Framework code of practice for sharing personal information

Promoting public access to official information
and protecting your personal information

Information Commissioner's Office

Content

Information Commissioner's foreword

Sharing information can bring many benefits. It can support more efficient, easier to access services. It can help to make sure that the vulnerable are given the protection they need, that organisations can cooperate to deliver the care that those with complex needs rely on. Law enforcement agencies must have access to the information they need to counter the increasingly sophisticated methods that fraudsters and other types of criminal are using. Our time is valuable. No one likes being asked to provide the same information over and over again. No one wants to discover that their doctor doesn't have access to relevant information about their health.

Sharing information presents risks. Information systems are becoming more complex and widespread. There is a potential for more information about our private lives, often highly sensitive, to become known to more and more people. There is a danger that the public will be left behind, subject to opaque information systems that they do not understand and that they have no control over. No one wants a huge database of personal information that anyone can access for any, ill-defined purpose.

This framework code of practice can be used in various ways in a variety of contexts. It contains simple, practical advice that will help all those involved in information sharing to develop the knowledge and confidence to make good quality decisions about sharing personal information. This framework code of practice will help to make sure that the benefits of information sharing are delivered, while maintaining public trust and respecting personal privacy.

Richard Thomas
Information Commissioner

About the framework code of practice

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 Act).
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 throughout the UK, including voluntary bodies. However, some of it will be of most relevance to public sector organisations. The framework code should be of use even where there is a statutory requirement to share information. Using the framework code will help organisations to make sure that they address all the main data protection compliance issues that are likely to arise when sharing information. This in turn should help organisations and their staff 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 consistent 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 gain the trust of the public and make sure 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, following good practice should make your information sharing more effective, allowing better services to be provided to the public. It should also enhance the reputation of your organisation in the eyes of the people you keep 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 other's information systems or by setting up a separate shared database. This may lead to the specific disclosure of a limited amount of information on a one-off basis or the regular sharing of large amounts of information, for example bulk matching name and address information in two databases. 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 types of information sharing.

The framework code is for use mainly 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 use his or her professional judgement to decide to share information with a social worker because there is concern about a particular child's welfare. The framework code is not primarily intended for use in cases like that, although it may still be of use if read alongside the relevant professional guidance.

How to use the framework code of practice

Your organisation's needs

This framework code 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 fill it in 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 work to.

We recognise that different organisations have different needs, depending on the sort of information sharing they're involved in. We anticipate a considerable degree of flexibility in how the framework is used. For example,

- it can be used to produce a stand-alone document
- some or all of its content can be integrated into existing policies and procedures; or
- it can be used as a checklist to evaluate existing policies and procedures.

We hope that the framework code will help organisations to design their own solutions to the compliance issues they face. However, the Information Commissioner's Office is willing to provide further advice and assistance when this is needed.

Endorsement

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. To provide an endorsement we would normally expect an organisation to agree to us auditing compliance with its code.

The framework code and compliance with the law

Drawing up a code and following its recommendations in practice cannot guarantee compliance with the Data Protection Act 1998. However, adhering to a properly drafted code of practice would be a significant step towards 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. The legal requirement is to comply with the law. No action can be taken over a failure to adopt good practice or to act on the recommendations of the framework code.

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 do the following.

1. Set out why you want to share personal information and what benefits you expect to achieve.
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. Give advice on finding alternatives to using personal information, for example using statistical information.
4. Describe the information that you need to share to achieve your objective and the organisations that need to be involved.
5. Outline the relevant legal provisions, that require or permit your organisation to share information, or prevent it from doing so.
6. Address any issues that might arise as the result of sharing confidential or sensitive information.
7. Say whether individuals' consent for information sharing is needed and, if so, how to obtain consent and what to do if consent is withheld.

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 whether you need to share information in a personally identifiable form, or whether anonymised or statistical information would be enough.

   You should determine right at the beginning of a project who will be responsible for dealing with the various compliance issues that will arise. All the organisations involved will have some responsibility. However, the organisation that originally collected the information has the primary responsibility for making sure it is handled properly. In particular, that organisation must make sure that sharing its information will not cause real unfairness or unwarranted detriment to individuals.

2. This can be done by carrying out a 'privacy impact assessment'. This involves assessing any benefits that the information sharing might bring to society or individuals. It also involves assessing any negative effects, such as an erosion of personal privacy, or the likelihood of damage, distress or embarrassment being caused to individuals. It should help to avoid or minimise the risk of any detriment being caused.

