Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000

Presented to Parliament by the Secretary of State for Digital, Culture, Media and Sport pursuant to section 46(6) of the Freedom of Information Act 2000

This publication is available at www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at GovernmentHelpPoint@nationalarchives.gov.uk

ISBN 978-1-5286-2517-3

CCS0221019740 07/21

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the APS Group on behalf of the Controller of Her Majesty's Stationery Office

Contents

Introduction

Freedom of Information Act 2000, section 46

CODE OF PRACTICE

Guidance to relevant authorities on the keeping, management and destruction of their records

This is a statutory code of practice issued under section 46 of the Freedom of Information Act 2000[1] (the 'FOIA'). The Secretary of State has consulted the Minister for the Cabinet Office, the Information Commissioner and the appropriate Northern Ireland Minister.

The Code of Practice was laid before parliament on 15 July 2021.

The Code falls into three sections:

- the first section introduces the Code and its legal basis;
- the second sets out the principles of good information management practice;
- the third section deals with historical records.

The annexes provide more information on:

- who the Code applies to;
- the status of the code and the obligation to comply with it;
- the role of the Departmental Record Officer and Information Manager;
- the roles of regulatory and other bodies;
- other sources of standards and guidance;
- a glossary of terms.

[1] The Freedom of Information Act can be found at: http://www.legislation.gov.uk/ukpga/2000/36/contents

Part One: Outline of the Code

1.1 Purpose of the Code

1.1.1. This Code of Practice (the 'Code') provides guidance to authorities which helps them to create a framework for keeping, managing and destroying their information, and therefore records. Complying with this Code will help authorities to account for their activities. It will also help them to comply with FOIA, the Environmental Information Regulations (EIR)[2] and other information rights legislation such as the UK General Data Protection Regulation (UK GDPR). It will assist them in complying with the Public Records Act 1958 (PRA) and The Public Records Act (Northern Ireland) 1923 (PRA (NI)) if they apply. It will also help public authorities to fulfil their duty to publish information about their activities and to comply with the Re-use of Public Sector Information Regulations 2015.

1.1.2. The Code does not attempt to provide an exhaustive set of guidelines for every authority that creates or holds information. Authorities should make themselves aware of relevant practice guidance issued by appropriate regulatory bodies, by the Information Commissioner's Office, by The National Archives (TNA), and by the Public Record Office of Northern Ireland (PRONI).

1.1.3. The Code takes a principles-based approach. The three principles of value, integrity and accountability provide a high-level framework for authorities to manage information and maintain a record of their activities. This approach can accommodate the varied procedural and technical environments in which authorities operate by setting out good practice.

1.1.4. The principles apply to information in any format or medium that the authority holds or that another body holds on its behalf. The principles inform good practice in the creation, management and destruction of information, and are applicable to the diverse procedural and technical environments in which authorities operate.

1.1.5. For the purposes of the Code, the term information is used as shorthand for both information and records. Not all information is a record.

1.2 The context of the Code

1.2.1. Authorities create and acquire information in the course of service delivery and policy development. Information may be an asset in the present and may become a resource for future generations.

1.2.2. Information technology has changed how people work and how authorities create and use information. The volume of information is a challenge for authorities so they need to manage it effectively.

[2] The Environmental Information Regulations 2004 can be found at: http://www.legislation.gov.uk/uksi/2004/3391/contents/made

1.2.3. Information can become a liability if it is not properly managed. Authorities should know what information they hold, why they hold it, how sensitive it is, and how it should be managed. They should keep information for as long as they need it and dispose of it when they no longer have a reason to keep it. Authorities can dispose of information by destroying it, transferring it to another body[3] or by transferring it to an archive.

1.2.4. Authorities should manage their information so as to create and maintain a record of their activities which, in turn, provides evidence of their activities. Authorities risk financial, legal and reputational damage if they do not manage their information, and therefore records, properly. Well managed information and records improves efficiency and decision-making.

1.3 The status of the Code

1.3.1. This is a statutory code of practice issued under s.46 of FOIA which provides a framework for managing information and records. Compliance with the Code provides authorities with a high level of confidence that they can comply with the requirements of FOIA.

1.3.2. Authorities should read the Code in conjunction with current legislation governing information and records.[4] Detailed guidance on specific topics is set out in Annex E.

1.3.3. The Code does not replace any professional codes of practice, codes of conduct, professional standards or regulations that impose duties to create and manage information on any authority covered by the Code.[5] Authorities have a duty to understand the regulatory framework in which they operate and to adhere to its requirements in addition to observing the requirements of the Code.

1.3.4. The Information Commissioner (the Commissioner) has a statutory duty to promote good practice and compliance with the Code. The Commissioner may take into account compliance with the Code before issuing a 'practice recommendation' under section 48 FOIA to public authorities whose practice does not comply with the Code.[6]

1.4 Who the Code applies to

1.4.1. The Code applies to 'relevant authorities'.[7] Section 46(7) of FOIA defines relevant authorities as (a) any public authority[8] and (b) any office or body which is not a public authority but whose administrative and departmental records are public records for the purposes of the PRA or, in Northern Ireland, the PRA(NI). This Code refers to them as 'authorities' throughout. Detailed information about who the code applies to is at Annex A.

1.4.2. The standards set out in the Code apply to authorities regardless of how long they have existed for, their size or proximity to central government. For example, a short-term body such as a public inquiry is subject to the Code in the same way as a government department, police forces and law enforcement, the courts, a regulatory body, a local authority or a school.

