Cabinet Office

Freedom of Information Code of Practice

This information is available on the GOV.UK website at:
https://www.gov.uk/government/publications/freedom-of-information-code-of-practice]

Contents

[back of contents page – for printed publications, leave this page blank]

Foreword

Freedom of Information is one of the pillars upon which open government operates. The Government is committed to supporting the effective operation of the Freedom of Information Act. For any Freedom of Information regime to be truly effective it is important that both its users and those subject to it have faith in it.

This Code of Practice provides guidance for public authorities on best practice in meeting their responsibilities under Part I of the Act. It sets the standard for all public authorities when considering how to respond to Freedom of Information requests.

The Information Commissioner also has a statutory duty to promote good practice by public authorities, including following this Code of Practice. In addition to this Code of Practice, public authorities should also consult the Commissioner's own guidance regarding best practice which can be found at www.ico.org.uk.

The Commissioner can issue practice recommendations where he or she considers that public authorities have not conformed with the guidance set out in this Code. The Commissioner can also refer to non-compliance with the Code in decision and enforcement notices.

This foreword does not form part of the Code itself.

Introduction

This Code of Practice provides guidance to public authorities on the discharge of their functions and responsibilities under Part I (Access to information held by public authorities) of the Freedom of Information Act 2000 ("the Act'). It is issued under section 45 of the Act.

1. Right of Access

Information

1.1 The Freedom of Information (FOI) Act 2000 ('the Act') gives a right of access to information. Any person who makes a request to a public authority for information is entitled:

- To be informed in writing by a public authority whether it holds information meeting the description set out in the request; and
- To have information the public authority holds relating to the request communicated to them.

These rights apply unless an exemption in Part II of the Act applies, or the request can be refused under sections 12 or 14, as set out in the legislation.

1.2 Section 84 of the Act defines the 'information' a public authority can be asked to provide under the Act. It makes clear that it means recorded information held in any form, electronic or paper.

1.3 Public authorities are not required to create new information in order to comply with a request for information under the Act. They only need to consider information already in existence at the time a request is received.

1.4 A request to a public authority for recorded information will be treated as a request under the Act, other than:

- information given out as part of routine business, for example, standard responses to general enquiries;
- a request for environmental information; or
- the requester's own personal data.

1.5 A request for environmental information only should be dealt with under the Environmental Information Regulations 2004[1], and a request for a person's own personal data should be dealt with under the subject access provisions of the Data Protection Act 2018. Sometimes it may be necessary to consider a request under more than one access regime.

1.6 The Act provides a right to information. Disclosing existing documents will often be the most straightforward way of providing information. However, in other cases it may be

[1] Public authorities may wish to refer to the Information Commissioner's *Regulation 16 Code of Practice: Discharge of Obligations of Public Authorities under the EIR*.

appropriate to extract the relevant information for disclosure and put in a single document rather than redact the existing document that contains it.

1.7 There will be occasions where a request is made under the Act but does not in fact meet the above description of being a request for recorded information. This may include requests for explanations, clarification of policy, comments on the public authority's business, and any other correspondence that does not follow the definition of a valid request in section 8. It is best practice to provide an applicant with an explanation of why their request will not be treated under the Act if this is the case and to respond to their correspondence through other channels as appropriate. It is open to the applicant to appeal the handling of their correspondence to the Information Commissioner's Office.

Information held

1.8 In order to respond to a request for information public authorities need to consider whether the requested information is 'held' for the purposes of the Act. This is because there may be instances when a public authority possesses information, either electronically or in physical copy, that does not meet the criteria for information 'held' set out in the Act and to which the obligations set out in the Act therefore do not apply.

1.9 Section 3(2) sets out the criteria for when information is held by a public authority for the purposes of the Act. This includes:

- information held by a public authority at the time of the request;
- information stored in off-site servers or cloud storage; and
- information held by other organisations and authorities on behalf of the public authority including, for example, off-site storage or information provided to lawyers for the purposes of litigation.

1.10 Information is 'held' by the public authority if it is retained for the purposes of the public authority's business. Purely personal, political, constituency, or trade union information, for example, will not be 'held' for the purposes of the Act and so will not be relevant for the purposes of the request. Where a public authority holds or stores information solely on behalf of another person or body that material will also not be 'held' by that authority for the purposes of the Act.

1.11 Information created after a request is received is not within the scope of the application and is therefore not "held" for the purposes of the Act. A search for information which has been deleted from a public authority's records before a request is received, and is only held in electronic back up files, should generally be regarded as not being held[2].

[2] Public authorities should make sure they are also aware of the guidance provided in the Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000.

1.12 Public authorities need to search for requested information in order to communicate to the applicant whether the information they are seeking is held or not held by that public authority. These searches should be conducted in a reasonable and intelligent way based on an understanding of how the public authority manages its records. Public authorities should concentrate their efforts on areas most likely to hold the requested information. If a reasonable search in the areas most likely to hold the requested information does not reveal the information sought, the public authority may consider that on the balance of probabilities the information is not held.

Section 77 (Offence of altering records etc. with intent to prevent disclosure)

1.13 Public authorities should make sure that their staff are aware that under section 77 of the Act it is a criminal offence to alter, deface, block, erase, destroy or conceal any information held by the public authority with the intention of preventing disclosure following a request under the Act for the information.

Valid requests

1.14 Section 8 sets out the criteria for what constitutes a valid request under the Act:

- Section 8(1)(a) requires that a request for information must be made in writing. This can either be in hard copy or electronically;
- Section 8(1)(b) requires that a request for information must state the name of the applicant and an address for correspondence. Applicants must provide their real name and not use a pseudonym. Both email and postal addresses are acceptable;
- Section 8(1)(c) requires that a request for information must also adequately describe the information sought.

1.15 Public authorities do not have to comply with requests that do not meet the requirements set out in section 8. It is good practice to write to the applicant and explain this if this is the case.

1.16 A request submitted through social media will be valid where it meets the requirements of section 8 by providing an applicant's name and address for correspondence and a clear request for information. Addresses for correspondence can take the form of an email address or a unique name or identifier on a social media platform (for example a Twitter handle), as well as postal addresses. Requests must be addressed directly to the public authority the applicant is seeking information from, which includes elected officials and appointed representatives, when acting in their formal capacity. In order to be addressed directly, a public authority must have a formal, monitorable presence on the particular platform being used by an applicant.

1.17 Requests submitted in a foreign language are not generally considered valid requests. Public authorities are not expected to obtain translations of suspected requests for information. It is good practice when receiving a request in a foreign language to ask the applicant to provide their request in English or Welsh in order for the request to be processed.

