

Sharing Personal Information and the Data Protection Act

A corporate guide to creating Information Sharing Protocols

Contents

- Introduction
- Developing an Information Sharing Protocol
- Key Components
- Approval, Implementation and Review

Appendix A

Explanation of terms used

Appendix B

Consent

Appendix C

Information Management Group members

NB: This guide has been developed by Worcestershire County Council, building on advice from the Central Government Department for Constitutional Affairs and from Solihull Metropolitan Borough Council

Introduction

Sharing Personal Information

We are increasingly encouraged to provide efficient, effective services by working more closely within our own organisation and with other bodies. The arrival of e-government is a major driver in requiring us to manage customer information well, across different organisations. By joining up our information resources, we can deliver a better service to the public. Often, this involves sharing personal information about individuals. The benefits are clear; a one stop shop for consumers. A unified public face with strong communication behind the scenes.

Whenever personal information is shared, the rights and freedoms of individuals should be respected. The Data Protection Act (DPA) exists to ensure that we *can* share personal information, without compromising the rights of individuals. The Performance and Innovation Unit, (part of Central Government's Cabinet Office) produced a report in 2002 entitled *Privacy and Data Sharing*, which recommends the creation of Information Sharing Protocols, to set a clearly defined framework within which personal information can be shared fairly and lawfully.

What is an Information Sharing Protocol?

An Information Sharing Protocol is effectively a contract between organisations (or sometimes between distinct parts of one organisation) who wish to share personal information. The contract agrees the personal data that are to be shared, the specific purposes for the sharing and sets restrictions on the uses of that information. Responsibilities are agreed and the Protocol should be signed by each Partner.

Information Sharing Protocols can only be developed in accordance with legislation and do not override the need for personal data to be shared lawfully. Most importantly, you must ensure you have the legal vires to carry out your information sharing project. This is covered by Step 6 of the Toolkit.

When are Information Sharing Protocols necessary?

Information Sharing Protocols are usually created when a number of agencies wish to make use of their clients' personal data, to meet a government driven initiative to improve service delivery. In general terms, if you intend to share personal data with another body/another part of WCC and/or there is a new purpose for which you wish to use personal data, the arrangements *may* need to be formalised in an Information Sharing Protocol. Check with the Data Protection Officer (DPO) (see Appendix C) to find out if a Protocol has already been created which may suit your purposes, or if the Protocol route is necessary at all. Protocols should be developed in liaison with the DPO or your Directorate Administrative Manager. See Appendix A for an explanation of some of the terms used in this guidance.

Developing an Information Sharing Protocol

To ensure consistency across WCC in approaching information sharing, this guidance should be used as a basic toolkit for creating and maintaining all Sharing Protocols. Once the 10 steps have been followed, you should have the mandatory key components for an Information Sharing Protocol.

10 Steps to creating an Information Sharing Protocol

1. Identify all Partners with whom personal data are to be shared

- 1.1 Consider both internal and external and current and potential partners
- 1.2 Form a working group to create the Protocol
 - Include senior representation – commitment to the task is necessary for the Protocol to be followed
 - Include consultation with operational staff. The Protocol must be workable in practice
 - Liaise with DPO/Directorate Administrative Manager as appropriate
 - All Partners and potential Partners should be involved from the start
- 1.3 Identify the status of each partner with regards to the personal information being shared. Who are the Data Controllers? Who are the Data Processors? (See Appendix A for explanations). Data Controllers have responsibilities for
 - setting the conditions of use
 - notifying with the Information Commissioner, via the DPO
 - responding to requests for access.
- 1.4 Determine how the Protocol will be approved by each Partner (see later section: Approval, Implementation and Review)

2. Determine the scope of the information sharing project

- 2.1 If the project involves a variety of partners and a number of data-categories (ie: types of personal data held), there may be too much detail for one Protocol. Instead, an *overarching Information Sharing Protocol* should first be developed, to which all parties agree. This sets the overall framework for sharing.
- 2.2 An overarching Protocol should include the following: (NB: The terms below are explained in more detail throughout this guidance)
 - List of all partners
 - Reason driving the data-sharing project
 - List of purposes of the project
 - List of types of data-categories involved (types may include: basic personal details, medical details, crime details)

- Condition under DPA by which sharing can occur
- Security standard
- Records management standard (ie: retention, destruction) (for advice, please contact WCC Modern Records Unit on *****
*****)
- Overall responsibilities for informing the data subjects, dealing with complaints and subject access requests, ensuring accuracy
- Review date
- List of individual protocols which sit within this overarching one
- Signatures of all Partner bodies (senior level)
- Definitions of terms used in the Protocol

2.3 *Individual Protocols* would then sit within the overarching agreement and would identify specifically which data is to be shared and who can have access, setting conditions accordingly. For example, a project between WCC, District Councils, Police and Health may have several purposes and an individual protocol may be needed for each purpose.

