

Content

About the Code:

Why a framework code of practice?

The benefits of using the framework code of practice.

How to use the framework code of practice.

Code of practice recommended content:

1. Deciding to share personal information

1. Why do you want to share?
2. What will the effect of sharing be?
3. What information do you need to share?
4. Statutory duties to share, restrictions on sharing.
5. Confidential or sensitive information.
6. Consent and objection.
7. Alternatives to sharing personal information.

2. Fairness and transparency

1. Drafting fair processing notices.
2. Providing fair processing information.
3. Informative, up to date notices.
4. Providing further information / dealing with enquiries.
5. Sharing without people's knowledge or consent.

3. Information standards

1. Information quality.
2. Recording information.
3. Relevance.
4. Reviewing information quality.

4. Retention of shared information

1. Retention periods.
2. Reviewing a retention policy.
3. Legal requirements to retain or delete.
4. Deletion and archiving.
5. Retaining information supplied by another organisation.
6. Compliance with your policy.

5. Security of shared information

1. Levels of security
2. Technical security arrangements
3. Organisational security arrangements

6. Access to personal information

1. Helping people get access to their information.
2. Other ways of giving access.
3. Providing all the information.
4. Sources, disclosures and uses of information.

7. Freedom of Information

1. Publication schemes.
2. Requests for personal and non-personal information.

8. Review

Appendix 1 – Other relevant guidance from the Information Commissioner.



About the Code

Why a framework code of practice?

The Information Commissioner's first statutory duty is to promote the following of good practice in the handling of personal information. 'Good practice' means practice that appears to the Commissioner to be desirable, having regard to the interests of individuals and the organisations that process personal information about them. Good practice includes, but is not limited to, compliance with the requirements of the Data Protection Act 1998.

The Commissioner has produced this framework code to help organisations to adopt good practice when sharing information about people. The framework code is intended to be of use to all organisations involved in information sharing. Using the framework code will help organisations to ensure that they address all the main data protection compliance issues that are likely to arise when personal information is being shared. This in turn should help front-line practitioners to make well-informed decisions about sharing personal information.

The benefits of using the framework code of practice

The framework code breaks down compliance with a fairly complex piece of legislation into a series of logical steps. These should be easy for you to follow in practice, even if you're not a data protection expert. Organisations will face different compliance issues, and may adopt their own approaches to dealing with them. However, using the framework code should help organisations to develop a common understanding and a consistency of approach.

Producing your own code of practice, and using it, will help you to establish good practice and to comply with the law. It will also help you to strike the balance between sharing personal information and protecting the people it's about. This should engender the trust of the public and ensure that they understand, and participate in, your information sharing initiatives.

Following a good quality code of practice will also give your staff the confidence to make well informed decisions, reducing the considerable uncertainty that can surround information sharing.

Ultimately, the following of good practice will make your information sharing more effective and will enhance the reputation of your organisation in the eyes of the people you handle information about.

What do we mean by ‘information sharing’?

There are two main sorts of information sharing. The first involves two or more organisations sharing information between them. This could be done by giving access to each others’ information systems or by setting up a separate shared database. The second involves the sharing of information between the various parts of a single organisation, for example between a local authority’s various departments. The content of the framework code should be relevant to both sorts of information sharing.

The framework code is for use primarily in circumstances where information is being shared on a routine, systematic basis. However in some cases information is shared in a more ad hoc way. For example, a teacher might decide to share information with a social worker because there is concern about a particular child’s welfare. The framework code is not intended for use in circumstances like that, although professionals may still find it useful.

How to use the framework code of practice.

This framework should be used by organisations that want to produce their own codes of practice for sharing information. It says what content a code of practice should have if it is to support good practice in the sharing of personal information. Organisations using the framework code must populate it with their own detailed content, reflecting their own business needs. Where a number of organisations are working collaboratively on an information sharing project, it is important that any codes of practice do not contradict each other or overlap confusingly. In many cases it is best to have a single code of practice that all the organisations involved in the information sharing comply with.

We recognise that different organisations have different needs, depending on the sort of information sharing they’re involved in. Some of the framework’s content won’t be relevant to some organisations. We expect a considerable degree of flexibility in how the framework is used. For example, some organisations will use it to produce a stand-alone document, whilst others may want to integrate some or all of its content into their existing policies and procedures. The content of this document could also be used as a checklist for an organisation to evaluate its existing policies and procedures.