Fees

1.18 It is open to public authorities, as a result of Regulations made under sections 9 and 13 of the Act, to charge for the cost of providing information requested under the Act. However, the majority of public authorities do not currently do so. It is also only possible to charge where information will be released. It is not possible for public authorities to charge for requests where, for example, information is being withheld under exemptions.

1.19 Where the public authority intends to charge for the cost of providing information, they should send a fees notice stating the amount to be paid, including how this has been calculated, as soon as possible within the 20 working day response period. The notice should inform applicants:

- that the 20 working day period for responding to the request will be paused until payment is received (it is reasonable to set a deadline of three months in which the fee should be paid);
- how to pay the fee; and
- their rights of complaint via internal review and to the Information Commissioner about the fee levied.

1.20 Public authorities may charge for:

- actual production expenses (e.g. redacting exempt information, printing or photocopying);
- transmission costs (e.g. postage); and
- complying with the applicant's preferences about the format in which they would like to receive the information (section 11) (e.g. scanning to a CD).

1.21 It is not possible to charge for any staff time where the cost of compliance falls below the cost limit (see Chapter 6). There is no obligation to comply with any request exceeding the cost limit. However, should a public authority decide to respond to a request that exceeds the cost limit on a voluntary basis it can charge for the staff time needed to do so. In such circumstances staff time is chargeable at a standard rate, including the cost of making redactions (but only the physical cost of making redactions and not staff time for considering whether exemptions apply), to be included in the initial fees notice.

1.22 Public authorities may already charge for supplying specific categories of information on a different statutory basis to the fees they are allowed to charge under the Act. They can continue to do this even when these charges are higher than the fees that can be charged

under the Act. However, public authorities may not charge where a statutory obligation to provide information free of charge already exists.

1.23 Once the fee is received, the public authority should process it promptly and inform the applicant of the revised 20 working day response deadline. It is permissible to wait until a cheque clears before recommencing work. Should a public authority underestimate the costs to be charged, it should not issue a second fees notice and should bear the additional cost itself.

Means of communication

1.24 Section 11 of the Act says that if an applicant states a preference for receiving information in a specific format a public authority shall, if they are required to disclose information, aim to meet this preference as far as is reasonably practicable. Applicants may, for instance, request to receive the information in an electronic or hard copy format.

1.25 When considering whether it is reasonable to meet an applicant's wishes under section 11, public authorities may, for instance, consider the cost and complexity of providing information in the format requested and the resources they have available.

1.26 If an applicant doesn't state a preference, public authorities can communicate information by "any means which are reasonable in the circumstances" as set out in section 11(4). For example, where the platform used by an applicant to make their request imposes restrictions on the format of a response (for example, Twitter restricts the length of a response and does not allow the direct attachment of documents) it would be reasonable to respond in another format.

1.27 Guidance on additional requirements in relation to datasets is provided in Chapter 11 and for model communications in Chapter 10.

2. Advice and assistance

2.1 Section 16 of the Act sets out a duty for public authorities to provide reasonable advice and assistance to applicants requesting information. This duty to advise and assist is enforceable by the Information Commissioner. If a public authority does not meet this duty, the Commissioner may issue a decision notice under section 50, or an enforcement notice under section 52.

2.2 Public authorities should bear in mind that other Acts of Parliament may also be relevant to the way in which they provide advice and assistance to applicants or potential applicants, for example, compliance with duties under the Equality Act 2010.

Advice and assistance to prospective requesters

2.3 Public authorities should, as a matter of best practice, publish a postal address and email address (or appropriate online alternative) to which applicants can send requests for information or for assistance.

2.4 There is no requirement for a request for recorded information specifically to mention the Act in order to be a valid FOI request. Where an applicant asks a public authority to disclose recorded information but does not specifically mention the Act, and the request complies with section 8 (see paragraph 1.14 above), the public authority should consider the request under the Act in any case and let the applicant know that this is how the request is being handled. Where a person seeks to make a request orally they should be advised to put their application in writing in accordance with section 8(1)(a) of the Act.

2.5 There may be circumstances where a person is unable to frame their request in writing, for example owing to a disability. In these instances the public authority should make sure that assistance is given to enable them to make a request for information. For example, advising the person that another person or agency (such as a Citizens Advice Bureau) may be able to assist them with the application, or make the application on their behalf. Public authorities may also consider, in exceptional circumstances, offering to take a note of the application over the telephone and sending the note to the applicant for confirmation. Once verified by the applicant this would constitute a written request for information and the statutory time limit for reply would begin when the written confirmation was received.

Clarifying the request

2.6 There may be instances when a public authority needs to contact an applicant to seek clarification either regarding their name or the information they are seeking in order for the request they have made to meet the requirements set out in section 8 of the Act.

2.7 If a public authority considers the applicant has not provided their real name the public authority can make the applicant aware it does not intend to respond to the request until further information is received from the applicant. For example, this may be the case when an applicant appears to have used a pseudonym rather than their own name.

2.8 There may also be occasions when a request is not clear enough to adequately describe the information sought by the applicant in such a way that the public authority can conduct a search for it. In these cases, public authorities may ask for more detail to enable them to identify the information sought.

2.9 Where a public authority asks for further information or clarification to enable the requester to meet the requirements of section 8, the 20 working day response period will not start until a satisfactory reply constituting a valid request is received. Letters should make clear that if no response is received the request will be considered closed by the public authority. Two months would be an appropriate length of time to wait to receive clarification before closing a request.

Reducing the cost of a request

2.10 Where it is estimated the cost of answering a request would exceed the "cost limit" beyond which the public authority is not required to answer a request (and the authority is not prepared to answer it), public authorities should provide applicants with advice and assistance to help them reframe or refocus their request with a view to bringing it within the costs limit. Further guidance on the appropriate "cost limit" can be found in Chapter 6.

Transferring requests for information

2.11 There will be occasions when a public authority is not able to comply with a request (or to comply with it in full) because it does not hold the information requested.

2.12 In most cases where a public authority does not hold the information, but thinks that another public authority does, they should respond to the applicant to inform them that the requested information is not held by them, and that it may be held by another public authority. The public authority should, as best practice where they can, provide the contact details for the public authority they believe holds the requested information.

2.13 Where the public authority who originally received the request wishes to ask a different public authority directly to deal with the request by transferring it to them, this should only be done with the applicant's agreement in case the requester objects to their details being passed on. This is because public authorities have a duty to respond to a requester and confirm whether or not they hold information in scope of the request as set out in paragraph 2.12 above.