2.4 Steps 3-10 should be applied as appropriate to either an overarching Protocol and/or a specific Protocol.

3. Establish the purposes for and method of data sharing

3.1 List the overall purposes of the project. Eg:

- To provide a support service for elderly victims of crime
- To provide information to Age Concern about crime trends

3.2 Plan out an overview of how the project will work in practice. Eg:

- Police victim support service is offered to all victims of crime
- Police Victim Support staff visit those who take up the service
- Personal data on elderly people is passed to WCC Social Services for follow up support to be provided
- WCC Social Services pass personal data to Age Concern

3.4 Through process mapping the project, data sharing areas are flagged and questions can be asked. Where can risks be minimised above?

- Do victims of crime know that their personal data may be passed to two more bodies when they take up the support service? Can they opt out of this transfer (is it necessary for the support)?
- Do Age Concern need personal data or can the information be anonymised? Frequently, statistical data is all that is necessary. Principle 3 of the Data Protection Act says information should be relevant and not excessive for the purposes. Whenever personal data is processed, what is the minimum amount necessary for the operation?

3.5 At this point, the purposes should be clearly outlined and the methods of transfer refined. This will be a useful basis for the next 7 steps.

4. List the categories of data to be shared

4.1 The overview now needs to be broken down further. For each purpose identified, the exact categories of data collected and shared should be listed, with initial thoughts on conditions of disclosure. This table provides an example:

Figure 1

Purpose	Data categories	Parties involved and roles:			
		Police attending crime	Police Victim Support Section	WCC Social Services	Age Concern
1. Provide support to elderly crime victims	Basic person details: names, addresses, age, gender	Obtained	Received from Police attending crime (if consent?)	Received from Police Victim Support (if consent?)	
	Crime details: Offence details, crime number (Note: This is sensitive personal data)	Obtained	Received from Police attending crime (if consent?)	Received from Police Victim Support (if consent?)	
2. Crime trends	Basic person details: name, addresses, age, gender	Obtained	Received from Police attending crime (if consent?)	Received from Police Victim Support (if consent?)	Statistics <i>not names</i> received from SS. (Addresses broadened to geographical area)

4.2 The table should contain

- Each purpose of the project
- The data categories involved in each purpose
- The roles of the various agencies involved (ie: obtainer, recipient) for each data category

4.3 Although this may seem a laborious process, it will clearly show *why* data is being shared, *what* is being shared, *to whom* it is being disclosed and *where* conditions need to be established/changes need to be made to the data before it is passed on.

4.4 Section 4 is necessary but, in a large project, may be appropriate at the level of Individual Protocols and not as part of an overarching information sharing agreement.

5. Establish conditions/restrictions on the use of the personal data

5.1 The table in *Figure 1* enables us to ask the following questions about specific data sharing activities. Aim to answer Yes to each question in the checklist:

- Is what is shared for each data category relevant to the particular purpose? (Do not share excessive personal data) (DPA Principle 3)
- Is data collected adequate enough to be able to distinguish between people? (DPA Principle 3)
- Can we guarantee data is only collected and further used for the agreed purpose? (DPA Principles 1 and 2)
- Do we have retention periods for all personal data collected and can we be sure mechanisms are in place to destroy the data once its retention period has been reached? (DPA Principle 5). (WCC has a corporate retention schedule. Contact the WCC Modern Records Unit on ***** for more information)

NB: For DPA Principles, see Appendix A

5.2 Considering the above points, the table should be amended until all the answers to the above checklist are 'Yes'. You should further expand the table to add in limitations on use, retention criteria, to ensure adequacy or set extra conditions such as anonymity of personal data before it is passed on. For example,