---

3 Public records can be presented as a gift under section 3(6) PRA. Transfer of ownership must be approved by The National Archives.

4 Detailed information on the status of the Code is at Annex B.

5 For example, Civil Servants must abide by the terms of the Civil Service Code, which states that they must 'keep accurate official records and handle information as openly as possible within the legal framework'.

6 The role and responsibilities of the Information Commissioner are set out at Annex D.

7 See Annex A – Who the Code applies to.

8 As defined by Schedule 1 FOIA

1.4.3. The Code does not apply to bodies subject to the Freedom of Information (Scotland) Act 2002 (FOI(S)A). A Code of Practice issued under s.61 FOI(S) A applies to these bodies. The Code does not apply to bodies subject to the Public Records (Scotland) Act 2011.

Part Two: Managing Information and Records

2.1 The Principles

2.1.1. There are many good reasons to keep information and those reasons may change over time. These include, but are not limited to, the following:

- for accountability and audit;
- to comply with regulatory requirements, including the provisions of FOIA;
- to protect legal and other rights and interests;
- as a historical record.

2.1.2. Authorities should consider opportunities to make use of the information either within the authority or elsewhere, now or in the future.

2.1.3. Authorities must periodically assess the information they hold. They must know why they are keeping it and must also be able to explain why they no longer hold information, by keeping a record of decisions to keep, archive or destroy information. The principles set out below should inform authorities' approach.

Value	The authority must understand, manage and use its information in a way that enables it to understand its value, in order to make effective decisions for the benefit of society. The value of information changes over time. Information will have *immediate* value when first created, satisfying its initial purpose. After this, it may continue to have *operational* value as working information. It may then have *evidentiary* value for audit, accountability or regulatory purposes. Information may have *potential* value if it can be used to create new knowledge, improve services or generate income. Finally, it may have *permanent* historic value. Historic value is the contribution of the information to the long-term memory of society, as well as the corporate memory of organisations. It helps inform and protect the individual rights of citizens and groups within society and shapes our sense of identity. Authorities must manage their information in such a way that they can assess its current and future value. They must keep information as long as they can show it has value and dispose of it when it no longer has value. Authorities must be able to explain why they no longer hold information.
Integrity	The authority and all its stakeholders must be able to rely upon and trust the information that it holds.
Accountability	The authority's information management must enable it to provide a clear and accurate account of its activity in accordance with its legal and other obligations.

2.2 Putting the principles into practice

2.2.1. To put these principles into practice, authorities must have in place appropriate governance, organisational capability and technical measures to ensure that they manage information in accordance with the Code.

2.2.2. The governance measures should include:

- clear responsibility for information and records management at an appropriately senior level;
- written rules on what to keep and when to destroy information to ensure that the authority maintains a record of its activities;[9]
- regular evaluation of the effectiveness of policies and rules and the extent to which they are being followed;
- written rules on access to the authority's information including personal information and other sensitive information;
- a governance framework that takes account of information risks such as inappropriate hoarding and loss of information which provides for the involvement of senior management.

2.2.3. Authorities should consider the implication for information management of restructuring and other organisational changes, sponsorship of other bodies, and the procurement of services from contractors.

2.2.4. The organisational capability of the authority should include:

- an information management function with a designated manager with day-to-day responsibility for information management and responsibility for decisions on access to the authority's information;
- a designated manager of sufficient seniority to ensure that the authority discharges its responsibilities under the Code, and that the authority is consistent in its approach to managing information, risk and access;
- adequate resources, to comply with the Code and any other statutory obligations;[10]
- suitably trained staff with the appropriate information management skills.

Authorities should:

- make sure that the designated manager has the resources to monitor compliance with the Code and other relevant statutory obligations;
- make sure that the designated manager is part of the authority's governance structure, has oversight of information risk and the ability to raise concerns at the most senior level;
- make sure that those taking decisions to destroy information on its behalf are authorised to do so by the authority.

Authorities should engage with the designated manager to make sure that their information is managed in conformity with the Code:

- before major organisational changes;

[9] Usually in the form of a retention schedule, a destruction schedule and/or a disposal schedule.

[10] Including but not limited to PRA, the PRA(NI), the UK GDPR and the Re-use of Public Sector Information Regulations 2015.

- before taking decisions about the design, development and procurement of IT systems and applications;
- before the publication scheme required by section 19 (3) FOIA is submitted to the ICO for approval;
- before the use and re-use of information, including copyright and Crown copyright material;[11]
- before entering cooperative arrangements with other authorities, before sponsoring other bodies, acquiring systems originating in another body and before procuring services from contractors.

The role of the designated manager will depend on the size and functions of the authority. In Government Departments the designated manager is the Departmental Record Officer (DRO) and in Northern Ireland the Information Manager (IM). Detailed information on these roles is provided at Annex C.

2.2.5 The technical capability of the authority should include:

- tools and systems to manage and organise information throughout its life;
- tools and systems to locate and use information, consistently applied across the authority;[12]
- back-up systems to recover from system failures and major disasters;
- systems to ensure that the destruction of information is carried out in line with its sensitivity and is permanent.