3. Consultation with Third Parties

3.1 There will be circumstances when a public authority should consult third parties about information held in scope of a request in order to consider whether information is suitable for disclosure. These may include:

- when requests for information relate to persons or bodies who are not the applicant and/or the public authority; or
- when disclosure of information is likely to affect the interests of persons or bodies who are not the applicant or the authority.

3.2 Public authorities may want to directly consult third parties in these circumstances particularly if, for example, there are contractual obligations which require consultation before information is released. In other circumstances it may be good practice to consult third parties, for example, where a public authority proposes to disclose information relating to third parties, or information which is likely to affect their business or private interests.

3.3 Consultation will often be necessary because third parties who have created or provided the information may have a better understanding of its sensitivity than the public authority. On this basis it is important the public authority understands the views provided by the third party and gives them appropriate weight. The expert view of a third party may, as long as it is reasonable, be helpful if the applicant appeals against any refusal. The views of third parties will be especially relevant in cases where it is necessary to consider the prejudice and public interest tests.

3.4 Public authorities are not required to accept views provided to them from third parties about whether or not information should be released. It is ultimately for the public authority handling the request to take the final decision on release following any consultation it undertakes.

3.5 If a decision is made to release information following consultation with a third party it will generally be best practice to give the third party advance notice or to draw it to their attention as soon as possible.

3.6 There may be occasions where information being considered by a public authority relates to a large number of third parties. If a public authority intends to release information that relates to a large number of third parties it may be helpful to contact a representative organisation who can express views on these parties' behalf rather than contacting each third party individually. Alternatively, if no representative organisation exists, public authorities can also consider only notifying or consulting a representative sample of third parties regarding the disclosure of information, but these will be case by case judgements for the relevant public authority.

4. Time limits for responding to requests

Statutory deadlines

4.1 The statutory deadlines for public authorities to respond to requests for information are set out in section 10(1) of the Act. These make clear that public authorities must respond to requests for information promptly and within 20 working days following the date of receipt of the request.

4.2 The date on which a request is received is the day on which it arrives or, if this is not a working day, the first working day following its arrival. Non-working days include weekends and public holidays.

4.3 Some public authorities are subject to different deadlines as a result of regulations made under section 10(4) of the Act. For example, maintained schools, academies, archives, the armed forces (frontline units) and information held outside the United Kingdom at for example, embassies, have had the initial 20 working day deadline extended in certain circumstances as they may sometimes find it difficult to deal with requests under the standard deadlines. These initial deadlines cannot go beyond 60 working days following receipt of a request, except where payment of a fee is awaited (paragraph 1.19).

Public interest test extensions

4.4 Public authorities may exceed the 20 working day deadline (or, where permitted by section 10(4) regulations, longer) if information falls within the scope of a qualified exemption and additional time is required to consider the public interest test. This is set out in Section 10(3) of the Act. This is normally described as a public interest test extension.

4.5 An extension is permitted "until such time as is reasonable in the circumstances", taking account, for example, of where the information is especially complex or voluminous, or where a public authority needs to consult third parties.

4.6 In general, it is best practice for an extension to be for no more than a further 20 working days although this will depend on the circumstances of the case, including again the complexity and volume of the material, and in some circumstances a longer extension may be appropriate.

4.7 Where public authorities decide a public interest test extension is required they should write to the applicant to inform them that this is the case, stating which exemption(s) it is rely on, and why, and ideally provide the applicant with a new deadline for when they should

receive their response. If the deadline has to be further extended they should write again to the applicant.

5. Internal reviews

5.1 It is best practice for each public authority to have a procedure in place for dealing with disputes about its handling of requests for information. These disputes will usually be dealt with as a request for an "internal review" of the original decision. Public authorities should distinguish between a request for an internal review, which seeks to challenge either the outcome or the process of the handling of the initial response, and a general complaint, which should be handled as general correspondence.

5.2 Public authorities are obliged, under section 17(7) of the Act, when responding to a request for information, to notify applicants of whether they have an internal review process and, if they do, to set out the details of their review procedures, including details of how applicants request an internal review. They should also inform the applicant of their right to complain to the Information Commissioner under section 50 if they are still dissatisfied following the outcome of the public authority's internal review.

5.3 It is usual practice to accept a request for an internal review made within 40 working days from the date a public authority has issued an initial response to a request and this should be made clear in that response to the applicant. Public authorities are not obliged to accept internal reviews after this date. Internal review requests should be made in writing to a public authority.

5.4 Requests for internal review should be acknowledged and the applicant informed of the target date for responding. This should normally be within 20 working days of receipt.

5.5 If an internal review is complex, requires consultation with third parties or the relevant information is of a high volume, public authorities may need longer than 20 working days to consider the issues and respond. In these instances, the public authority should inform the applicant and provide a reasonable target date by which they will be able to respond to the internal review. It is best practice for this to be no more than an additional 20 working days, although there will sometimes be legitimate reasons why a longer extension is needed.

5.6 In the event that clarification of an internal review request is required from the applicant, the normal 20 working day time period will not begin until it is received.

5.7 Public authorities who are allowed to exceed the normal 20 working day deadline as a result of regulations made under section 10(4), for example maintained schools and the armed forces, should apply the same time scales to internal reviews.

5.8 The internal review procedure should provide a fair and thorough review of procedures and decisions taken in relation to the Act. This includes decisions taken about where the public interest lies if a qualified exemption has been used. It might also include applying a different or additional exemption(s).

5.9 It is best practice, wherever possible, for the internal review to be undertaken by someone other than the person who took the original decision. The public authority should in all cases re-evaluate their handling of the request, and pay particular attention to concerns raised by the applicant.

5.10 The applicant should be informed of the outcome of their internal review and a record should be kept of all such reviews and the final decision made.

5.11 If the outcome of an internal review is a decision that information previously withheld should now be disclosed, the information should normally be provided at the same time as the applicant is informed of the outcome of the review. If this is not possible, the applicant should be informed how soon the information will be provided.

5.12 In responding to a request for an internal review, the applicant should again be informed of their right to apply to the Information Commissioner for a review of whether the public authority has met the requirements of the Act.

6. Cost limit

6.1 Section 12 of the Act allows public authorities to refuse to deal with any requests where they estimate that responding to the request would exceed the "appropriate limit", or 'cost limit' as it is more commonly known.