Figure 2

Purpose	Data categories	Parties involved and roles:			
		Police SOC	Police Victim Support Section	WCC Social Services	Age Concern
1. Provide support to elderly crime victims	Basic person details: names, addresses, age, gender	Obtained -Gain all initials and check spellings. -Retain on PNC for x years	Received from SOC (if agree?) - Only use for Victim Support -Retain for 1y after close of case	Received from Police Victim Support (if agree?) - Only use for Victim Support follow up -Retain for x years after close of case	

6. Is the information sharing compatible with the Data Protection Act?

- 6.1 Even though the table defines how and why we want to share personal information, we still need to satisfy the requirements of the Data Protection Act. Ensure that your purposes are lawful and that your project is not ultra-vires. This means you must have the statutory power to share the data. We cannot use personal data for a secondary purpose if this would mean we are acting ultra-vires. For example, Council Tax data can only be used for the purpose of Council Tax administration. To use it for any other purpose would be unlawful. Information sharing should not contravene any legislation (such as Copyright law, Common law of Confidentiality, Human Rights Act). It is important to identify and list the statutory basis for the sharing.
- 6.2 Processing personal information (in whatever format), includes obtaining, using, disclosing, sharing, destroying. Whenever we process, we must meet a condition in Schedule 2 of the Act.
- 6.3 Does *each* processing operation within each purpose of your table (ie: each obtaining, each disclosure) meet one of the following conditions?

Schedule 2:

- Consent of data subject
 - Processing is necessary for a contract to which the data subject is party
 - Processing is necessary for compliance with a Data Controller's legal obligation
 - Processing is necessary to protect the vital interests of the data subject
 - Processing is necessary for the administration of justice, for the exercise of functions conferred by enactment, for functions of a public nature exercised in the public interest
 - Processing is necessary to satisfy the legitimate interests of the Data Controller/a third party, except where the processing is unwarranted by reason of prejudice to the rights and freedoms of the data subject
- 6.4 If sensitive personal data is being processed, a condition in Schedule 3 of the Act must *also* be met. Sensitive personal data, in the Data Protection Act, means personal data which relates to
- the racial/ethnic origin of the data subject
 - his/her political opinions
 - his/her religious or similar beliefs
 - his/her membership of a trade union
 - his/her physical or mental health or condition
 - his/her sexual life
 - the commission or alleged commission by him/her of an offence and any related proceedings

Therefore, in addition to Schedule 2, one of the following conditions must be met for each processing operation in your table if the processing involves a sensitive purpose/data category:

Schedule 3:

- Explicit consent of data subject
- Processing is necessary for Employment Law
- Processing is necessary to protect vital interests of data subject or another, where consent cannot be given or has been unreasonably withheld
- Processing is by a not-for-profit organisation and has safeguards to protect the rights and freedoms of individuals
- Processing is of information made public by deliberate action of data subject
- Processing is necessary for legal proceedings
- Processing is necessary for the administration of justice, for the exercise of functions conferred by enactment
- Processing is necessary for medical purposes, undertaken by a health professional
- Processing is of racial/ethnic origin data and is necessary to monitor equality of opportunity
- Processing is specified by order of Secretary of State

6.5 Which condition should be used?

- Consent is one option. The definition of consent is very important. Can you guarantee that
 - It is fully informed?
 - It is freely given?
 - It can be freely withdrawn?
 - It can be refreshed?

Consent should also be in writing and any withdrawal of consent must be communicated to all parties who are involved with that individual's personal data for that purpose. See Appendix B for a more detailed explanation of consent and a specimen consent form. Do *not* ask for consent if you intend to go ahead with the processing anyway. It should not be used as a first choice to be followed by other measures if the answer is 'no'. This would be unfair to the data subject and can only engender mistrust. If another condition in the Act can be found instead, it should be used. Consent should only be asked for when there is a genuine opportunity to refuse. (There is a difference between asking for consent and informing people what you are doing with their personal data. The latter is obligatory, unless an exemption applies – see Step 7).

- If the Schedule 2 (and 3) condition you wish to use is 'necessary for functions conferred by enactment', the actual basis for this should be found. Identify which specific part of the Statute you are relying upon and state it explicitly in the Protocol. To meet this condition,

the sharing must be necessary to meet the legislative requirement. For example, Section 115 of the Crime and Disorder Act states that anyone has the power to disclose information to a police authority/local authority if it is necessary for the purposes of crime prevention. This is not a licence to allow all sharing of all personal data in connection with crime. It is important to be aware that there is a difference between enabling and obliging legislation. (You may need to refer to Legal Services or the DPO (see Appendix C) to discuss this further).