2.3 Keeping, finding and using information

2.3.1. Authorities must define how long to keep information and dispose of it when it is no longer needed. Authorities can dispose of information by destroying it, transferring it to another body, or by transferring it to an archive. Authorities must be able to explain why information is no longer held either by reference to a record of its destruction or by reference to the authority's policy.[13]

2.3.2. Authorities should keep information for as long as it has value; for example if:

- the authority needs it for reference or accountability purposes, to comply with regulatory requirements or to protect legal and other rights and interests. This is particularly important if the authority has a duty of care towards vulnerable groups;
- the authority has selected it for permanent preservation under either the PRA or PRA(NI), equivalent local government legislation[14] or in accordance with the authority's publication scheme published under FOIA section 19(3);
- the authority has identified ways to make use of the information either within the authority or elsewhere, now or in the future – for example, to improve services or generate income;

[11] See Annex E – Other sources of standards and guidance

[12] The authority must be able to locate and retrieve information within the statutory timescale or explain why it is not held, why it cannot be disclosed or why it cannot be located and retrieved within the appropriate limit.

[13] Section 77 FOIA has provision for authorities to be charged with destroying records to prevent disclosure, and data protection legislation contains further provisions on transparency of retention, so it is important that any disposition decision is properly documented.

[14] Local Government (Records) Act 1962; Local Government Act 1972 (ss224-8); Local Government (Wales) Act 1994.

- the authority has assessed that it can be used for another purpose, such as statistical, scientific, medical or historical research (subject to Data Protection legislation safeguards);
- it contains or relates to information requested under FOIA or the EIRs. This may indicate long-term value;
- there are exceptional circumstances such as a moratorium on destruction of information, a police investigation, a public inquiry, or legal action.[15]

2.3.3. Authorities should be able to collect and keep technical and contextual information about their records in order to understand their value. 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.

2.3.4. Authorities should be able to transfer technical and contextual information to a successor body and, if selected for permanent preservation, to an archive.

2.3.5. Authorities should endeavour to hold information in an appropriate environment. Physical and digital information should be managed in a manner appropriate to the medium in order to preserve its value.

2.3.6. Authorities should take action to conserve physical records if there are signs of damage according to best practice. Digital information should be subject to the appropriate active digital continuity.[16]

2.3.7. Authorities should make reasonable efforts to recover or preserve physical records and digital information that is found to be damaged or unusable, including their technical and contextual information, keeping a record of any action taken.

2.3.8. Authorities should make reasonable efforts to recover contextual information for 'orphaned information' which they judge to have value, keeping a record of any action taken.

2.3.9. Authorities should have appropriate tools to identify, locate and retrieve information when required. An effective search capability should be maintained alongside controls to protect sensitive information.[17]

2.4 Authorities must be able to trust their information. To do this, they must:

- be able to establish when information was created and who it was created by;
- have in place policies and processes for information security that comply with relevant legislation, guidance and codes of practice;
- apply access and permission controls throughout the life of the information to prevent unauthorised or unlawful access;
- have appropriate technical and organisational measures to prevent accidental loss, destruction or damage, to their information.

---

[15] For example, where an Inquiry leads to criminal proceedings.

[16] See Annex E – Other sources of standards and guidance

[17] In response to a complaint, the Information Commissioner will consider the scope, quality, thoroughness and results of the searches undertaken, unless it is clear from the authority's policies that the information will have been destroyed or transferred to another organisation.

2.5 The UK GDPR requires authorities to destroy personal data when it is no longer needed for the purpose for which they collected it (Article 5 1(e)); however authorities are permitted to keep personal data for scientific or historical research purposes, statistical purposes, or for archiving purposes in the public interest. Authorities should handle personal data in their records in accordance with guidance issued by the ICO and TNA where it relates to public records.

2.6 Disposition

2.6.1. Authorities must decide how to dispose of information that no longer has value. Authorities can dispose of information by destroying it, transferring it to another body[18] or by transferring it to an archive.

2.6.2. Authorities must take disposition decisions in line with their policy and the security classification of the information. Disposition decisions must be recorded. Those taking disposition decisions must be properly authorised to do so.

2.7 Destroying information

2.7.1. Authorities should destroy or delete information that no longer has value. Destruction decisions should take into account the current value of the information and any potential future value. Destroying information is essential to maintaining an effective information management capability, and means that authorities avoid the unnecessary financial burden of searching, maintaining and storing information that is no longer needed.

2.7.2. Authorities should make destruction decisions in accordance with an up-to-date policy, using a method or process that is applied consistently and that has been approved by the authority. Destruction policies should be sufficiently flexible to adapt to the requirements of extraordinary circumstances such as litigation or a public inquiry.

2.7.3. Authorities should ensure that staff are aware that there is no need to keep ephemeral material, and this may be destroyed on a routine basis. For example, by deleting trivial emails and messages after they have been read and discouraging staff from keeping multiple or personal copies of documents.

2.7.4. Authorities should have a destruction schedule to enable them to identify and destroy information that is not needed at the appropriate time, as determined by their policy.

2.7.5. Authorities may authorise staff or contractors to destroy information but the authority will remain responsible for decisions to destroy information and for ensuring that they are carried out.

2.7.6. Authorities should be able to explain why they no longer hold information, either by reference to a record of its destruction or by reference to the authority's policy. If destruction is carried out by a contractor, the authority should obtain proof, for example, a certificate of destruction.

2.7.7. Authorities should destroy information by a method appropriate to the sensitivity or security classification of the information. Efforts to destroy information should also be proportionate to its sensitivity and security classification.