6.2 If a public authority calculates that responding to a request will take it over the cost limit it is not obliged to provide a substantive response. The cost limit is calculated at a flat rate of £25 per hour. For central government departments the cost limit is £600 (24 hours) and for all other public authorities is £450 (18 hours).

6.3 Public authorities can only include certain activities when estimating whether responding to a request would breach the cost limit. These are:

- establishing whether information is held;
- locating and retrieving information; and
- extracting relevant information from the document containing it.

6.4 Other factors including redaction time or any other expenses likely to occur in cost limit calculations cannot be included when estimating whether the response would exceed the cost limit.

6.5 When calculating the cost limit public authorities can aggregate requests which ask for the same or similar information and are received within a 60 working day period. These requests can either be from the same person or a group of people acting together.

6.6 Public authorities do not have to search for information in scope of a request until the cost limit is reached, even if the applicant requests that they do so. If responding to one part of a request would exceed the cost limit, public authorities do not have to provide a response to any other parts of the request.

6.7 The cost limit can be applied on the basis of a reasonable estimate at the time the request is received. Public authorities are not under any obligation to make a precise calculation although estimates should be sensible and realistic.

6.8 Public authorities should generally focus their attention on the locations most likely to hold the relevant information. Searches may take longer, for example, where information is only held in paper records or they are organised in a way that does not lend itself to the request in question. In some cases it may be helpful to conduct a sampling exercise to help establish likely cost but this is not essential.

6.9 Where a request is refused under section 12, public authorities should consider what advice and assistance can be provided to help the applicant reframe or refocus their request

with a view to bringing it within the cost limit. This may include suggesting that the subject or timespan of the request is narrowed. Any refined request should be treated as a new request for the purposes of the Act.

6.10 The cost limit should be applied before any exemption in Part II of the Act. This is because it will generally be necessary to establish whether information is held and to collate it before applying an exemption.

7. Vexatious requests

7.1 Under section 14(1) of the Act a public authority is not obliged to provide a substantive response to a request if the request is vexatious. Like section 12, section 14 should be considered before consideration of any exemption in Part II of the Act.

7.2 The Act does not define what makes a vexatious request, though there are a number of Tribunal cases which have offered clarity and guidance on this issue. The Information Commissioner's Office's guidance for dealing with vexatious requests gives details of these. Public authorities should consider each case on its own facts, taking into consideration the best practice factors below. Section 14(1) may be used in a number of circumstances where a request, or the impact of a request, is not justifiable or reasonable.

7.3 Public authorities should always think carefully about applying section 14. However, Section 14(1) should not be considered as something to be applied as a last resort or in exceptional circumstances.

7.4 There will be times when a request is so unreasonable or objectionable that it is clear it is a vexatious request. For example, an abusive or offensive request that causes an unjustifiable level of distress or where threats are, or have been, made against staff.

7.5 In other circumstances it may be less immediately obvious that a request should be considered as vexatious. A public authority should consider a request vexatious where the request is likely to cause a disproportionate or unjustified level of disruption, irritation or distress. Factors public authorities might therefore want to consider include:

- the burden it places on a public authority and its staff;
- the likely motives for the request;
- the potential value or purpose of the request;
- any harassment or distress to staff.

7.6 It may be helpful for a public authority to ask itself the following questions when considering whether a request is vexatious:

- What is the burden imposed on the public authority by the request?
- Is there a personal grudge behind the request?
- Is the requester unreasonably persisting in seeking information in relation to issues already addressed by the public authority?
- Does the request have any serious purpose or value?

7.7 Public authorities can also take into account the wider context of a request to help them identify whether a request should be considered vexatious. For example:

- what other requests have been made by the same requester to the public authority;
- the number and subject matter of the requests if there are multiple requests; and
- previous dealings with the requester.

Having looked at the wider context, it is then important to assess whether the evidence supports or weakens the vexatious argument.

7.8 There may also be times when a public authority considers that responding to a new request following a series of previous requests would engage section 14(1) because doing so would be disruptive or burdensome to the public authority given the volume of previous correspondence.

7.9 The following are examples public authorities may want to use when considering whether a request is vexatious:

- When an applicant has engaged in a large volume of sustained correspondence over a number of years in abusive or confrontational language.
- Contact with a public authority that can be classified as long, detailed and overlapping. For example, a scenario when a requester has written to a series of officers on the same matters, repeating requests before a public authority has had the opportunity to answer an initial request and where responding to this correspondence would be a significant distraction from the public authority's main functions.
- Where a public authority considers that there is a deliberate 'campaign' by a number of requesters to purposefully disrupt the public authority's activities and functions via a high volume of requests on the same or similar topics.

These examples should not limit public authorities from using section 14 in other circumstances, as the reasons why a request might be considered vexatious will depend on the specific factors in each case. The website of the Information Commissioner's Office publishes examples of case law on this issue which may also be helpful to public authorities when considering whether a request is vexatious.

7.10 Public authorities should also keep in mind the requirements of section 8, in particular, the requirement for applicants to provide their real name and not use a pseudonym. As set out in paragraphs 1.14 and 1.15 pseudonymous requests are not valid requests under the Act. However, the use of pseudonyms may also form part of broader considerations when considering whether or not a request, or a series of requests, should be considered vexatious.

7.11 Finally, public authorities should note that the public interest in obtaining the material does not act as a 'trump card', overriding the vexatious elements of the request and requiring the public authority to respond to the request.

Interaction between section 12 (cost limit) and 14(1) (vexatious requests)

7.12 In some cases, responding to the request is so burdensome for the public authority in terms of resources and time that the request can be refused under section 14(1). This is likely to apply in cases where it would create a very significant burden for the public authority to:

- prepare the information for publication;
- redact the information for disclosure;
- consult third parties;
- apply exemptions.

7.13 It is not possible to use section 12 (cost limit) to refuse a request based on the above factors. In these cases, public authorities may want to instead consider using section 14 to refuse to respond to the request based on the burden that responding to the request would create.

7.14 Public authorities should avoid using section 14 for burdensome requests unnecessarily. On this basis they should always consider whether section 12 applies in the first instance. For example, if a public authority considers that locating and extracting the information in scope would exceed the cost limit, section 12 is likely to be most appropriate. However, if, for the reasons set out in paragraphs 7.12 to 7.13 above, section 12 cannot apply they should consider refusing the request using section 14(1).

7.15 An example of when this may happen may include the burden of redacting multiple entries on a large database as, although it may be possible to locate the database easily, redacting relevant entries (if there are thousands of entries) may create an unsustainable burden for the authority.