- 6.6 Once you are sure that your processing is lawful and you can justify all your intended processing operations with a condition under Schedule 2 (and under Schedule 3 if it concerns sensitive personal data), the condition(s) should be an explicit statement in your Information Sharing Protocol. You should by now have satisfied two thirds of Principle 1 of the DPA. To satisfy the third arm, see Step 7

7. Inform the data subjects

- 7.1 Principles 1 and 2 of the DPA state that personal information must be *fairly obtained for specified purposes*. To be fair, we must be transparent. This means that when the data is first collected, the data subject must be told
- Who is collecting their information (the Data Controller)
 - For what purposes their personal details will be used
 - Anything else which is important to state in order to ensure they are fully informed (this will include any disclosures we plan to make)

Therefore, if we are collecting personal information for one reason (eg: to record a crime) and intend to use it for another (eg: to provide victim support), then we should tell them about both purposes. (This is a separate issue to gaining consent. You may wish to choose consent as your *condition* for sharing, but this is unconnected to the obligation to inform data subjects of the processing anyway). All of this information needs to be included in a *Fair Obtaining Notice* (see glossary in Appendix A) to the data subject prior to collection of their personal data. For advice on compiling a Fair Obtaining Notice, please ask the DPO (Appendix C)

- 7.2 There will be a limited number of situations when you will not have to be transparent. This means you do not have to tell the data subject what you are doing with their personal information. These situations are explicit in the Act. Examples of this are
- If by telling them, you would be likely to prejudice criminal proceedings
 - If by telling them, you would be likely to endanger their mental/physical health
- Before applying an exemption like this, or to find out more, you should consult with the DPO (see Appendix C).

- 7.3 For the purposes of the Sharing Protocol, it will be necessary to clarify who is responsible for telling the data subjects at the point of data collection about the identity of the data controller(s), the purposes of the collection and anything else deemed necessary (such as all the disclosures). This responsibility should be made explicit in the Protocol.

8. Dealing with Subject Access Requests and complaints about information handling

- 8.1 Under the Data Protection Act 1998, individuals have a right to see personal information held about them by organisations. Data Controllers can charge a fee of up to £10 in most cases, should ensure they can verify the identity of the applicant and must then respond within 40 days, providing
- information about the processing, including purposes and recipients of the personal data
 - a description and copy of their personal data held
 - information about any automated decision making affecting the data subject
 - information about sources, if available
- There are situations when an exemption applies and the personal data can be withheld.
- 8.2 WCC has a corporate procedure for dealing with requests for access to information. Contact the DPO (see Appendix C) for more information.
- 8.3 For the purposes of the Protocol, each partner should have a mechanism for dealing with subject access requests. Responsibility for dealing with requests for personal information held as part of the partnership project should be clarified and made explicit in the Protocol.
- 8.4 If a request is received for personal data and the applicant is not the data subject, the release of that data may constitute a disclosure to a third party and the following should apply:
- If the applicant is acting on behalf of the data subject, proof of their identity and authority to act should be obtained (in WCC this forms part of our standard application form for a request for access to personal information).
 - If the request is from a body exercising their statutory powers, proof of their identity and of their statutory powers should be sought.
 - For all requests of this nature (ie: not from the data subject), each partner's Data Protection Officer should be involved. (See Appendix C for WCC's DPO contact details)
- 8.5 Each Partner should also have an established policy for dealing with complaints, whether about subject access requests or about

information handling generally. WCC has a Corporate Representation Procedure; contact the Customer Services Officer on *****)

9. Security measures should protect the personal data. Make certain that personal data are accurate and up to date

- 9.1 Principle 7 of the DPA requires that appropriate technical and organisational measures are taken against unlawful or unauthorised processing and against destruction, damage or loss of personal data. Security requirements should be a key part of your Sharing Protocol and the nature of the data to be processed should be taken into account. (Therefore, security around sensitive personal data should be stronger). It would be advisable to follow a checklist.
- 9.2 Security Checklist. Does each partner have
- A security policy?
 - Procedures/training for staff about security of personal data, confidentiality, Data Protection?
 - Password protection, physical access control?
 - Secure means of transferring personal data, both manually and electronically?
 - A business continuity plan/disaster plan in place?
 - Protective markings on information held?
 - A commitment to/awareness of the security standard ISO17799? (The Department for Constitutional Affairs recommends this as the benchmark for information security).
- 9.3 A common standard of security, appropriate to the nature of the personal data, should be agreed and be explicit in the Protocol
- 9.4 Principle 4 of the DPA requires that personal data is accurate and, where necessary, kept up to date. Mechanisms should be in place for ensuring accuracy. It may be useful to identify one Partner as being responsible for checking the accuracy of personal data held, at specific intervals. Any inaccuracies should be communicated to all Partners.

