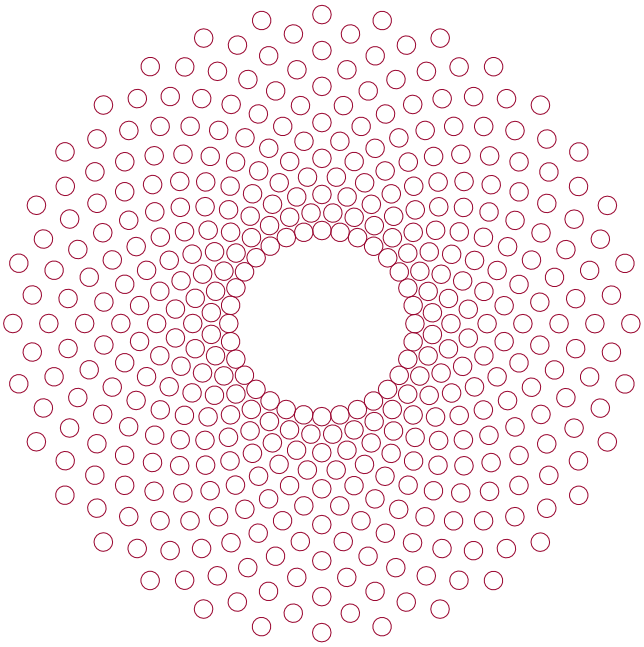
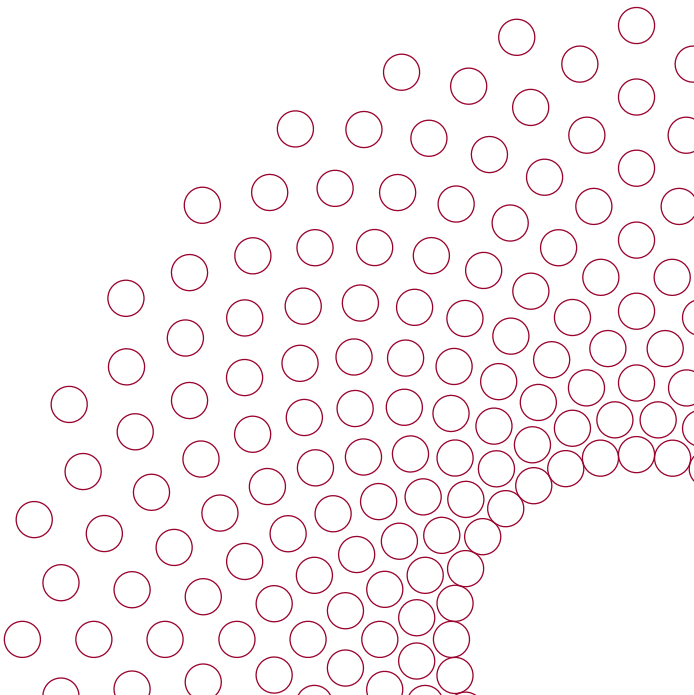
Ministry of JUSTICE

The National Archives

Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000





Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000

Presented to Parliament by the Lord Chancellor
pursuant to section 46(6) of the Freedom of Information Act 2000

Contents

Foreword

Introduction

(i) The Code of Practice ("the Code") which follows fulfils the duty of the Lord Chancellor set out in section 46 of the Freedom of Information Act 2000[1] (the Act). This foreword provides background but does not form part of the Code itself.

(ii) The Code is in two parts. In Part 1, the Code provides guidance to all relevant 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. This applies not only to public authorities but also to other bodies that are subject to the Public Records Act 1958 or the Public Records[2] Act (Northern Ireland) 1923. Collectively they are called relevant authorities.

(iii) The Code also describes, in Part 2, the procedure to be followed for timely and effective review and transfer of public records to The National Archives[3] or to a place 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) 1923.[4]

Importance of records management

(iv) 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 Environmental Information Regulations 2004 (the EIR).

(v) 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:

---

[1] The Act can be seen at http://www.opsi.gov.uk/acts/acts2000/ukpga_20000036_en_1.

[2]Public records are the records of bodies that are subject to the Public Records Act 1958 or the Public Records Act (Northern Ireland) 1923. 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.

[3]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.

[4]The Public Records legislation 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.

- It supports an 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 and its actions;
- It enables protection of the rights and interests of an 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;
- It provides institutional memory.

(vi) 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 service;
- Financial or legal loss if information required as evidence is not available or cannot be relied upon;
- 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.

