 years but asking the authority to reconsider the later date designated for release or re-review;
- By questioning the basis on which it is considered that the information may be withheld for longer than 30 years and asking the authority to reconsider the case;
- By taking such other action as it deems appropriate within its role as defined in the Public Records Act 1958.

If the Advisory Council accepts that the information should be withheld, the records will be transferred as closed (in whole or in part as appropriate) and the relevant closure period applied.

20.3 Transfer of closed records to places of deposit for public records

Places of deposit should be informed which records cannot be made publicly available on transfer, which exemptions apply to the information they contain and for what reason, and for how long those exemptions should be applied.

20.4 Transfer of closed records to the Public Record Office of Northern Ireland

In Northern Ireland there are separate administrative arrangements requiring that schedules be submitted to the Public Record Office of Northern Ireland for review and advice. If the outcome of the review is that the records should be closed after transfer, the schedule will be considered by the Sensitivity Review Group (for which see Foreword paragraph (xv)). The Sensitivity Review Group may respond as follows:

- By accepting that the information should be withheld for longer than 30 years and earmarking the records for release or re-review at the date identified on the schedule;
- By questioning the basis on which it is considered that the information may be withheld for longer than 30 years and asking the responsible authority to reconsider the case.

21 Access after transfer

21.1 Freedom of Information requests after transfer

For the avoidance of doubt, none of the actions described in this Code affects the statutory rights of access established under the Act or the EIR. Requests for exempt information in public records transferred to The National Archives, a place of deposit for public records or the Public Record Office of Northern Ireland will be dealt with on a case by case basis in accordance with the provisions of the Act or the EIR.

21.2 Expiry of closure periods

When an exemption has ceased to apply under section 63 of the Act the records will become automatically available to members of the public at the date specified in the finalised schedule (i.e. the schedule after it has been reviewed by the Advisory Council or the Sensitivity Review Group as appropriate). In other cases, if the authority concerned wishes to extend the period during which the information is to be withheld, it should submit a further schedule explaining the sensitivity of the information. This is to be done before the expiry of the period stated in the earlier schedule. The National Archives and Advisory Council will then review the schedule in accordance with the process described in paragraph 20.2 above. In Northern Ireland, Ministerial agreement is required for any further extension of the stated period.

Annex A Standards and guidance supporting the Code of Practice

Part 1 of the Code

1. British Standards (BSI)

Relevant Standards issued by the British Standards Institution include:

BS ISO 15489-1, *Information and documentation – Records management – Part 1: General*

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*

BS 10008 *Evidential weight and legal admissibility of electronic information – Specification* [draft standard issued for public consultation 30 April 2008]

BIP 0008:2004 *Code of Practice for legal admissibility and evidential weight of information stored electronically*

BS 8470:2006, *Secure destruction of confidential material. Code of practice*

BS 4783, *Storage, transportation and maintenance of media for use in data processing and information storage*

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

The National Archives publishes standards, guidance and toolkits on the management of records in all formats, covering their entire life cycle. Initially written for government departments, they can be applied in other parts of the public sector. They are available on The National Archives website at

http://www.nationalarchives.gov.uk/recordsmanagement/?source=ddmenu_services1 and
http://www.nationalarchives.gov.uk/electronicrecords/?source=ddmenu_services2

In addition, a standard on metadata for records management is available through Govtalk – see

http://www.govtalk.gov.uk/documents/Records_management_metadata_standard_2002.pdf

3. Sector-specific guidance

Guidance is available for specific sectors as follows:

Local government – The Records Management Society has issued guidelines on retention and information audits for local government – see

<http://www.rms-gb.org.uk/resources>

Further and higher education – JISC (Joint Information Systems Committee) Infonet has produced an information management Infokit – see

<http://www.jiscinfonet.ac.uk/information-management>

Schools – The Records Management Society has issued a records management toolkit for schools – see

<http://www.rms-gb.org.uk/resources/848>

The police – The Home Secretary has issued a code of practice on the management of police information – see

<http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/CodeofPracticeFinal12073.pdf?view=Standard&pubID=224859>

It is supported by guidance produced by the National Centre of Policing Excellence on behalf of the Association of Chief Police Officers – see

<http://www.npia.police.uk/en/8492.htm>

<http://www.crimereduction.homeoffice.gov.uk/policing21.htm>

The National Health Service – The Department of Health has issued a code of practice for the NHS – see

http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4131747

Part 2 of the Code

4. Transfer of records to the National Archives or a place of deposit

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/documents/acquisition_strategy.pdf and