Repeated requests

7.16 Under section 14(2) of the Act, if a public authority has previously complied with a request for information (i.e. provided the information sought), it does not need to comply with a further request for the same information made by the same person, unless a reasonable interval has elapsed between compliance with the first request and receipt of the second. A repeated request should be interpreted as an identical or substantially similar request. This will depend on the circumstances and each case should be considered on its own merits.

Section 14 responses

7.17 If a public authority considers section 14 applies in any circumstances other than that referred in paragraph 7.14 they should provide a refusal notice to the applicant. This should

be issued within 20 working days and explain that the public authority considers section 14 to be engaged. Public authorities should also include details of their internal review procedures and the right to appeal to the Information Commissioner. There is no obligation to explain why the request is vexatious, though public authorities may wish to do so as part of their section 16 duty to provide advice and assistance.

7.18 There will be some circumstances when a public authority does not need to provide a refusal notice. Section 17(6) sets out that a public authority is not obliged to issue a refusal notice where it considers that it is unreasonable in all the circumstances to do so. For example, if a refusal notice has previously been issued for an earlier vexatious or repeated request, and the public authority does not consider it reasonable to issue a further notice. It is worth noting that although section 17(6) excludes a public authority from the duty to provide a refusal notice, the public authority is still required to establish that each request is vexatious.

7.19 Public authorities should consider keeping an ongoing evidence log to record relevant correspondence or behaviour that has been taken into account when using section 14. This will be helpful in the event the applicant complains about the handling of the request.

8. Publication Schemes

8.1 Section 19 of the FOI Act requires all public authorities to adopt and maintain a publication scheme. This element of the Act is designed to increase transparency and allow members of the public to routinely access information relating to the functions of a public authority.

8.2 The Information Commissioner's Office has approved a model publication scheme which public authorities should use in the first instance.

Public authorities should also produce a guide to the scheme setting out:

- what information is published and by what means;
- a schedule of fees, which should set out clearly any charges for obtaining any of the information.

8.3 Publication schemes must be updated and maintained, so public authorities must have a process for reviewing published information in order to ensure it is updated at appropriate intervals. Public authorities should also follow the timescales for publication of particular types of information as set out in the Information Commissioner's Office guidance.[3]

8.4 This Code of Practice provides more specific guidance on two areas to supplement the existing guidance by the Information Commissioner's Office.

Compliance Statistics

8.5 Public authorities with over 100 Full Time Equivalent (FTE) employees should, as a matter of best practice, publish details of their performance on handling requests for information under the Act. The information should include:

- The number of requests received during the period;
- The number of the received requests that have not yet been processed (you may also wish to show how many of these outstanding requests have extended deadlines or a stopped clock, e.g. because a fee notice has been issued);
- The number of the received requests that were processed in full (including numbers for those that were met within the statutory deadline, those where the deadline was extended and those where the processing took longer than the statutory deadline);
- The number of requests where the information was granted in full;
- The number of requests where the information was refused in full (you may wish to separately identify those where this was because the information was not held);

[3] This guidance is available on the Information Commissioner's website: https://ico.org.uk

- The number of requests where the information was granted in part and refused in part;
- The number of requests received that have been referred for internal review (this needs only reporting annually).

8.6 It is for individual public authorities to decide whether they wish to publish more detailed information than that set out above (they may, for example, wish to show a breakdown of the exemptions they have used for refusing requests or to show a breakdown of the outcomes for their internal reviews). When public authorities publish their statistics, they should do so on a quarterly basis, in line with central government. Publication schemes are likely to form the best vehicle for publishing this information. A guide on producing a suitable publication scheme can be found on the Information Commissioner's website.

Senior Executive Pay & Benefits

8.7 Public authorities should also ensure publication schemes contain data to deliver sufficient transparency regarding the pay and benefits of senior executives and their equivalents.

8.8 In recent years, central government departments have increased the range of data published in respect of senior officials and primarily those at Director level (SCS2) and above. There will not always be a direct read-across for other public authorities but when considering what type of information should be published, authorities should consider those at management board level as a minimum equivalent.

8.9 Public authorities should publish information that covers the following four areas:

- **Pay**. Senior staff who form a public authority's senior management team; for central government departments this would be staff at Director level and above. Many other public sectors have published guidance, which set out sector-relevant salary levels suitable for publication (for example, the Local Government Association's "*Local Transparency Guidance - Publishing Organisation Information*"). The Information Commissioner's Office also publishes sector-relevant advice on this issue. Names and/or job titles should also be included (see 8.10 below).
- **Expenses.** As above, staff on the senior management team, including elected officials and appointed representatives, if these are not already covered elsewhere. This should cover details of international and domestic travel and business expenses.
- **Benefits in kind.** As above. Benefits in kind refer to benefits employees receive from their employment but which are not included in their salary. Examples include, company cars, private medical insurance paid for by an employer or cheap loans. Data should be published to the nearest £100.
- **Hospitality.** As above. This should include any gifts, hospitality and benefits that are received from third parties (though this does not need to include small and insignificant items of hospitality, such as refreshments). This should include the name of the person or organisation that offered the gift or hospitality and the type of gift or hospitality received. This may also include additional information, such as whether the staff member was accompanied by a spouse, family member or friend.

8.10 When publishing the names and other details of individual staff, public authorities need to bear in mind the general principle that it is acceptable to name senior managers who expect to be held publicly accountable, but that this does not extend to junior staff who do not have that same expectation. The Information Commissioner's Office generally upholds this distinction.

8.11 Public authorities should publish this type of information at regular intervals. It is recommended that information about pay should be published annually, expenses quarterly and benefits in kind annually. Public authorities can refer to the Information Commissioner's Office guidance as direction to the expected minimum level of detail. Local authorities should follow the publication requirements in the statutory Local Government Transparency Code on senior salary.

9. Transparency and confidentiality obligations in contracts and outsourced services

Transparency

9.1 As more public services are contracted out to the private sector it is important that they are delivered in a transparent way, to ensure accountability to the user and taxpayer. There will be some circumstances when contractors hold information about contractual arrangements on behalf of a public authority which will then be subject to the Act.

9.2 It is important that contractors and public authorities are clear what this information is, and that it is made readily available to the contracting public authority when it receives requests under the Act.