(vii) The Code is a supplement to the provisions in the Act and its adoption will help authorities comply with their duties under the Act. Consequently, all relevant authorities are strongly encouraged to pay heed to the guidance in the Code. The Code is complemented by the Code of Practice under section 45 of the Act and the Code of Practice under Regulation 16 of the EIR.

(viii) 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.

Role of the Information Commissioner

(ix) The Information Commissioner has a duty under section 47 of the Act to promote the following of good practice by public authorities and in particular to promote observance of the requirements of the Act and the provisions of this Code of Practice. In order to carry out that duty specifically in relation to the Code, the Act confers a number of powers on the Commissioner.

Practice recommendations

(x) 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, the Commissioner 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 the Commissioner's opinion, be taken to promote conformity with the Code. A practice recommendation cannot be directly enforced by the Information Commissioner. However, a failure to comply with a practice recommendation may lead to a failure to comply with the Act or could lead to an adverse comment in a report to Parliament by the Information Commissioner.

Information Notices

(xi) If the Information Commissioner reasonably requires any information in order to determine whether the practice of an authority conforms with that recommended in the 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.

Enforcement of information notices

(xii) 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 Acts

(xiii) 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 bodies subject to that Act in respect of the records they create or hold. It also requires the Chief Executive of The National Archives[5] to supervise the discharge of those duties.

(xiv) 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.

---

[5] 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.

(xv) 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 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 and the Sensitivity Review Group in Northern Ireland

(xvi) The Advisory Council on National Records and Archives[6] (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.[7] The Lord Chancellor, having received the advice of his Advisory Council, 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.[8]

(xvii) 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 for the Lord Chancellor to issue to authorities.

(xviii) 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.

---

[6]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.

[7]In this context, the term 'public records' applies only to the records of bodies that are subject to the Public Records Act 1958.

[8]The term 'historical record' is defined at section 62 of the Act.

CODE OF PRACTICE

(Freedom of Information Act 2000, section 46)
Guidance to relevant authorities on
(1) The management of their records and
(2) The review and transfer of public records

The Lord Chancellor, having consulted 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 16 July 2009 pursuant to section 46(6) of the Freedom of Information Act 2000.

Introduction

1 Aims of the Code

1.1 The aims of the Code are:

- To set out the practices which relevant authorities[9] should follow in relation to the creation, keeping, management and destruction of their records (Part 1 of the Code); and

- To describe the arrangements which bodies responsible for public records[10] 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).

1.2. 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.

1.3 Part 2 provides a framework for the review and transfer of public records that have been selected for permanent preservation at The National Archives[11], 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[12] that apply and indicate for how long they should apply.

---

[9]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.

[10]Public records are the records of bodies that are subject to the Public Records 1958 or the Public Records Act (Northern Ireland) 1923. 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]In the Environmental Information Regulations 2004 (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.

2 Scope of the Code

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 files series and digital 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.

3 Interpretation

For the purposes of this Code, 'records' are defined as in the relevant British Standard[13], 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 specific terms which are not defined in the Act 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 the Act.

4 Supplementary guidance

More detailed guidance on both parts of the Code has been published separately. Standards and guidance which support the objectives of this Code most directly are listed at Annex B.

[13]BS ISO 15489-1:2001 Information and documentation – Records management – Part 1: General.

Part 1: Records Management

5 Summary of recommended good practice in records management

5.1 Good practice in records management is made up of a number of key elements. The following list summarises the good practice recommended in Part 1 of the Code. Guidance on each element is given in sections 6-14 of this Part.

a) Authorities should have in place organisational arrangements that support records management (see section 6);
b) 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 section 7);
c) Authorities should ensure they keep the records they will need for business, regulatory, legal and accountability purposes (see section 8);
d) Authorities should keep their records in systems that enable records to be stored and retrieved as necessary (see section 9);
e) 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 section 10);
f) Authorities should ensure that records are stored securely and that access to them is controlled (see section 11);
g) 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 section 12);
h) 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 section 13);
i) Authorities should monitor compliance with the Code and assess the overall effectiveness of the programme (see section 14).

6 Organisational arrangements to support records management

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

6.1 These arrangements should include:

a) 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;
b) 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;

c) 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, 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;

d) 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;

e) 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;

f) 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;

g) 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 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;

h) An agreed programme for managing records in accordance with this part of the Code;

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

7 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.

7.1 The policy should be endorsed by senior management, for example at board level, and should be readily available to staff at all levels.

7.2 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.

7.3 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.