The Information Commissioner will endorse a code of practice based on the framework provided it addresses all its substantive content. For a code to be meaningful it must be adhered to in practice. In order to provide an endorsement we would normally expect an organisation to agree to our auditing compliance with its code.

Drawing up a code and following its recommendations in practice cannot guarantee compliance with the Data Protection Act 1998. However, adherence to a properly drafted code of practice would constitute a significant step to achieving compliance with the Act.

Each part of the framework code begins with a clear statement of what the Act requires. However, some of the content of the framework code goes beyond the strict legal requirements of the law. We have done this as part of our statutory duty to promote good practice in the handling of personal information.

Code of practice recommended content:

1. Deciding to share personal information

The law:

Any information sharing must be necessary. Any information shared must be relevant and not excessive.

Your code of practice should:

1. Set out why you want to share personal information.
2. Provide for a realistic appraisal of the likely effect of the sharing on the people the information is about, and of their likely reaction to it.
3. Describe the information that you need to share to achieve your objective and the organisations that need to be involved.
4. Outline the relevant statutory provisions, if your organisation is legally required, or permitted, to share information or is prevented from doing so.
5. Address any issues that might arise as the result of sharing confidential or sensitive information.
6. Say whether individuals' consent for information sharing is needed and if so, how to obtain consent and what to do if consent is withheld.
7. Give advice on finding alternatives to using personal information.

Points to remember:

1. Before you start sharing information you should decide and document the objective that it is meant to achieve. Only once you have done this can you address other data protection compliance issues, for example deciding what information is relevant.
2. This process is often termed a 'privacy impact assessment'. It should assess any benefits that the information sharing might bring to society or individuals. It should also assess any negative effects, such as an erosion of personal privacy, or the likelihood of damage, distress or embarrassment being caused to individuals. It should determine ways to avoid or minimise the unwarranted detrimental effects on individuals.
3. Only relevant information may be shared. Another organisation should not be allowed to have access to all the information you hold. You should work out which information items may be shared and who with. This should be reviewed regularly to prevent the sharing of information that is not relevant to achieving your objective. Where you are

sharing information internally, for example within a local authority, the same considerations apply. If only certain departments are involved in providing the service that the information sharing is intended to support, only those departments should have access to the information.

4. Some organisations are required by law to share information for certain purposes, for example as part of a local crime reduction partnership. In such cases you must be clear about what information you are required to share and in what circumstances. If you are unclear about this you should seek legal advice. Other organisations are permitted to share information, for example where this is necessary for a local authority to carry out its functions. In some cases an organisation may be expressly prohibited from sharing the information they hold. Such organisations must be clear about the nature of any such prohibition. Again, if necessary, legal advice about your powers should be obtained.
5. The threshold for sharing confidential or sensitive information is generally higher than for sharing other forms of information. This is because the unnecessary or inappropriate sharing of this sort of information is more likely to cause damage, distress or embarrassment to individuals. Some information is so sensitive, for example that contained in a health record, that in normal circumstances a patient's explicit consent must be obtained if you want to share or use it for a purpose other than healthcare.
6. Sometimes data protection law only requires that the individual knows about the sharing of information, it is not always necessary to obtain his or her consent for this. However, if you decide that you do need consent, this must be specific, informed and freely given agreement. A failure to object does not constitute consent. Most importantly, the individual must understand what is being consented to and the consequences of giving or withholding consent. If you are relying on consent to share information about a person, you must stop doing so if consent expires or is withdrawn. You must be clear with members of the public about the role that consent plays in your information sharing. In this context, consent is not genuine unless its withdrawal leads to the information sharing being stopped.
7. It is not justified, in data protection terms, to share information that identifies people when anonymised or statistical information could be used. This sort of approach can help to protect personal privacy whilst still allowing organisations to carry out their functions. In some planning contexts, for example, it may only be necessary to use general demographic information about people living in certain areas, rather than identifiable individuals' names, addresses and dates of birth.

2. Fairness and transparency

The law:

Personal information shall be processed fairly. When you obtain information from a person the processing won't be fair unless:

- you say who you are, unless this is obvious
- you say what purpose the information will be processed for
- you provide any other information necessary to enable the processing to be fair.