[18] Public records can be presented as a gift under section 3(6) PRA. Transfer of ownership must be approved by The National Archives.

2.7.8. Destruction/deletion should be permanent, which means all known copies and versions of the information, including back-ups, have been destroyed or deleted and cannot be recovered by processes within the control and capability of the authority.

2.8 Responsibilities where information is shared

2.8.1. Where the authority works jointly with another authority, body or contractor, a lead or commissioning authority should be agreed which will remain responsible for ensuring that information is managed in accordance with the Code throughout its life.[19]

2.8.2. The authority and its partner authorities, bodies or contractors should set out their responsibilities in an information sharing agreement.[20] This includes where information in separate authorities' systems is integrated by technical means.

The agreement should specify:

- the obligation to record decisions, particularly in relation to the transfer or destruction of information;
- obligations under copyright, data protection legislation and FOIA;
- record management controls and any special requirements for the security and handling of personal information;
- the ownership of any copyright.[21]

2.8.3. Authorities should ensure that information sharing arrangements enable them to comply with the requirements of the PRA or the PRA(NI) where at least one authority is subject to the legislation.

2.9 Monitoring and assurance

2.9.1. Authorities must assess their policies and procedures against the requirements of the Code at regular intervals and update them if necessary. Risks associated with non-compliance should be included in the authority's framework for managing risk.

2.9.2. Authorities should engage with information management assurance and audit regimes in their field. Measures may include self-assessment tools, external assessments, peer reviews and accreditation schemes.

2.9.3. Under FOIA, the Information Commissioner may, with the consent of any public authority, assess whether that authority is following good practice.

---

[19] Unless alternative arrangements have been formally agreed, for example a data controller to data controller share. Contractors must support compliance with all aspects of FOIA.

[20] This is particularly important where public money is being used to procure services from those not subject to FOIA.

[21] Crown copyright cannot be assigned or delegated as part of an information sharing agreement without the authority of the Keeper of Public Records.

Part Three: Historical records

3.1 Introduction

3.1.1. Some authorities, such as government departments, the courts and other national institutions are subject to the PRA. Authorities subject to the PRA have a statutory duty to select records of historic value for permanent preservation in TNA or a Place of Deposit. Northern Ireland authorities, such as government departments, local authorities and institutions are subject to the PRA(NI). Authorities subject to the PRA(NI) select records of historic value in collaboration with the PRONI.

3.1.2. For authorities that are not subject to the PRA or PRA(NI) Part 3 does not form part of the Code, however these authorities may wish to operate with regard to Part 3 where it is helpful.

3.1.3. Authorities not subject to the PRA or PRA(NI) should seek to identify records that have permanent or historical value and arrange to transfer them to either:

- an accredited archive service[22] or;
- a storage provider compliant with the relevant British Standards[23] and able to provide the necessary access.

If the authority intends to preserve the records itself, it should endeavour to comply with the relevant British Standards.

3.2 Transfer of public records

3.2.1. Authorities subject to the PRA must make and implement decisions on the management of public records by the statutory deadline,[24] no later than 20 years after their creation. Authorities can choose to retain information for business purposes or dispose of information by transferring it to another body[25], transferring it to an archive or by destroying it.

To take decisions, authorities must:

- understand the content, context and sensitivity of the records that they hold;
- review records throughout their life;
- have a documented process for selecting records for retention, transfer or destruction.

[22] Accredited archive services can be found at https://www.nationalarchives.gov.uk/archives-sector/archive-service-accreditation/accredited-archive-services/

[23] See Annex E – Other sources of standards and guidance for BS EN 16893:2018 and BS 4971:2017.

[24] s.3(4) of PRA, as affected by the transitional arrangements set out in article 2.2 of The Public Records (Transfer to the Public Record Office) (Transitional and Saving Provisions) Order 2012

[25] Public records can be presented as a gift under section *3(6) PRA. Transfer of ownership must be approved by The National Archives.*

3.2.2. Authorities in Northern Ireland have duties in respect of the records they create and manage under the PRA(NI) and the Disposal of Documents Orders (S.R. & O 1925 No 167 and No 170) which requires that records must be transferred to and preserved by the PRONI. These bodies must:

- have an agreed Retention and Disposal schedule which identifies what information is held by the authority, and sets out retention periods and final disposition actions;
- review the information throughout its life in order to implement decisions on disposition.

3.2.3. Authorities may transfer records selected for permanent preservation earlier if they no longer need them for business purposes and the receiving records authority agrees.

3.2.4. Authorities must transfer records selected for permanent preservation to:

- TNA, or
- A Place of Deposit appointed to hold them under section 4(3) of the PRA, or
- The PRONI under section 3(8) of the PRA,[26] or
- The PRONI under the PRA(NI), or
- A Place of Deposit approved by the Keeper of Public Records under s. 4(1) PRA.

3.2.5. Authorities must transfer records in line with guidance issued by the Keeper of Public Records and the Deputy Keeper (NI). Authorities must ensure that transfers are properly documented.

3.2.6. TNA and PRONI have issued guidance on the appraisal, selection, sensitivity review, preparation and transfer of records. Links to this guidance are in Annex E. This section indicates some broad principles.