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

8 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

8.1 Authorities should consider what records they are likely to need about 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 Charity Commission is required by its legislation to keep an accurate and up-to-date register of charities. This factor also includes standards applying to the sector or authority or to particular functions such as finance;
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, 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.

8.2 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;
e) Where and how they should be stored, for example in a case file.

8.3 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 demonstrated if required by showing them to:

a) Be authentic, that is, they are what they say they are;
b) Be reliable, that is, they can be trusted as a full and accurate record;
c) Have integrity, that is, they have not been altered since they were created or filed;
d) Be usable, that is, they can be retrieved, read and used.

Ensuring those records are kept

8.4 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.

8.5 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.

8.6 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.

9 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

9.1 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 EIR require them progressively to make environmental information available to the public by electronic means (Regulation 4).

9.2 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, 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.

9.3 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 the Act;
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;
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.

9.4 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

9.5 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.

9.6 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 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.

9.7 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.

10 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

10.1 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 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.

10.2 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.

10.3 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 the Act.

Storing records

10.4 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.

10.5 Authorities should be aware of any specific requirements for records storage that apply to them. For example, the Adoption National Minimum Standards issued by the Department of Health and the Welsh Assembly Government in 2003 require indexes and case files for children to be securely stored to minimise the risk of damage from fire or water.

10.6 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.

10.7 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 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.

10.8 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

10.9 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.

10.10 Records in digital systems 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, reliable and usable for as long as it is required. The strategy should provide 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.

10.11 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.

10.12 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.

10.13 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.

10.14 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

10.15 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.

11 Security and access

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

11.1 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.

11.2 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.

11.3 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.

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

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

12 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.

12.1 For the purpose of this Code, disposal means the decision as to whether the record should be destroyed, transferred to an archives service for permanent preservation or presented,[14] and the putting into effect of that decision.

General principle

12.2 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 5th data protection principle which requires that personal data is kept only for as long as it is needed.

12.3 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 the Act. This may indicate historical value and destruction should be delayed while this is re-assessed.

Making disposal decisions

12.4 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;
- **c)** Have been formally adopted by the authority;
- **d)** Are applied by properly authorised staff;
- **e)** Take account of security and confidentiality needs.

12.5 The policies should take the form of:

---

[14] Presentation is allowed by section 3(6) of the Public Records Act 1958. It transfers ownership of the records to the receiving body and is undertaken by The National Archives in consultation with the authority.

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[15] 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.

12.6 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.

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

12.7 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.

12.8 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

12.9 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.

12.10 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.

---

[15]Some authorities use the term 'retention schedules'. Because 'retention' has a specific meaning in Part 2 of the Code, the term disposal schedules is used throughout the Code.

12.11 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.

12.12 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

12.13 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.

12.14 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 77 of the Act that records were destroyed in order to prevent their disclosure in response to a request for information.

Records for permanent preservation

12.15 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.

12.16 Part 2 of the 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.

13 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.

13.1 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 the Act.

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

13.3 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.

13.4 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.

14 Monitoring and reporting on records and information management

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

14.1 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.

14.2 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 the Act.

14.3 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.

14.4 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.

14.5 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 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

15 Purpose of Part 2

15.1 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 Archives[16], 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.

15.2 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 places of deposit 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.

16 Selection of public records for permanent preservation

16.1 Section 12 of the 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, transferred to an archives service for permanent preservation or presented[17] and the putting into effect of that decision.

16.2 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 12.

17 Retention or transfer of public records

Records subject to the Public Records Act 1958

17.1 Under the Public Records Act 1958, records selected for preservation must be transferred by the time they are 30 years old[18] unless the Lord Chancellor gives authorisation for them to be retained in the department for a further period under section 3(4) of the Public Records Act 1958. Records may be transferred earlier by agreement between the parties involved.

---

[16] See Footnote 11 for an explanation of why this name has been used in the Code

[17] See footnote 14.

[18] The date by which records must be transferred is calculated from the year after the last date on the file. It was the subject of an independent review in 2008 and the Code will be amended to reflect any changes introduced as a consequence.

17.2 Public records may be transferred either to The National Archives or to a place of deposit for public records appointed by the Lord Chancellor[19] under section 4 of that Act. For guidance on which records may be transferred to which archives service, and on the transfer of UK public records relating to Northern Ireland, see Annex B. For the avoidance of doubt, Part 2 of the Code applies to all such transfers.

17.3 Authorities should submit applications to retain records for a further period to The National Archives for review and advice. The Lord Chancellor's Advisory Council will then consider the case in favour of retention for a further 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.