Your code of practice should:

1. Give guidance on the drafting of 'fair processing notices'.
2. Advise on ensuring notices are actively provided or, at least, freely available to the people you want to share information about.
3. Ensure that 'fair processing notices' give a genuinely informative explanation of how information will be shared and that they are updated when necessary.
4. Provide for ways of dealing with requests for further information and enquiries from members of the public
5. Help to ensure that explanations are given of the circumstances in which information may be shared without the individuals' knowledge or consent

Points to remember:

1. Fair processing notices, or 'privacy policies' as they are sometimes known, are intended to inform the people the information is about how it will be shared and what it will be used for. This means that notices have to be drafted in a way that the people it's aimed at will understand. Drafting notices for children and others whose level of understanding may be relatively low requires particular care. You should avoid legalistic language and adopt a plain-English, readable approach. Ideally, your code of practice should contain examples of model fair processing notices.

You must decide whether a single fair processing notice is sufficient to inform the public of all the information sharing that your organisation carries out. In some cases it would be good practice to produce a separate fair processing notice for a particular information sharing initiative. This would allow much more detailed and specific fair processing information to be provided. In other cases a more general notice could suffice.

2. A fair processing notice is meaningless unless people can read it and understand it. At least, you should make sure your fair processing notice is readily available. You should try, though, to actively provide fair processing notices to people, for example when you hold meetings with them or send out a letter. You should normally provide 'fair processing' information when you first obtain information about a person.

Where you intend to share confidential or particularly sensitive information you should actively communicate your fair processing information.

3. Information sharing arrangements can be quite complicated, with different sorts of information being shared between various agencies. However, you have to give a comprehensive and accurate description of what information is being shared and who it's being shared with. An information sharing arrangement can change over time, for example where a public body is placed under a new statutory duty to share information to deal with a particular problem. This requires the public body to periodically review its fair processing information to ensure that it still provides an accurate description of the information sharing being carried out.

- It can be useful to adopt a 'layered' approach to providing fair processing information. This involves having a relatively simple explanation backed up by a more detailed version for people who want a more comprehensive explanation. This can be done fairly easily in online contexts.

4. Sometimes people will have queries about how information about them is being shared, or may object to this. It is good practice for organisations to have systems in place for dealing with enquiries about information sharing in a timely and helpful manner. The analysis of queries and complaints should help you to understand public attitudes to the information sharing you're carrying out, and to make any necessary improvements.

5. This can only happen in limited circumstances, for example where telling someone about the disclosure of information would lead to a crime going undetected or to an individual suffering harm. However, you should be prepared to be open with the public about the types of circumstance in which information may be disclosed without their knowledge or consent.

3. Information standards

The law:

Information shall be adequate, relevant, not excessive, accurate and up to date.

Your code of practice should contain:

1. Procedures for checking that information is of good enough quality before it is shared.
2. Methods for making sure that shared information is recorded in a compatible format.
3. Methods for checking periodically that shared information is of sufficient quality.
4. Procedures for ensuring that any information that is being shared is relevant and not excessive.
5. Methods for making sure that any problems with personal information, e.g. inaccuracy, are also rectified by all the organisations that have received the information.

Points to remember:

1. It is good practice to check the quality of the information before it is shared, otherwise inaccuracies and other problems will be spread across information systems. In general, any plan to share information should trigger action to ensure that inaccurate records are corrected, irrelevant ones weeded out, out of date ones updated and so forth.
2. Different organisations may record the same information in different ways. For example, a person's date of birth can be recorded in various formats. This can lead to records being mis-matched or becoming corrupted. Before sharing information you must make sure that the organisations involved have a common way of recording key information, for example by deciding on a standard format for recording people's names. If a common standard for recording information cannot be established, a robust means of conversion must be deployed.
3. Only once you have a clearly defined objective, for example the delivery of a particular service, can you make an informed decision about the information that is necessary to carry out that objective. You should be able to justify the sharing of each item of information on the grounds that its sharing is necessary to achieve the objective. You must not share information if it is not necessary to do so. It is good practice to periodically review the information sharing and to check that all the information being shared is necessary to achieving your objective. Any unnecessary sharing of information should cease. However, in

some contexts it is impossible to determine with certainty whether it is necessary to share a particular piece of information. In such cases, experience and professional judgement must be relied on.

4. It is good practice to check from time to time whether the information being shared is of good enough quality. For example, a sample of records could be looked at to make sure the information contained in them is being kept up to date. It is a good idea to show the records to the people they are about so that the quality of information on them can be checked. Although this may only reveal deficiencies in a particular record, it could indicate wider systemic failure that can then be addressed.
5. The spreading of inaccurate information across a network can cause significant problems for individuals. If you discover that you have shared inaccurate information, you should not only correct your own records but ensure that the information is also corrected by others holding it. You need to have procedures in place for dealing with situations where there are disagreements between organisations about the accuracy of a record. In some cases, the best course of action might be to ask the individual him or herself whether their record is correct.