3.2.7. Authorities must identify appropriate exemptions under FOIA for information that remains sensitive. They must apply to the Secretary of State for Digital, Culture, Media and Sport for approval to retain records or extracts of records beyond 20 years, or transfer records to an archive with FOIA exemptions applied. In Northern Ireland, they must apply to the appropriate Minister for Public Records, for approval to retain records beyond 20 years, or transfer records to an archive with FOIA exemptions applied.

3.2.8. Authorities should consult with other authorities that are likely to be affected by their access decisions. This is particularly important for records being transferred before they have reached 20 years.

3.2.9. Authorities must submit a schedule for review to TNA, PRONI or a Place of Deposit where it proposes to transfer records subject to FOI exemptions. A schedule must be submitted, that:

- identifies the information clearly;
- cites the relevant exemption(s) that they consider to be engaged by the record;
- explains why the information should not be released;

[26] s.3(8) PRA also permits transfer to the National Records of Scotland.

- identifies a date at which release would either be appropriate or the case for release should be reconsidered.

3.2.10. The Advisory Council on National Records and Archives (ACNRA), chaired by the Master of the Rolls, advises the Secretary of State on applications to retain records and the application of qualified FOIA exemptions as applied at the point that those records are transferred to TNA. In Northern Ireland, the Sensitivity Review Group (SRG) advises the Deputy Keeper of Public Records on applications, who advises the appropriate Minister responsible for NI public records.

3.3 Access to historical information transferred under FOI exemptions

3.3.1. TNA, the Place of Deposit or PRONI should notify the authority where information is due to be released after being transferred with exemptions. The authority is responsible for reviewing the information for remaining sensitivities and for making any further applications for withholding under FOIA exemptions.[27]

3.3.2. Authorities subject to the PRA must obtain written consent from TNA before presenting records as a gift[28] to a museum or research body.

3.3.3. Where exempt information is transferred to the National Records of Scotland, requests should be dealt with in accordance with UK access legislation.[29]

3.4 Retention of public records

3.4.1. Authorities must consider the nature of the records that need to be retained in order to decide the most appropriate course of action. The authority must:

1. establish whether the records are covered by a standard authorisation, for example the Security and Intelligence Instrument,[30] which permits retention under s.3(4) PRA, or;
2. apply to the Secretary of State when it needs to retain its public records for longer than 20 years.[31] The ACNRA will make recommendations to the Secretary of State for Digital, Culture, Media and Sport who is responsible for deciding the application.

3.4.2. In Northern Ireland, to retain records for longer than 20 years, the principal officer of the department or a judge (for court records) may certify to the Minister responsible for NI public records that they should be retained.

3.4.3. Retaining records without approval breaches the PRA and PRA(NI) and may also involve the unlawful processing of personal data.

---

27 https://www.nationalarchives.gov.uk/documents/information-management/procedures-for-closure-on-transfer.pdf

28 Under s.3(6) PRA

29 Freedom of Information (Scotland) Act 2002 and Environmental Information (Scotland) Regulations 2004

30 https://www.gov.uk/government/publications/signed-instrument-for-the-retention-of-public-records

31 Applications are made through TNA or a Place of Deposit.

3.5 Obligations where departments sponsor other bodies

3.5.1. The authority should support any authority that it sponsors to meet its information and records management responsibilities in accordance with the Code.

3.5.2. Before any authority closes, the sponsoring authority should make sure that plans are in place for the management of its information so that access decisions can continue to be made.

3.5.3. Authorities should ensure that any short-term body that it sponsors (such as an inquiry) maintains a record of its activity and meets its responsibilities in accordance with the Code.

3.5.4. Authorities that are short-term bodies create public records. They should:

- create and develop their information management plans in discussion with their sponsoring body from the outset;
- engage directly with TNA or the PRONI.

Annex A – Who the Code applies to

s.46 (1) FOIA states that the code applies to 'relevant authorities'. s.46(7) defines relevant authorities as:

a. any public authority, and

b. any office or body which is not a public authority but whose administrative and departmental records are public records for the purposes of the Public Records Act 1958 or the Public Records Act (Northern Ireland) 1923.

A 'public authority' is any body listed in Schedule 1 FOIA. This means that the Code applies to any body in England, Wales and Northern Ireland that is subject to FOIA. It also applies to UK-wide bodies based in Scotland that are subject to FOIA.

The Code also applies to bodies subject to the PRA[32] and PRA(NI). These are listed in Schedule 1 part I and II PRA and s.1(2) PRA(NI). There is much overlap, but the term 'relevant authorities' covers, for example, bodies such as courts and tribunals that are not subject to FOIA.

The Code does not apply to bodies subject to the Freedom of Information (Scotland) Act 2002 (FOI(S)A). A Code of Practice issued under s.61 FOI(S)A applies to these bodies.

[32] Welsh public records are defined, and Welsh public record bodies listed, in s148 of the Government of Wales Act 2006. The category of Welsh public records is currently latent, until such time as the Welsh Assembly transfers responsibility for Welsh public records to Wales under s147 of the 2006 Act. At the time of publication, Welsh public records are managed as though they are public records under the 1958 Act. All bodies listed in s148 of the Government of Wales Act should consider themselves relevant authorities and therefore subject to the Code.