Records subject to the Public Records Act (Northern Ireland) 1923

17.4 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 responsible for Northern Ireland public records that they should be retained.

18 Determining the access status of public records before transfer

The access review

18.1 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:

- **a)** Consider which information must be available to the public on transfer because no exemptions under the Act or the EIR apply;
- **b)** Consider whether the information must be released in the public interest, notwithstanding the application of an exemption under the Act or the EIR;
- **c)** Consider which information must be available to the public at 30 years because relevant exemptions in the Act have ceased to apply; [20]
- **d)** Consider which information should be withheld from public access through the application of an exemption under the Act or the EIR.

18.2 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 being transferred earlier than required.

---

[19] 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 seniority.

[20] At present some exemptions in the Act fall away after 30 years. Their duration was the subject of an independent review in 2008 and the Code will be amended to reflect any changes introduced as a consequence.

Public records to be transferred as open

18.3 If the outcome of the review is that records are to be transferred as open, the transferring department should designate the records as open. There will be no formal review of this designation by The National Archives, places of deposit or the Public Record Office of Northern Ireland.

Public records to be transferred as subject to an exemption - general

18.4 If the outcome of the review is 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:

a) Identifies the information precisely;
b) Cites the relevant exemption(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.

18.5 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.

Public records to be transferred as subject to an exemption - The National Archives

18.6 The schedule described above should be submitted to The National Archives for review and advice prior to transfer. 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

a) 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;
b) 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;
c) 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;

18.7 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.

Public records to be transferred as subject to an exemption - the Public Record Office of Northern Ireland

18.8 The schedule described at paragraph 18.4 should be submitted to the Public Record Office of Northern Ireland for review and advice.

18.9 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. The Sensitivity Review Group may respond as follows:

a) 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;

b) 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.

18.10 If the Sensitivity Review Group 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.

Public records to be transferred as subject to an exemption - places of deposit for public records

18.11 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.

19 Transmission of public records

19.1 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.

20 Access after transfer of public records

Freedom of Information requests after transfer

20.1 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.

Expiry of closure periods

20.2 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).

20.3 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 process outlined at paragraphs 18.6-18.10 will then be applied. In Northern Ireland, Ministerial agreement is required for any further extension of the closure period and referral to the Minister will be an additional stage in the process.

Annex A Glossary

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

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

Place of deposit – an archives office appointed to receive, preserve and provide access to public records that have been selected for preservation but are not to be transferred to The National Archives. The power of appointment has been delegated by the Lord Chancellor to the Chief Executive of The National Archives or an officer of appropriate seniority.

Presentation – an arrangement under the Public Records Act 1958 whereby records that have not been selected for permanent preservation are presented to an appropriate body by The National Archives.

Public records – records that are subject to the Public Records Act 1958 or the Public Records Act (Northern Ireland) 1923. The records of government departments and their executive agencies, some non-departmental public bodies, the courts, the NHS and the armed forces are public records. Local government records are not public records in England and Wales but those in Northern Ireland are.

Records – 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. [21]

Retention – an arrangement under the Public Records Act 1958 whereby authorities are permitted to delay the transfer of specified public records for an agreed period and to retain them until the end of that period.

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.

[21] This definition is taken from BS ISO 15489-1:2001 Information and documentation – Records management – Part 1: General.

Annex B Standards and guidance supporting the Code

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*

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 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 - see

http://www.nationalarchives.gov.uk/services/default.htm?source=services

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:

Central government

In addition to standards and guidance issued by The National Archives referred to above, protected records[22] are subject to data handling guidance issued by the Cabinet Office - see

http://www.cabinetoffice.gov.uk/mediacabinetoffice/csia/assets/dhr/cross_gov080625.pdf

Local government

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

http://www.rms-gb.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

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

[22]The scope of the term 'protected records' is explained within the document.

The National Health Service

The Department of Health has issued a code of practice for the NHS - see

http://www.dh.gov.uk/enPublicationsandstatistics/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/index/professional_information/records_and_information_management.htm

6. Determining whether exemptions apply

Guidance on FOI exemptions has been issued by the Information Commissioner's Office, the regulator of both the Act and the EIR – see

http://www.ico.gov.uk/tools_and_resources/document_library/freedom_of_information.aspx

Guidance has also been issued by the Ministry of Justice – see

http://www.justice.gov.uk/guidance/foi-exemptions-guidance.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

Guidance has also been issued by The National Archives:
Access to Public Records - see

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 - see

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