10. Inform the Information Commissioner through each Data Controller's Notification

- 10.1 Data Controllers should each have a Notification with the Information Commissioner, which should be renewed on an annual basis and updated whenever a change to processing occurs
- 10.2 If your project involves a change to current processing of personal data (new purpose, new data subjects, new recipients), then this should be included in each Partner's Notification. It would be useful to agree a standard entry that all Partners could Notify. Discuss this with the DPO (for contact details, see Appendix C)

Key Components of an Information Sharing Protocol

On completion of the 10 Steps, the groundwork has been achieved and the protocol is now ready to be written and signed.

The minimum criteria that an Information Sharing Protocol should contain and make explicit is as follows:

(NB: By Information Sharing Protocol, we mean either one Protocol, or the overarching agreement along with its constituent individual Protocols)

- A list of all Partners involved in the project, with key representatives and contact numbers (usually the members of the working group)
- Date that the Protocol was agreed and from when it applies
- Definitions of terms used
- Clear purposes of the project
- Legislative basis for the project
- All data categories to be collected are specified
- It is clear which Partners have access to which categories of data and this is specified
- Any further conditions on the use of the data (ie: anonymised) are agreed and stated
- Retention periods are agreed for the personal data used as part of the project
- A Schedule 2 condition is agreed and stated (if a statutory basis; the exact wording is quoted)
- A Schedule 3 condition is agreed and stated for sensitive personal data
- Fair obtaining notices are agreed and responsibility assigned
- Procedures and responsibility for dealing with subject access requests and complaints are agreed and stated
- A common security standard is agreed
- Measures for ensuring accuracy are agreed and responsibility assigned
- It is agreed that each partner shall update their Notification with the Information Commissioner to take account of the work of the project
- A review date (for the Protocol) is agreed and stated (see next section)
- Signatures are obtained from each Partner at a senior level (ie: Chief Executive)

Approval, Implementation and Review

Approval

Legal Services may be involved in the formation of your Information Sharing Protocol. The Protocol should be approved by the relevant Boards of all the Partners. In WCC, this may be the senior Board in your Directorate or, if the project is cross-Directorate, it may need approval from the Chief Officer Management Board (COMB)

Registering the ISP

The Information Management Group maintain a central register of all Information Sharing Protocols. It is important that you register your Protocol by contacting either the DPO or your Directorate Administrative Manager (see Appendix C).

Implementation

Before implementing the Protocol, all employees who are likely to be affected by the implications should be trained in how to use personal data for the project within the confines of the Protocol. It may be useful to perform a pilot run (3 months?) to see how the Protocol works in practice.

Regular Review

Once the Protocol signatures have been obtained, this is not the end of the process. Your Protocol should contain a regular review period, which will usually be an annual occurrence, but may be shorter or longer depending on the nature of the project. (If a pilot is used, the review should occur first at the end of the pilot period).

The original working group should perform the review and a representative from the Information Management Group should be involved.

The main questions to consider are as follows:

- Has the Protocol worked in practice?
- Have all the Partners met their agreed responsibilities?
- If not, where have problems occurred and how might they be rectified?

This may also be an appropriate time to check accuracy of personal data held, and refresh consent (if consent has been obtained).

Signatures of the Partners should be gained again.

For any problems encountered whilst developing an Information Sharing Protocol, please contact the DPO or your Directorate Administrative Manager (see Appendix C)

Appendix A

Explanation of Terms used

This guidance uses terminology from the Data Protection Act 1998 with which you may not be familiar. The list below aims to explain these terms. If you would like further clarification, please contact the Data Protection Officer or your Directorate Administrative Manager (see Appendix C)

Data Controller

The person (individual or a body) who determines the purposes for and the manner in which personal data are processed. WCC is a Data Controller. Data Controllers must comply with the Data Protection Act. In a partnership, it may be that all partners are Data Controllers.