Annex B – Status of the Code and the obligation to comply

The Code is issued under section 46 FOIA. It fulfils the duty of the Secretary of State for Digital, Culture, Media and Sport to provide guidance to relevant authorities on the practice which, in the opinion of the Secretary of State, it would 'be desirable for them to follow in connection with the keeping, management and destruction of their records.' (s.46(1))

The Code should be read alongside legislation governing information and records such as the PRA and the PRA(NI). These impose duties on government departments and other public record bodies to select records for permanent preservation and preserve them under the guidance of the Keeper of Public Records. Bodies subject to the PRA should read the Code alongside guidance published by TNA. Bodies subject to the PRA(NI) should read the Code alongside guidance published by the PRONI.

The Code complements the Code of Practice issued under s.45 FOIA and the Code of Practice issued under reg.16 EIR.

Compliance with the Code means that Authorities are more likely to comply with other legislation on the keeping, management and destruction of their records, including the Freedom of Information Act 2000, Public Records Act 1958 and the Data Protection Act 2018,[33] and other statutory obligations such as the right to inspect documents under the Local Government Act 1972.[34]

The Information Commissioner has a statutory duty to promote good practice and to promote compliance with the Code. The Commissioner may issue a 'practice recommendation' under section 48 FOIA to public authorities whose practice does not conform to the Code.

[33] http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

[34] http://www.legislation.gov.uk/ukpga/1972/70/part/VA

Annex C – The Departmental Record Officer and Information Manager

The role of the designated manager will vary according to the size and functions of the authority. In Government Departments this is the Departmental Record Officer (DRO) and in Northern Ireland the Information Manager (IM).

The role of the DRO/IM:

Oversight

The DRO/IM:

- oversees the appraisal, selection, review, retention and destruction of records and arrangements for access to the organisation's records;
- makes sure the authority keeps to the principles of the Code so that they know why they keep different categories of information and destroy information when they no longer need it;
- authorises the use of absolute exemptions and consulting the ACNRA about the use of qualified exemptions, in respect of records or parts of records when they are due for transfer;
- applies to the ACNRA[35] when seeking authority to retain records;
- provides schedules of the records that they propose to transfer subject to FOIA exemptions, and of records or parts of records which they propose to retain.

In Northern Ireland, the Information Manager has responsibility for:

- the retention and disposition of public records;
- ensuring that public records transferring to the PRONI are accompanied by access decisions;
- applications to the SRG in order to apply exemptions to certain records or parts of records in line with published guidance.

Monitoring and assessment

The DRO/IM:

- monitors compliance with the Code, reporting to the senior leadership of the authority;
- assesses the authority's policies and procedures against the requirements of the Code at regular intervals and updates them if necessary;
- assesses performance against the requirements of the Code and recommends measures to improve performance if necessary.

[35] Applications are made via The National Archives or a Place of Deposit.

Retaining and destroying information

The DRO/IM:

- makes sure the authority has policies on retaining and destroying information, can decide what to keep and what to destroy, and can explain its decisions;
- makes sure that the authority destroys information consistently and in line with its policies;
- makes sure that the authority destroys information using a method appropriate to the sensitivity or security classification of the information and that it records destruction and, if destruction is carried out by a contractor that it is certified;
- ensures that the procedure destroys all known copies and versions including back-ups and they cannot be recovered, taking into account that the efforts should be proportionate to the sensitivity and security classification of the information.

Permanent preservation

The DRO/IM:

- oversees the appraisal and selection of records for permanent preservation and transfer to an accredited archive;
- oversees the review of records selected for transfer to identify sensitivities in the records which have a bearing on public access to the records;
- applies to retain records or parts of records selected for permanent preservation;
- applies FOI exemptions to records or parts of records selected for permanent preservation;
- supplies TNA / PRONI with data on information and records on request.

Annex D – The roles of regulatory and other bodies

The Keeper of Public Records and The National Archives

Under the PRA, the Chief Executive and Keeper of Public Records at TNA is responsible for the preservation and safekeeping of historic public records.[36]

TNA will issue guidance to bodies subject to the PRA on the management of their information. This guidance covers the entire life span of that information to ensure that they can transfer public records that have reached 20 years old.

TNA will collect information and carry out assessments of bodies to ensure that information is managed in line with legislation and the provisions of this Code.

TNA will issue guidance, training and develop tools to help authorities manage their information so as to compile an official record of their activities for the future.

TNA provides Archive Accreditation which enables archives to function as Places of Deposit under s.4 PRA. As Places of Deposit, these archives are able to accept public records, as well as other records of authorities not covered by PRA or PRA(NI) for example, specialist technical records, records of local interest and police force records.

The Secretary of State and the Advisory Council on National Records and Archives

ACNRA is an advisory Non Departmental Public Body (NDPB) appointed under s.1(2) PRA. It is chaired by the Master of the Rolls.

It advises The Secretary of State for Digital, Culture, Media and Sport (the Secretary of State) when a body applies to retain records under s.3(4) PRA. The Secretary of State approves retention for a specified period by signing a Retention Instrument.

ACNRA will advise the Secretary of State when a body[37] has made an application to retain records that are 20 years old, which would otherwise be transferred to TNA.

The ACNRA will advise bodies on the public interest in relation to qualified FOIA exemptions in so far as they apply to records transferring to TNA. The ACNRA also advises departmental ministers on the access status of their records, when those records are at the point of transfer to TNA, and again when the access status is due for review.

The ACNRA will advise bodies on the public interest in relation to engaged qualified exemptions (regardless of whether absolute exemptions, the use of which is for the authority to determine, are also to be applied) as defined under FOIA, when a record is at the point of transfer to TNA. ACNRA will respond to bodies (in whole or in part as appropriate) if one of the following ways:

---

[36] Public records are the records created by the bodies set out at the First Schedule (Part II) of the PRA and Chapter 20 s1 (2) of the PRA(NI).