3. It is not justified to share information that identifies people when anonymised or statistical information could be used as an alternative. This sort of approach can protect personal privacy while 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.

4. Only relevant information and the minimum necessary to achieve the objective may be shared. You should review your arrangements 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.

5. Some organisations are required by law to share information for a particular purpose. In these 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 get legal advice. Other organisations are allowed 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. These organisations must be clear about the nature of any such prohibition. Again, if necessary, you should get legal advice about your powers.

   Many public sector organisations are bound by the European Convention on Human Rights. This means that any information sharing they carry out must be compatible with the convention, in particular the right to respect for private and family life. Organisations should also take into account any relevant professional guidance or industry code.

   You should regularly check your notification under the Act to make sure that it describes any organisations you are sharing information with.

6. 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 non-medical purpose.

7. 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 to legitimise your processing of information, this must be a specific, informed and freely given agreement. In this context, a failure to object is not 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.

2. Fairness and transparency

The law

Personal information shall be processed fairly. The processing won't be fair unless the person has, is provided with, or has readily available:

- information about your identity
- information about the purpose the information will be processed for, and
- any other information necessary to enable the processing to be fair.

Your code of practice should do the following.

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 a notice has 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, easy-to-read approach. Ideally, your code of practice should contain examples of model fair processing notices.

   You must decide whether a single fair processing notice is enough 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 be enough. An existing notice may already explain all the information sharing you are engaged in. If this is the case, no further action is needed.

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 proactively, though, to 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 review its fair processing information regularly to make sure 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 on-line contexts.

4. Sometimes people will have questions 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 questions and complaints should help you to understand public attitudes to the information sharing you're carrying out, and to make any necessary improvements.

5. There are cases where it is legitimate to share information without a person's knowledge or consent. This might be the case where a failure to share information about a parent's lifestyle would put a child at risk. There are also other situations where information should be shared despite a lack of consent, for example, where the sharing is necessary to safeguard public safety in an emergency situation. In many criminal justice contexts it is not feasible to get consent, because doing so may prejudice a particular investigation. However, you should be prepared to be open with the public about the sorts of circumstances in which you may share information 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 the following.

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. Procedures for making sure that any information that is being shared is relevant and not excessive.
4. Methods for checking regularly that shared information is of sufficient quality.
5. Methods for making sure that any problems with personal information, for example, 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 make sure that inaccurate records are corrected, irrelevant ones weeded out, out-of-date ones updated and so on. It is not always possible to check the accuracy of every record: in these cases a sample of records should be checked.

   There should be mechanisms in place to help organisations to resolve problems where there is disagreement over an information quality issue.

   The exchange of information in paper form can cause particular problems. It can be very difficult to make sure that an organisation's collection of paper records is corrected once an inaccuracy is detected.

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 mismatched 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 you cannot establish a common standard for recording information, you must develop a reliable means of converting the information.

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 regularly review the information sharing and to check that all the information being shared is necessary for 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 these cases, you must rely on experience and professional judgement.

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 make sure 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 whether his or her 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 do the following.

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 regular 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. Make sure that any out-of-date information that still needs to be retained but is not permanently deleted is safely archived or put 'off-line'.
5. Specify whether information supplied by another organisation should be deleted or returned to its supplier.
6. Provide a mechanism for making sure 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. This 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; and
   - the ease or difficulty of making sure 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. It can be very difficult to assess the significance of the information you hold. In these cases you must rely on experience and professional expertise to come to a balanced decision about whether to retain or delete the information.

3. For example, there are various legal requirements and professional guidelines relating to the retention of health records. There may also be a legal requirement to keep an audit trail for a certain period of time.

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 'off-line' it must still be necessary to hold it and you must be prepared to give subject access to it and comply with the data protection principles. If it is appropriate to delete a record from your live system you should also delete it from any back-up of your information you keep.

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 the information sharing was intended to deal with has been resolved, all the organisations involved should delete their copies of the information. Paper records can cause particular problems. It can be easy to overlook the presence of old paper records in archives or filing systems.

   The various organisations involved in an information sharing initiative may need to set their own retention periods for information. However, if shared information should be deleted, for example because it is no longer relevant for the initiative's purposes, then all the organisations with copies of the information should delete it. If the information 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 regularly audit the personal information you hold to make sure 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 do the following.