Data Processor

Any person (individual or body, other than an employee of the Data Controller) who processes data on behalf of the Data Controller. For example, if WCC out-sources a function, such as debt collection, to an outside agency, then that agency is a Data Processor, working on our behalf.

Data Subject

An individual who is the subject of personal data. This could be a member of the public or an employee of WCC.

Fair Obtaining Notice

Unless an exemption applies, the data subject must be told certain information about the processing of their personal data, upon the point of collection. The key elements of this are the identity of the data controller, the purposes of the processing and anything else necessary to guarantee fairness (this may include disclosures, how long their data will be retained)

Personal Data

Data relating to an individual who can be identified from those data, or from those data together with any other information in the possession of (or likely to come into the possession of) the Data Controller. Therefore, for example, if we can put a payroll number and a name together, we have personal data.

Processing

Obtaining, recording, holding, organising, adapting, retrieving, consulting, disclosing, aligning, blocking, erasing or destroying the data. Processing effectively means doing anything with data.

Sensitive Personal Data

Personal data consisting of information as to

- the racial/ethnic origin of the data subject
- his/her political opinions
- his/her religious or similar beliefs
- his/her membership of a trade union
- his/her physical or mental health or condition
- his/her sexual life

- the commission or alleged commission by him/her of an offence and any related proceedings

Subject Access Requests

Data Subjects have a right to ask to see and have copies of information held about themselves. To action this right, the Data Subject can make a Subject Access Request. Contact the Data Protection Officer (see Appendix C) for information on dealing with these requests.

Third Parties

In relation to personal data, third party means any person other than the Data Subject, the Data Controller (including employees), or any Data Processors (including employees)

The Data Protection Principles

There are 8 Data Protection Principles. These form the backbone of the Act and are referenced throughout this guidance. In summary, the Principles are as follows:

1. Personal data must be processed fairly and lawfully and that processing must satisfy at least one of the conditions in Schedule 2 of the Act. If sensitive data is being processed, then at least one condition in Schedule 3 must also be satisfied.
2. Personal data shall be obtained for only one or more specified and lawful purposes and shall not be further processed in any manner incompatible with those purposes
3. Personal data shall be adequate, relevant and not excessive for the purposes
4. Personal data shall be accurate and, where appropriate, kept up to date
5. Personal data shall not be held for any longer than is necessary
6. Personal data shall be processed in accordance with the rights of the data subject
7. Appropriate technical and organisational measures shall be taken to protect personal data
8. Personal data shall not be transferred outside the European Economic Area unless adequate protection is provided

For further explanation of the Principles, please contact the Data Protection Officer (see Appendix C)

Appendix B

Consent – guidance notes

What is consent?

Consent is one of the conditions under Schedules 2 and 3 of the Data Protection Act which can be used as a legitimate basis for processing personal data. If you do choose to ask for consent, you should ensure that there is a genuine opportunity for data subjects to refuse and to be confident that the processing will not go ahead. This appendix aims to act as further guidance on obtaining consent.

Consent has all too often been either assumed or implied. Unfortunately, when something goes wrong it has been very difficult to prove if consent was actually given. Today it is almost always recommended that consent should be in a permanent form (ie: written).

In order to give consent, a person must

- Have the capacity to take a particular decision
- Have received sufficient information to make that decision (ie: be fully informed)
- Not be acting under duress (ie: consent is freely given)

Capacity

For a person to have capacity, (s)he must be able to comprehend and retain the information material to the decision and must be able to weigh this information in the decision making process.

While under current law, no-one can provide consent on behalf of an adult in order to satisfy the Common law requirement, it is generally accepted by the courts that decisions about treatment, and the disclosure of information, should be made by those responsible for providing care and that they should be in the best interests of the individual concerned.

The Data Protection Act does not create an age limit for making subject access requests or for giving consent. Following the case of *Gillick v West Norfolk and Wisbech AHA* (1986), the courts have held that young people (below the age of 16) who have sufficient understanding and intelligence to enable them to understand fully what is involved will also have the capacity to consent.

For parental consent, the Children's Act 1989 sets out persons who may have parental responsibility. These include:

- The child's parents if married to each other at the time of conception or birth
- The child's mother, but not the father if they were not so married unless the father has acquired parental responsibility via a court order or a parental responsibility agreement or the couple subsequently marry
- The child's legally appointed guardian

- A person in whose favour the court has made a residence order in respect of the child
- A local authority designated in a care order in respect of the child
- A local authority or other authorised person who holds an emergency protection order in respect of the child

Fully informed consent

If consent is needed, all those involved in the project who first collect the personal data should ensure that the individual is made fully aware of what their consent allows.