[37] NHS organisations are generally independent statutory bodies for data protection and FOI purposes.

a. accepting that the information may be withheld for longer than 20 years and earmarking the records for release or re-review at the date identified by the authority;

b. accepting that the information may be withheld for longer than 20 years but asking the authority to reconsider the proposed date for release or re-review;

c. questioning the basis on which it is considered that the information may be withheld for longer than 20 years, asking the authority to reconsider the case, and, exceptionally, to request sight of the record;

d. advising departmental ministers against the application of FOI exemptions contrary to the recommendations of that department's officials.

If ACNRA accepts that the information should be withheld, the records will be transferred subject to exemptions (in whole or in part as appropriate) with the relevant period applied.

Departmental officials must consult their Minister if ACNRA and the department are unable to agree. The ACNRA should approve the terms in which the position is put to the Minister. The minister's decision will be final. If the Minister chooses not to take advice and records or part of records continue to be withheld, this outcome will be stated in the ACNRA's annual report to the Secretary of State.

The Public Record Office of Northern Ireland

The PRONI provides information management guidance to support public record-transferring bodies to meet their responsibilities in accordance with the PRA(NI), the Data Protection Act 2018 and FOIA. Alongside the Code, bodies in Northern Ireland should conform to guidance published by the PRONI which gives practical advice on information management as it relates specifically to public record keeping in Northern Ireland.

The Sensitivity Review Group Northern Ireland

The Northern Ireland SRG is made up of representatives of Northern Ireland departments and provides advice on the release of public records. The PRONI 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. The Deputy Keeper will provide advice to the Minister responsible for NI public records.

The Information Commissioner

S.47 FOIA obliges the Information Commissioner to promote good practice by public authorities and in particular to promote observance of the requirements of the Act and the provisions of this Code. The ICO may, with the consent of an authority, assess whether that authority is following good practice. The FOIA confers a number of powers on the ICO to effect these responsibilities.

The ICO may issue a practice recommendation under s.48 FOIA if it appears that a public authority's practices do not conform to this Code. The ICO must consult with the Keeper of Public Records before issuing a practice recommendation in respect of records which are public records under the PRA or with the Deputy Keeper of the Records in respect of records which are public records for the purpose of the PRA(NI).

A practice recommendation will be in writing and will specify which provisions of the Code have not been met and the steps that should be taken to comply with the Code. The ICO cannot enforce a practice recommendation but failure to comply may result in failure to comply with FOIA or EIR. The ICO may include an adverse comment in a report to Parliament.

Under s.51 FOIA, the ICO may serve a written information notice on a public authority in order to obtain information to determine whether the practice of an authority conforms to the Code. Public authorities may appeal against an information notice (s.57 FOIA).

Under s.54 FOIA, the ICO may seek an order for contempt of court should a public authority fail to comply with an information notice.

Annex E – Other sources of standards and guidance

A. Guidance for public record bodies

The Keeper of Public Records publishes guidance and resources on the management of recorded information in all formats, covering its entire life. Other relevant authorities may adopt the principles and practice set out in this guidance as a model for their own practice.

http://nationalarchives.gov.uk/information-management/manage-information/planning/departmental-record-officer/role-departmental-record-officer

https://www.nationalarchives.gov.uk/documents/information-management/retention.pdf

https://www.nationalarchives.gov.uk/information-management/re-using-public-sector-information/uk-government-licensing-framework/crown-copyright/

PRONI publishes guidance and standards for Northern Ireland public record bodies. This can be found at https://www.nidirect.gov.uk/articles/records-management-public-bodies

Disposal of Documents Order 167 (Northern Ireland) 1925.

B. Guidance for local government and NHS bodies

Local government: https://standards.esd.org.uk/

NHS bodies: https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections

C. Guidance on access to information and exemptions

Guidance on both FOI exemptions and EIR exceptions is published by the Information Commissioner's Office at:

https://ico.org.uk/for-organisations/guidance-index/freedom-of-information-and-environmental-information-regulations/

Guidance on Publications Schemes is published by the ICO at: https://ico.org.uk/for-organisations/guide-to-freedom-of-information/publication-scheme/

Guidance on access to public records is published by TNA at: http://nationalarchives.gov.uk/information-management/manage-information/selection-and-transfer/sensitivity-reviews-on-selected-records/access-to-public-records/

Redaction: guidelines for the editing of exempt information from paper and electronic documents prior to release: https://www.nationalarchives.gov.uk/documents/information-management/redaction_toolkit.pdf

Procedures for closure on transfer: https://www.nationalarchives.gov.uk/documents/information-management/procedures-for-closure-on-transfer.pdf

D. Data Protection Guidance

The ICO publishes guidance for organisations on the UK GDPR and DPA at https://ico.org.uk/for-organisations/guide-to-data-protection/

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

TNA has published a Guide to Archiving Personal Data at:

http://www.nationalarchives.gov.uk/documents/information-management/guide-to-archiving-personal-data.pdf

E. Digital continuity and preservation

TNA publishes guidance on digital continuity at: http://www.nationalarchives.gov.uk/documents/information-management/managing-digital-continuity.pdf

A handbook published by the Digital Preservation Coalition can be found at: https://www.dpconline.org/handbook