Information held on behalf of a contracting public authority

9.3 When entering into a contract with a third party it is likely that both the public authority and the contractor will hold information about these contractual arrangements. If a contractor holds information relating to the contract "on behalf" of a public authority, this information should be considered in the same way as information held by a public authority and so will be subject to the Act (as explained in Chapter 1). Such information would, for example, include that which a public authority has placed in the custody of a contractor (e.g. record storage) or where a contract stipulates that certain information about service delivery is held on behalf of an authority for FOI purposes.

9.4 When entering into a contract the public authority and the contractor should agree what types of information they consider will be held by the contractor on behalf of the public authority and indicate this in the contract or in an annex or schedule. They should also think about putting in place appropriate arrangements for the public authority to gain access to the information if a request is made under the Act.

9.5 These appropriate arrangements may include:

- how and when the contractor should be approached for information, and who the contact points in each organisation are;
- how quickly the information should be provided to the public authority bearing in mind the statutory deadline for responding to the request;
- how any disagreement about disclosure between the public authority and contractor will be addressed;

- how any request for internal review or subsequent appeal to the Information Commissioner will be handled;
- the contractor's responsibility for maintaining adequate systems for record keeping in relation to information held on behalf of the public authority; and
- where the public authority itself holds the requested information, the circumstances under which the public authority must consult the contractor about disclosure and the process to be adopted in such cases.

9.6 These arrangements should, as good practice, be set out in the contract or in a related Memorandum of Understanding.

9.7 Given the statutory obligations of public authorities to respond to requests under the Act, and the fact that information held on their behalf by contractors is information subject to the Act, contractors must comply with requests by a public authority for access to such information, and must do so in a timely manner.

9.8 Requests for information held by contractors on behalf of a public authority should be answered by the public authority. Contractors receiving requests should pass them to the public authority for consideration or respond to the applicant to let them know they should direct their request to the relevant public authority.

Contract clauses

9.9 Where contractors deliver services on behalf of a public authority the contract with the public authority will need to make clear that contractors will need to fully assist the public authority with their obligations under the Act in line with the guidance set out in this chapter. The contract should include details of how non-compliance with these obligations will be dealt with. This should apply to both new and amended contracts.

9.10 If existing contracts do not set out these provisions, public authorities and contractors should consider alternatives to ensuring that the contractor provides the public authority access to information held on the public authority's behalf. Options to consider include a supplementary Memorandum of Understanding.

9.11 Public authorities may be asked to accept confidentiality clauses when entering into a contract with a third party. Public authorities should carefully consider whether these agreements are compatible with their obligations under the Act and the public interest in accountability. It is important that both the public authority and the contractor are aware of the legal limits placed on the enforceability of such confidentiality clauses[4] and the importance of making sure that the public can gain access to a wide range of information about contracts and their delivery. Public authorities should be mindful of any broader transparency obligations to publish regular details of spending, tenders and contracts on external suppliers; contracts should not hinder such transparency reporting.

[4] Under common law a breach of a duty of confidentiality is not enforceable in the courts where an overriding public interest justifies the breach.

9.12 Where there is good reason to include non-disclosure provisions in a contract, however, it may be helpful for public authorities and contractors to agree the types of information which should not be disclosed within a contract and the reasons for this confidentiality.

9.13 There may also be circumstances when public authorities offer or accept confidentiality arrangements that are not set out within a contract. Public authorities should also follow the guidance set out in this chapter in these circumstances. There will be circumstances when these agreements will be appropriate in order for the public authority to receive information from a third party; hence, this information may be protected by the exemptions in the Act. It will be important that both the public authority and the third party are aware of the legal limits placed on the enforceability of expectations of confidentiality and the public interest in transparency, as well as for authorities to ensure that such expectations are created only where it is appropriate to do so.

10. Communicating with a requester

10.1 Public authorities may find the following guidance helpful for ensuring responses to requests for information and internal reviews meet the requirements set out in the Act.

10.2 Any initial response to a request for information under the Act should contain:

- A statement that the request has been dealt with under the Act;
- Confirmation that the requested information is held or not held by the public authority or a statement neither confirming or denying whether the information is held;
- The process, contact details and timescales for the public authority's internal review appeals process;
- Information about the applicant's further right of appeal to the Information Commissioner and contact details for the Information Commissioner's Office.
- If some or all of the information cannot be disclosed, details setting out why this is the case, including the sections (with subsections) the public authority is relying on if relevant. When explaining the application of named exemptions, however, public authorities are not expected to provide any information which is itself exempt.

10.3 The response to a request for an Internal Review should contain:

- Whether the Internal Reviewer agrees with the original response or not;
- Whether the reviewer considers that new exemptions are applicable and, if so, details of these exemptions and why they are engaged (to the extent they can without providing exempt information);
- Information about the applicant's further right of appeal to the Information Commissioner and contact details for the Information Commissioner's Office.

11. Datasets

11.1 Sections 11,11A, 11B and 19 of Part I of the Act provide additional rights in relation to the disclosure and, in some cases, re-use of datasets.

11.2 The provisions governing the release of a dataset apply to all datasets held by any public authority subject to the Act.

11.3 Provisions relating to re-use only apply to the relatively small proportion of datasets not subject to the Re-use of Public Sector Information (PSI) Regulations 2015[5]. Guidance about the re-use of datasets under the FOI Act is provided in Annex B to this Code of Practice.

11.4 The Act does not require the creation of datasets for publication, nor does it require datasets to be updated if they would not otherwise have been updated as part of the public authority's function. In deciding whether to release a dataset, a public authority should consider any exemptions which may apply and in particular, the exemption in section 40 of the Act relating to personal data and the Information Commissioner's Code of Practice on Anonymisation.

11.5 These considerations should also be taken into account when considering the release of an incomplete or draft dataset. When releasing an incomplete dataset it is good practice to explain the dataset is not complete and the likely implications of this.

i. Scope

11.6 The definition of dataset is limited to the criteria specified at section 11(5) of the Act.

11.7 The first part of the definition (subsection (5)(a)) means that the datasets caught by the Act are those datasets which a public authority has originally obtained or recorded for the purposes of providing services or carrying out its functions, including decision-making.

11.8 The second part of the definition limits datasets to factual information subject to the two criteria in subsection (5)(b). The intention behind the first criterion is to catch 'raw' or 'source' data. Calculation of information within the dataset does not count as 'analysis' or 'interpretation'. Therefore aggregated data forming a high-level dataset (such as the creation of annual figures from data that were collected weekly), form a dataset within the definition of the Act.

11.9 The second criterion excludes official statistics which are subject to their own regime of disclosure and publication, including under the Statistics and Registration Service Act 2007.