4. Retention of shared information

The law:

Personal information shall not be kept for longer than is necessary.

Your code of practice should:

1. Specify retention periods for the different types of information you hold, including retention times for the various items held within a record.
2. Provide for the periodic review of retention periods, based on assessment of business need.
3. Set out any legal requirements or professional guidelines relevant to the retention or disposal of the information you hold.
4. Ensure that any out of date information that still needs to be retained is not permanently deleted is safely archived or put 'offline'.
5. Specify whether information supplied by another organisation should be deleted or returned to its supplier.
6. Provide a mechanism for ensuring that your retention procedures are being adhered to in practice.

Points to remember:

1. Automated systems can be used to delete a specific piece of information after a pre-determined period. Such a facility is particularly useful where a large number of records of the same type are held.

Considerations for judging retention periods include:

- the current and future value of the information for the purpose for which it is held
- the costs, risks and liabilities associated with retaining the information
- the ease or difficulty of ensuring the information remains accurate and up to date.

2. You should review your retention policy in the light of operational experience. If records that are being retained are not being used, this would call into question the need to retain them.
3. For example, there are various legal requirements and professional guidelines relating to the retention of health records.

4. There is a significant difference between permanently, irreversibly deleting a record and merely archiving it. If you merely archive a record or store it 'offline' it must still be necessary to hold it and you must be prepared to give subject access to it and hold it in compliance with the data protection principles.
5. The various organisations sharing information should have an agreement about what should happen once the need to share the information has passed. In some cases the best course of action might be to return the shared information to the organisation that supplied it without retaining a copy. In other cases, for example where the particular issue that information sharing was intended to deal with has been resolved, all the organisations involved should delete their copies of the information.

If information you hold should be deleted, for example because it no longer serves a useful purpose or has a statutory retention period that has been exceeded, you must make sure that any organisation that has a copy of the information also deletes it. It might be possible to anonymise the information, in which case it can be retained indefinitely.
6. A good way to do this is to periodically audit the personal information you hold to ensure that information is not being retained for too long or deleted prematurely.

5. Security of shared information

The law:

Personal information shall be protected by appropriate technical and organisational measures.

Your code of practice should:

1. Describe ways of evaluating the level of security that needs to be in place.
2. Set out standards for the technical security arrangements that must be in place to protect shared information.
3. Describe the organisational security arrangements that must be in place to protect shared information.

Points to remember:

1. Your key consideration should be to ensure that your security is adequate in relation to the damage to individuals that a security breach could cause. More sensitive or confidential information therefore needs a higher level of security. However, rather than having different security standards for different pieces of information, it might be easier to adopt a 'highest common denominator' approach, i.e. to afford all the information you hold a high level of security. A good approach is for all the organisations involved in information sharing to adopt a common security standard, e.g. ISO17799 or ISO27001.
2. A difficulty that can arise when information is shared is that the various organisations involved can have different standards of security and security cultures. It can be very difficult to establish a common security standard where there are differences in organisations' IT systems and procedures. Problems of this sort should be addressed before any personal information is shared. It is the responsibility of the organisation providing the information to be shared to ensure that it will continue to be protected by sufficient security once other organisations have access to it.
3. Different organisations may have different cultures of security, and considerations similar to those outlined in the point above apply. Again, it is important that any relative weaknesses in an organisations' security are rectified, for example by carrying out inter-organisational training, before any personal information is shared between them. Where an organisation employs another organisation to process personal information on its behalf, a contract must be in place to ensure the information remains properly protected.

6. Access to personal information

The law:

Individuals have a right of access to information about them.

Your code of practice should:

1. Set out ways for making sure people can gain access to information about them easily.
2. Provide alternative ways for giving people access to their records.
3. Describe ways of making sure that a person gets access to all the information he or she is entitled to.
4. Give guidance on advising the public about the uses, sources and disclosures of information about them.
5. Provide guidance about relevant exemptions from the right of subject access, i.e. cases where information will be withheld from a person who makes a request for access.