<http://www.nationalarchives.gov.uk/recordsmanagement/disposition/faq.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/foi_guide.pdf

5. Transfer of records to the Public Record Office of Northern Ireland

The Public Record Office of Northern Ireland has published guidance on transferring records – see

http://www.proni.gov.uk/guidance_for_reviewers_on_the_completion_of_pr_14_historical_forms.pdf and

http://www.proni.gov.uk/guidance_for_reviewers_on_the_completion_of_pr_14_forms.pdf

6. Determining whether exemptions apply

Guidance on FOI exemptions has been issued by the Ministry of Justice – see

<http://www.dca.gov.uk/foi/guidance/index.htm>

Guidance on EIR exceptions has been issued by the Department of the Environment, Food and Rural Affairs – see

<http://www.defra.gov.uk/corporate/opengov/eir/guidance/full-guidance/pdf/guidance-7.pdf>

See also guidance from The National Archives in *Access to Public Records* at

http://www.nationalarchives.gov.uk/documents/access_manual.pdf

and *Redaction: guidelines for the editing of exempt information from paper and electronic documents prior to release* at

http://www.nationalarchives.gov.uk/documents/redaction_toolkit.pdf

Annex B Criteria for the retention of public records

Section 3(4) of the Public Records Act 1958 requires departments to transfer to The National Archives – or to an approved place of deposit – records that have been selected for permanent preservation. This must take place by the time the records are thirty years old²⁵, unless departments receive authorisation to retain them. Provision for retention is made in the second part of section 3(4).

“In the opinion of the person who is responsible for them, they are required for administrative purposes or ought to be retained for any other special reason and, where that person is not the Lord Chancellor, the Lord Chancellor has been informed of the facts and given his approval.”

Authorisation is provided by the Lord Chancellor acting on advice from his Advisory Council, which scrutinises all applications.

The most common grounds for retention are set out below. The numbers are those used on applications to the Advisory Council. Normally a retention period of up to 5 years is granted when grounds 1 to 5 or 7 are satisfied and up to 10 years for ground 6.

Grounds for retention

- 1 Records or series of records which have not been selected for transfer to The National Archives or a place of deposit, but which the department has retained beyond 30 years because they are required for its own administrative purposes.
- 2 Records or series of records that have been selected for transfer to The National Archives or place of deposit but are still required for administrative purposes.
- 3 Series of records which are known to contain items over 30 years old, but which it is more effective to treat as a unit for appraisal purposes to review at a later date related to the age of other records in the series.
- 4 Records or series of records which form part of a backlog awaiting appraisal or preparation for transfer.
- 5 Records or series of records which have been retained for the writing of official histories.
- 6 Records retained in departments on security or other specified grounds.
- 7 Records of international organisations for which there is not yet any agreement for release.

²⁵ See footnote 21

Blanket retentions

In some instances the Lord Chancellor has given his approval to the retention of large categories of records of a similar character. The reasons for non-disclosure are the same for each record covered by such approvals. The most widely used blanket is that relating to records held by the security and intelligence agencies.

The consultation criteria

The six consultation criteria are as follows:

- 1 Consult widely throughout the process, allowing a minimum of twelve weeks for written consultation at least once during the development of the policy.
- 2 Be clear about what your proposals are, who may be affected, what questions are being asked and the timescale for responses.
- 3 Ensure that your consultation is clear, concise and widely accessible.
- 4 Give feedback regarding the responses received and how the consultation process influenced the policy.
- 5 Monitor your department's effectiveness at consultation, including through the use of a designated consultation co-ordinator.
- 6 Ensure your consultation follows better regulation best practice, including carrying out an Impact assessment if appropriate.

These criteria must be reproduced within all consultation documents.

Consultation co-ordinator contact details

If you have any complaints or comments about the consultation process rather than about the topic covered by this paper you should contact Hywel Thomas, The National Archives Consultation Co-ordinator:

Hywel Thomas
Consultation Co-ordinator
The National Archives
Kew
Surrey TW9 4DU.

Tel: +44 (0)208 392 5321
Fax: +44 (0)20 8487 9203
Email: hywel.thomas@nationalarchives.gov.uk

If your complaint or comments refer to the topic covered by this paper rather than to the consultation process please direct them to the contact given under the **How to Respond** section of this paper on [page 16](#).

The National Archives
Kew, Richmond
Surrey TW9 4DU
nationalarchives.gov.uk

June 2008