[5] http://www.nationalarchives.gov.uk/information-management/re-using-public-sector-information/

11.10 Subsection 5(c) is also intended to ensure only 'raw' or 'source' data is captured within the meaning of a dataset. The key consideration here is whether the reorganisation or adaptation represents a 'material alteration' to the original presentation of the dataset. Minor or insignificant changes to a dataset will not take it outside the definition.

11.11 The other key consideration in the definition is how much, if any, of the data in the dataset has been changed or altered. If 'all or most' of the data in the dataset meet the criteria set out in subsection 5, then the dataset will fall within the definition. Examples of where datasets will continue to fall under the definition within the Act include:

- The original dataset used to form a new dataset;
- Amended datasets where work has been undertaken to improve the quality of a dataset;
- Datasets that have been anonymised, or otherwise had exempt information removed.

11.12 Where information requested meets the definition of a dataset, the authority will be under a duty to provide the dataset in a re-usable format where reasonably practicable.

ii. Disclosing datasets in an electronic form which is capable of re-use

11.13 When releasing any dataset under the Act public authorities must, as far as reasonably practicable, provide it in a re-usable format. A re-usable format is one that is machine readable, such as Comma-separated Value (CSV) format.

11.14 Where datasets are only held in non-re-usable formats, the public authority is not obliged to convert the dataset before releasing it where it is not reasonably practicable to do so.

11.15 In deciding whether it would be practicable to provide the dataset in a re-usable format, the public authority can take account of all the relevant circumstances. These circumstances may include the time and the cost involved in converting the dataset from a proprietary to a re-usable format, and the resources available to the public authority.

11.16 If the public authority concludes that it would not be reasonably practicable to provide the dataset in a re-usable format, then the public authority must still provide the dataset in another format.

iii. Standards applicable to public authorities in connection with the disclosure of a dataset

11.17 When releasing datasets public authorities should adhere to the Public Data Principles where possible. These principles are expected good practice for central government departments and recommended for the wider public sector.

11.18 It is recommended good practice that datasets will be accompanied by sufficient metadata and contextual information about how and why the dataset was compiled or created.

11.19 When procuring new data processing systems, public authorities should reference the Government Principles for Open Standards in new government information technology specifications for software interoperability, data and document formats. The Principles are compulsory for central government departments, their agencies, non-departmental public bodies and any other bodies for which they are responsible.

iv. Cost of providing the dataset in a reusable format

11.20 If the cost of complying with the request would not exceed the appropriate limit and the information is not otherwise exempt, the public authority must provide the dataset (subject to any right to charge a fee). If the requester expresses a preference for the dataset in electronic form, the public authority must provide it in a reusable format, so far as reasonably practicable. A public authority may not charge for the cost of providing the dataset in a reusable format, but, in deciding whether it would be reasonably practicable to provide it in that format, it can take account of the cost, time and resources that would be involved.

v. Publication of datasets as part of a publication scheme

11.21 Public authorities should consider publishing existing and newly created datasets as part of their publication scheme. If the dataset would be released on request, the public authority should consider publishing it through the public authority's publication scheme.

11.22 Public authorities should consider their long term plans and processes for the collection and storage of datasets, keeping in mind that they should be made easily accessible and in a re-usable format for requests or publication as part of their publication scheme as well as for normal business purposes.

11.23 When publishing a dataset on their website, public authorities, should, where possible, publish it in a machine readable format, so that the data can be directly downloaded from a given URL.

11.24 If a dataset has been requested from a public authority under the Act, then the authority must publish that dataset in accordance with its publication scheme unless the public authority is satisfied that it would not be appropriate to publish it. If the public authority holds an updated version of the dataset it must also publish the updated version, unless it is satisfied that it is not appropriate to do so.

11.25 When the public authority publishes the dataset under its publication scheme, it must (as for responding to a request) provide it in an electronic form that is capable of re-use, where it is reasonably practicable to do so.

Annex A – Table of FOI Act Exemption Clauses

The table below sets out a straightforward reference guide to the exemption clauses that are set out under Part II of the FOI Act. Detailed guidance on the application of these exemptions is set out on the website of the Information Commissioner's Office.

* starred exemptions are absolute; all other exemptions require a public interest test.

Section No.	Description
21 *	Information accessible to the applicant by other means.
22	Information intended for future publication, including that obtained in the course of a programme of research.
23 *	Information supplied by, or relating to, bodies dealing with security matters.
24	Information for the purpose of safeguarding national security.
26	Information that may prejudice defence of the realm.
27	Information that may prejudice international relations.
28	Information that may prejudice relations between administrations within the United Kingdom.
29	Information that may prejudice the economic or financial interests of the United Kingdom.
30	Information held for the purposes of investigations and proceedings conducted by public authorities.
31	Information that may prejudice law enforcement.
32 *	Information contained in court documents and records.
33	Information that may prejudice the exercise of audit functions.
34 *	Information that may infringe the privileges of either House of Parliament.

35	Information that relates to the formulation or development of Government policy.
36	Information that may prejudice the collective responsibility of Ministers, inhibit the free and frank provision of advice or prejudice the effective conduct of public affairs.
37*	Information relating to communications with Her Majesty and other members of the Royal Household or the conferring of honours (absolute exemption in relation only to communications with the Sovereign, the heir to the Throne and second in line to the Throne).
38	Information that may be likely to endanger the safety or the physical or mental health of an individual.
39	Information relating to environmental information.
40 *	Personal data (absolute exemption in relation only to information that is the personal data of the applicant).
41 *	Information that is obtained from another person or public authority and would constitute a breach of confidence.
42	Information that is covered by legal professional privilege.
43	Information that constitutes a trade secret or may prejudice commercial interests.
44 *	Information that is prohibited from disclosure by any enactment, EU obligation or would constitute contempt of court.

Annex B – Re-use of datasets

As well as providing additional rights in relation to the disclosure of datasets, the Act also provides for the re-use of datasets not subject to the Re-use of Public Sector Information (PSI) Regulations 2015. The National Archives has provided separate guidance about the re-use of information[6] in accordance with those Regulations.

Only where the PSI Regulations do not apply, should re-use be considered under the Act. They do not apply to datasets held by educational and research establishments, public service broadcasters, cultural or performing arts bodies (other than public sector museums, libraries and archives), or when held by other public authorities for purposes unrelated to their public task.[7] The easiest way for a public authority to comply with the licensing requirements of both FOI and PSI is to make datasets available for re-use under the Open Government Licence, where appropriate.