Points to remember:

1. Where information is being shared between a number of organisations it can be difficult for people to work out how to gain access to all the information that's held about them. It is good practice to provide a single point of contact for people to go to when they want to access their information, and to make people aware of this facility.
2. Organisations are required by law to give people access to information about them. A fee of £10 can be charged and access must be given within 40 calendar days. However, it is good practice to provide faster, cheaper ways for people to gain access to information about them. This could be done by showing people their records when you come into contact with them or by setting up facilities to allow records to be viewed securely online.
3. When personal information is shared between several bodies it can be difficult to determine what information is held. It's very important, therefore, that organisations sharing information adopt good records management practices, to allow them to locate and provide all the information held about a person in the event of an access request being made.

4. When a request for personal information is made, the organisation is required by law to also describe the purposes for which the information is held and its recipients, i.e. who it is disclosed to. This part of the right of subject access is particularly important in the context of information sharing. You are also required to provide the individual with any information you have as to the information's source. In some cases information about someone may have been provided by another individual. This might be the case, for example, where a child's social work file contains information provided by a concerned neighbour. In cases like that, information about the source should normally be withheld.
5. Whether or not an exemption applies depends on the information in question, and in some cases on the effect that releasing the information would have on the individual. However, organisations dealing with a particular type of record are likely to find that they wish to rely on the same exemptions in respect of the access requests they receive. If this is the case, it would be useful to provide detailed advice to staff about how a particular exemption, or exemptions, work. It is good practice to be as open as possible with the public about the circumstances in which you will withhold information from them. In some cases this will not be possible, for example where telling a person that you hold exempt information about them would prejudice the purposes of law-enforcement by 'tipping off' an individual that he or she is being investigated.

7. Freedom of Information

The law:

The Freedom of Information Act 2000 gives everyone the right to ask for information held by a public authority, to be told whether the information is held, and, unless exempt, to have a copy of the information.

Your code of practice should:

1. Encourage the inclusion of material about information sharing in your FOI publication scheme.
2. Give advice on providing assistance to members of the public who make requests for a mixture of personal and non-personal information.

Points to remember:

1. Most, if not all, public sector bodies involved in sharing information are covered by the Freedom of Information Act. This means they are required to include various information that they hold in their FOI publication scheme. It is good practice to include the 'paperwork' relating to information sharing in the publication scheme, including any relevant code of practice. There is a strong public interest in members of the public being able to find out easily why information is being shared, which organisations are involved and what standards and safeguards are in place.
2. Often people will make requests for information that cover both personal and non-personal information. For example, a person may request information about them that is being shared between various agencies and information about those agencies' policies for sharing information.

Data protection and freedom of information may be dealt with by separate parts of your organisation, and a hybrid request may have to be dealt with under both pieces of legislation. However, it is good practice to be as helpful as possible when dealing with requests of this sort, especially as members of the public may not understand the difference between a data protection and an FOI request.

(This framework code of practice does not contain recommendations about the handling of mainstream freedom of information requests. The Information Commissioner has published comprehensive advice about this elsewhere.)

8. Review

You should keep your information sharing procedures under review, and should update your documentation when necessary. Codes of practice and other documentation can soon become out of date, given the rapid changes that can take place in an organisation's information sharing practices.

In particular, you should check whether:

1. Your fair processing notices still provide an accurate explanation of your information sharing activity.
2. Your procedures for ensuring the quality of information are being adhered to and are working in practice.
3. Organisations you are sharing information are also meeting agreed quality standards.
4. Retention periods are being adhered to and continue to reflect business need.
5. Security remains adequate and, if not, that any security breaches have been investigated and acted upon.
6. Individuals are being given access to all the information they are entitled to, and that they are finding it easy to exercise their rights.
7. Your FOI publication scheme is being kept up to date.

Appendix 1 – Other relevant guidance from the Information Commissioner, available at www.ico.gov.uk

- Sharing personal information: Our approach. (A general position paper on information sharing.)
- The use of personal information held for collecting and administering Council Tax.
- Data sharing between different Local Authority departments.
- The use and disclosure of information about business people.
- The Crime and Disorder Act 1998: data protection implications for information sharing
- Sharing information about you. (Gives advice to the public about information sharing.)

If you would like to contact us please call 08456 306060, or 01625 545745
if you would prefer to call a national rate number.

e: mail@ico.gsi.gov.uk

w: www.ico.gov.uk



August 2007

Information Commissioner's Office
Wycliffe House, Water Lane
Wilmslow, Cheshire SK9 5AF