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 make sure 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, that is, 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, for example, ISO17799 or ISO27001. Adopting the Government Protective Marking Scheme can also help organisations to make sure there is consistency when handling personal information.
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. You should address problems of this sort before you share any personal information. It is the primary responsibility of the organisation providing the information to be shared to make sure that it will continue to be protected by adequate security once other organisations have access to it. There should be arrangements in place that set out who is allowed to access or alter a record.
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 organisation's security are rectified. This could be done by the organisations involved delivering a common training package, 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 make sure the information remains properly protected. In some cases, for example where very sensitive information is involved, staff may be subject to a vetting procedure. If vetting is justified, staff from other organisations that have access to the information should be subject to equivalent security procedures.

6. Access to personal information

The law

Individuals have a right of access to information about them.

Your code of practice should do the following.

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, that is, 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 in a permanent form. For most records, you can charge a fee of £10 and you must give access 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 on-line.
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 when they receive an access request.

4. When an organisation receives a request for personal information, it is required by law to also describe the purposes for which the information is held and its recipients, that is, 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 and the Freedom of Information (Scotland) Act 2002 give 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 do the following.

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.

   Making your 'paperwork' available to the public proactively should help to reassure individuals and to establish an increased level of trust and confidence in your organisation's information sharing practices.

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

It is very important to regularly assess whether your sharing of information is having the desired effect, for example in terms of reducing crime or providing a more efficient service to the public. When assessing your information sharing it is also important to consider any complaints or questions that you have received from members of the public.

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

When something goes wrong, for example, a security breach, it is important to find out the cause of this and to take action to prevent it happening again.

In particular, you should check whether:

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

Appendix 1 –
The data protection principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless;

   (a) at least one of the conditions in Schedule 2 is met; and

   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2 Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4 Personal data shall be accurate and, where necessary, kept up to date.

5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6 Personal data shall be processed in accordance with the rights of data subjects under this Act.

7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

This is not a full explanation of the principles. For more information, see our Legal Guidance.

Appendix 2 – Example of a simple information sharing procedure

Procedure for sharing information between Newtown Constabulary, Reporter to the children's panel and social work departments.

1 Contact details

1.1 Named individuals in Council Social Work departments and Area Children's Reporters.

2 Types of information

2.1 Child Protection Initial Report Form NM/59/2 to be sent to appropriate Social Work Department and Children's Reporter. These will be marked CONFIDENTIAL.

2.2 Memoranda as required. These will always be marked CONFIDENTIAL.

2.3 Crime reports may also be disclosed.

2.4 Verbal information will be shared at case conferences. This information will be either RESTRICTED or CONFIDENTIAL. Minutes should be classified according to the value of information in them.

3 How to handle the information

3.1 Transmission

3.1.1 RESTRICTED information can be transmitted over the telephone or sent by fax. CONFIDENTIAL information must be sent in a double envelope with the protective marking shown on the inner one.

3.2 Storage

3.2.1 All information must be kept under lock and key when not in the personal custody of an authorised person. The "need-to-know" principle will be strictly enforced. CONFIDENTIAL information needs to be protected by two barriers, for example, a locked container in a locked room.

3.3 Release to third parties

3.3.1 No information provided by partners to these procedures will be released to any third party without the permission of the owning partner.

Appendix 3 – 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.)
- 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. (Advice to the public about information sharing.)

Appendix 4 –
Other sources of advice and guidance

Audit Commission: www.audit-commission.gov.uk

Cabinet Office: www.cabinetoffice.gov.uk

Chief Information Officer Council: www.cio.gov.uk

Communities and Local Government: www.communities.gov.uk

Department for Children, Schools and Families: www.dfes.gov.uk

Department of Health : www.dh.gov.uk

Essex Trust Charter: www.essexinformationsharing.gov.uk

Improvement Service: www.improvementservice.org.uk

London Connects: www.londonconnects.gov.uk

Ministry of Justice: www.justice.gov.uk

National Archives: www.nationalarchives.gov.uk

Public Record Office of Northern Ireland: www.proni.gov.uk

Records Management Society: www.rms-gb.org.uk

Society of Archivists: www.archives.org.uk

The Scottish Government: www.scotland.gov.uk

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

October 2007

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

Information Commissioner's Office