Giving permission for datasets to be re-used

Public authorities should release datasets with accompanying details of licence conditions that apply to the re-use of the dataset or any limitation on re-use by virtue of third party intellectual property rights.

Consideration should also be given to the extent to which such information is exempt from disclosure under sections 41 and 43(2) of the Act.

The public authority should ascertain whether copyright and/or database rights ('intellectual property') in the dataset are owned solely by the authority or whether there is a third party interest. Nothing in the Act's re-use provisions overrides the rights of any third parties who may own intellectual property contained in the datasets. If a public authority grants a licence to re-use a dataset or part of a dataset containing third party intellectual property without the owner's permission it may constitute an infringement of the third party's rights.

Where there is a third party interest any re-use licence must permit re-use only of those parts of the dataset that the public authority owns. If possible, and subject to any confidentiality requirements, the public authority should identify the requester who owns the remainder of the rights.

In some cases the public authority may be able to obtain the third party's permission to grant the re-use of the third party intellectual property outside the Act.

[6] http://www.nationalarchives.gov.uk/information-management/re-using-public-sector-information/
[7] http://www.nationalarchives.gov.uk/documents/information-management/guidance-on-public-task-statements.pdf

UK government policy is that, wherever possible, Crown Copyright material should be made available for re-use. If in doubt it is advisable to seek legal advice.

Licensing

If the dataset that is being provided, or any part of it, is a relevant copyright work owned solely by the public authority, the public authority must make that work available for re-use in accordance with the terms of one of the licences specified in the following paragraphs. The UK Government Licensing Framework[8] (UKGLF) provides an overview of the arrangements for licensing the use and re-use of public sector information. The starting point is that public authorities are encouraged to use the Open Government Licence for datasets which can be re-used without charge.

The Open Government Licence is the default licensing model for most Crown copyright information produced by the UK Government and supplied without charge. It is a non-transactional open licence which enables use and re-use with virtually no restrictions. It is applicable when use and re-use, including for commercial purposes, is at no cost to the user/re-user. Established as part of a wider UK Government Licensing Framework, it is hosted on The National Archives website[9].

It is recognised that the Open Government Licence will not be appropriate in all cases, for example, in circumstances where information may only be used for non-commercial purposes. The Non-Commercial Government Licence was developed to incorporate that situation. As with the Open Government Licence, public authorities can link to the Non-Commercial Government Licence on The National Archives website.

Where a public authority charges a fee for the re-use of a dataset, it must do so in accordance with the Charged Licence. The licence consists of standard licensing terms and, like the above licences, forms part of the UK Government Licensing Framework. It can also be accessed on The National Archives website[10].

Costs and fees

It is important to distinguish between the cost to the public authority of disclosing a dataset (including in a re-usable format), and the fees that can be charged to the applicant for making a dataset available for re-use under section 11A (or, where relevant, the equivalent charging provisions in the PSI).

---

[8] http://www.nationalarchives.gov.uk/information-management/re-using-public-sector-information/licensing-for-re-use/ukglf/

[9] http://www.nationalarchives.gov.uk/information-management/re-using-public-sector-information/uk-government-licensing-framework/open-government-licence/

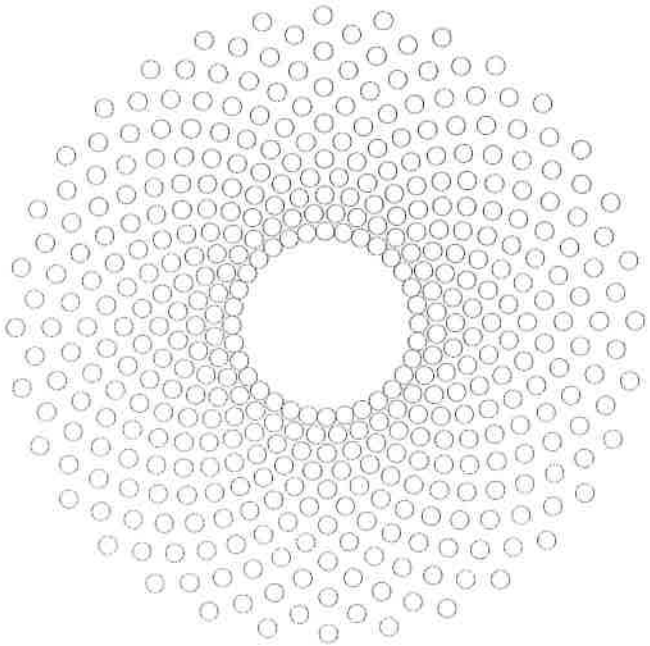
[10] http://www.nationalarchives.gov.uk/information-management/re-using-public-sector-information/uk-government-licensing-framework/open-government-licence/other-licences/

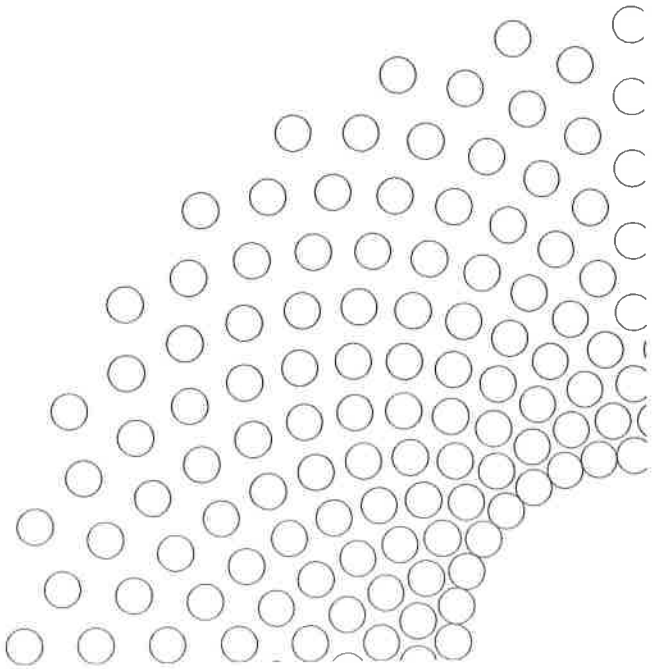
The Freedom of Information (Fees for Re-use of Datasets) Regulations 2013 provide that public authorities may charge a fee for making relevant copyright works available for re-use, unless it already has another applicable statutory power to charge. If a public authority wishes to charge a fee, and is already entitled to do so under any other applicable legislation for the re-use of the relevant copyright work, then it must do so on that other statutory basis instead of these regulations.

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