A fair obtaining notice (see Step 7 Inform the Data Subjects) should be provided whether consent is needed or not. However, where consent is needed, a fair obtaining notice will be a useful method of explaining the following:

- Identity of the Data Controller (ie: body collecting their data)
- Why their personal data is being collected (purposes)
- Any organisations with whom the data will be shared
- The exact details of the personal data that is required from them

If there is an opportunity to opt out of any of the above provisions, this should be made clear at the point of obtaining consent.

The person should be told that they have a right to withhold consent or to withdraw it at any time.

If the individual needs the information about the project in another format, such as braille or audiotape, or in another language for those who may have difficulty understanding English, this should be provided.

The consent form should be signed by the data subject, or their authorised agent (see Capacity).

Consent should be....

- Freely given, without any pressure or undue influence being exerted on the individual
- Specific to the purpose for which it was obtained. Consent for one purpose does not mean it can be used for another.
- Freely withdrawn (have you mechanisms in place for dealing with this?)
- Refreshed (is this part of your review process?)

Specimen consent procedures and form

If you do choose to use consent as your Schedule 2 (and 3) condition for processing, there are certain steps to take.

By following procedures and developing a consent form, you will be letting people make a fully informed choice as to whether or not to consent. You must ensure, however, that you can meet all the commitments that you promise!

Specimen procedures

1. Fully inform people as to what their consent means, provide them with the necessary supporting information and ensure that they have the capacity to consent. You may wish to do this through using a checklist for the staff member to follow:

- I have explained to the person:-
 - Why we would like to collect their information
 - Who will have access to their information
 - How long their information will be kept
 - Why we may wish to share their information
 - With whom we may wish to share their information
 - What information we may share
 - Their right to decline their provision of/our further use of their information
 - Their right to *withdraw* consent to their provision of/our further use of their information and what this will mean
 - The procedure for them to access to their records under DPA 1998
 - The procedure for them to complain
- I have provided the person with copies of the following explanatory booklets or leaflets.....
- I am satisfied that the person is capable of understanding the information that I have given to them and that they have capacity to give informed consent of their own free will or
- I am satisfied that this person does not have capacity and that an appointed representative is completing the consent form on their behalf.
- Signed (staff member)
- Date

This checklist should be recorded and kept with the consent form. For some long term uses of data, there should be a renewal of this process to refresh consent.

Specimen consent form

An example of how the above translates into a consent form is as follows:

Police Victim Support Service Consent Form

If you choose to complete this form, the information you provide will be used by the Police to provide you with an optional Victim Support Service. Your form will be retained for only 1 year after the support has been provided.

Your details will only be accessed by those employees of the Police Service who provide Victim Support. However, if you are over 60 and wish to receive further support, you may wish us to pass the information you provide on this form to WCC Social Services. This further option will be explained to you in more detail by the Police Victim Support Service.

You can withdraw your consent to either of the above uses of your information at any time but this may affect the level of support which can be provided.

You have a right to access the information we hold about you, subject to exemptions under the Data Protection Act 1998. You also have a right to complain. Please contact ***** or write to ***** for more details.

<p>Your details:</p> <p>Name:</p> <p>Address:</p> <p>Age range* (please circle): 60 or below 61 or above</p> <p>Crime Number:</p> <p>*This field is optional</p>

I confirm that I have understood the information above and I consent to my details being used accordingly

Signature

Date

If you are unable to manage your own affairs and someone has been appointed to sign for you then please pass this form to them to read and sign if they consent to your personal data being used as explained above.

Representative's name and relationship to the person referred to on this form:

Name

Relationship

Appendix C

The Information Management Group

The Information Management Group has been formed to provide a corporate steer to managing information in line with current legislation. Particular drivers are

- The Data Protection Act 1998
- The Freedom of Information Act 2000
- E-Government targets for delivering services electronically by 2005

The Group reports to the E-Government Programme Board and comprises representatives from all Directorates, whose work involves the management of information.

Members

The Information Management Group will hold a central register of Information Sharing Protocols. Please contact your Directorate Administrative Manager or the Data Protection Officer if you are developing an Information Sharing Protocol.