F. Government guidance

https://www.gov.uk/government/publications/managing-public-money

http://gov.wales/managing-welsh-public-money

https://www.finance-ni.gov.uk/articles/managing-public-money-ni-mpmni

https://www.crowncommercial.gov.uk/agreements/rm3781?gclid=EAIaIQobChMIs5eD49aF5gIVDLDtCh2GfgeaEAAYASAAEgJwQvD_BwE

https://www.gov.uk/government/publications/government-security-classifications

G. British Standards Institute (BSI)

The BSI has issues a number of Standards related to information management:

BS ISO 15489-1:2016 *Information and documentation - Records management - Part 1: Concepts and Principles*

BS EN ISO/IEC 27001:2017 *Information technology. Security techniques. Information security management systems. Requirements*

BS EN ISO/IEC 27002:2017 *Information technology. Security techniques. Code of practice for information security controls*

BS 10008-1:2020 *Evidential weight and legal admissibility of electronically stored information (ESI) – Specification*

BS ISO 16175-1:2020 *Information and documentation. Processes and functional requirements for software for managing records. Functional requirements and associated guidance for any applications that manage digital records*

ISO 16175-2:2020 *Information and documentation - Principles and functional requirements for records in electronic office environments. Part 2: Guidelines and functional requirements for digital records management systems*

BS EN 15713:2009 *Secure destruction of confidential material – Code of practice* [under review]

BS 4783-8:1994. *Storage, transportation and maintenance of media for use in data processing and information storage. Recommendations for 4 mm and 8 mm helical scan tape cartridges.*

BS 4971:2017 *Conservation and care of archive and library collections*

EN 16893:2018 *Conservation of Cultural Heritage – Specifications for location, construction and modification of buildings or rooms intended for the storage or use of heritage collection*

Annex F – Glossary

The glossary is provided to help explain the terms and concepts used in the Code, but does not form part of the Code itself.

Appraisal – the process of distinguishing information of continuing value from that of no further value so that the latter may be subject to disposition.

Appraisal methodology – the process in place which ensures an efficient, consistent, auditable and transparent approach to understanding how records are appraised and why they are selected.

Authority refers to public authorities subject to the Freedom of Information Act 2000 and bodies subject to the Public Records Act 1958 or The Public Records Act (Northern Ireland) 1923.

Contractor – a privately owned or publicly traded but not a state-owned enterprise – either for profit or non-profit – that produces goods or services under contract for the government.

Destruction – the process of eliminating or deleting a record, beyond any possible reconstruction. [BS ISO 15489-1:2016]

Digital continuity is the ability to use your information in the way you need, for as long as you need. Managing digital continuity means making sure that information is complete, available and usable to meet your organisation's needs and obligations. Activities that can help you manage digital continuity include information management, information risk assessment and understanding technical dependencies.

Digital Preservation refers to the series of managed activities necessary to ensure long term access to digital materials. It includes actions to maintain persistence and fixity, manage dependencies, survive media failure and maintain usability and context through generations of technological, organisational and societal change.

Disposition – a range of processes associated with implementing destruction or transfer decisions which are documented in the disposal schedule.

Disposal schedule – a schedule that identifies types of information and specifies how long it will be kept before it is either reviewed, designated for permanent preservation or destroyed. [BS ISO 15489-1:2016]

Data Protection – measures undertaken in accordance with data protection legislation, including the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (UK GDPR).

Information Asset – a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Information assets have recognisable and manageable value, risk, content and lifecycles.

Keeping records – creating, handling and storing information in an orderly way to record the transactional activities of the authority.

Metadata – contextual information that describes and gives more information about the records and information such as title, author, date, subjects, keywords etc. It enables the management and use of records over time and within and across domains. [ISO 23081-2:2007, 3.7]

Place of Deposit – an archive appointed to receive, preserve and provide access to public records selected for permanent preservation but not transferred to The National Archives. The power of appointment is delegated by the Secretary of State to the Chief Executive and Keeper of The National Archives or an officer of appropriate seniority.

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

Public records – records created by bodies subject to the Public Records Act 1958 or the Public Records Act (Northern Ireland) 1923. The term 'public records' includes Welsh public records as defined by section 148 of the Government of Wales Act 2006. Public records are the records of government departments and their executive agencies, some non-departmental public bodies, the courts, the NHS and the armed forces. In England and Wales local government records are not public records, but those in Northern Ireland are.

Records – recorded information created, received, and maintained as evidence and as an asset by an organisation or person, in pursuit of legal obligations or in the transaction of business. [BS ISO 15489-1:2016]

Records management – the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.

Retention – an arrangement under the Public Records Act 1958 whereby authorities are permitted by the Secretary of State for Digital, Culture, Media and Sport to delay the transfer of specified public records for an agreed period and to retain them until the end of that period.

Selection – a decision making process which encompasses initial appraisal judgements and determines which records will be selected for permanent preservation and transferred to an archive.

Sensitivity review – a process whereby public records are reviewed by the public record-transferring body to identify whether they should be retained, transferred or transferred subject to FOI exemptions.

Transfer – the process of transferring public records to an archive such as The National Archives, The Public Record Office of Northern Ireland or a Place of Deposit. Under s 3(6) PRA, authorities can also present public records as 'gifts' to other bodies, such as a museum or research body. Transfer of ownership must be approved by The National Archives.

CCS0221019740
978-1-5286-2517-3