

Solihull Metropolitan Borough Council

GENERAL PROTOCOL

**For Inter-agency
Information Sharing
Within Solihull**

Endorsed by Solihull MBC – Corporate Management Team 17 June 2003

Endorsed by Resources Executive Member 7 July 2003

Reviewed: July 2006

Next Review: July 2009

CONTENT

1. INTRODUCTION	1
1.1. Background.....	1
1.2. Objectives of the General Protocol.....	1
1.3. The Document.....	2
2. LEGISLATION	2
2.1. General	2
3. GENERAL PRINCIPLES	3
4. THE PRINCIPLES GOVERNING THE SHARING OF PERSONAL INFORMATION	4
4.1. General	4
4.2. Lead Person.....	4
4.3. Individual Protocol.....	5
4.4. Confidentiality.....	5
4.5. Compliance With The Data Protection Act	6
4.6. Request for Access To Records.....	6
4.7. Consent.....	7
4.8. Time Limit On Consent	7
4.9. Recording Of Consent.....	7
4.10. Withdrawal Of Consent/Add Or Amend Restrictions	8
4.11. Disclosure Without Consent	8
4.12. Making Disclosure	9
4.13. Recording Disclosure	9
4.14. Disclosure Of A Deceased's Personal Information.....	9
4.15. Complaints Procedure.....	9
4.16. Staff Confidentiality Agreement.....	10
4.17. Staff Awareness	10
4.18. Staff Training.....	10
4.19. Storage Of Personal Information	10
4.20. Access To Personal Information	11
4.21. Retention Of Personal Information	11
4.22. Transfer Of Personal Information	11
4.23. Compromise Of Confidentiality.....	11
4.24. Use Of Personal Information Other Than For An Agreed Purpose	12
5. INDEMNITY	13
6. AGREEMENT	13
7. SIGNATORIES AND PRODUCTION OF DOCUMENTS	13
8. SIGNATORIES	15

Appendix A - LEGISLATION	1
1. Introduction	1
2. Data Protection Act 1998	1
3. Human Rights Act 1998	5
4. Crime and Disorder Act 1998	6
5. Common Law Duty of Confidentiality	6
6. Regulation of Investigatory Powers Act 2000	7
7. Caldicott	7
Appendix B - GUIDANCE NOTES	1
1. Consent	1
2. Capacity	2
3. Young Persons	2
4. Parental Responsibility	3
5. Obtaining Consent	3
6. Disclosure of Personal Information	4
7. Disclosure with consent	4
8. Disclosure without consent	5
9. Recording Consent	6
10. Use Of Personal Information For Purposes Other Than Agreed	7
Appendix C - SPECIMEN INDIVIDUAL PROTOCOL	1
Appendix D - SPECIMEN CONSENT FORM	1
Appendix E - SPECIMEN INFORMATION LEAFLET	1

GENERAL PROTOCOL FOR INTER-AGENCY INFORMATION SHARING WITHIN SOLIHULL

1. INTRODUCTION

1.1. Background

- 1.1.1. Solihull Metropolitan Borough Council's Vision is that citizens should receive the services that they need in a fast, efficient and personalised manner. This clearly requires all public agencies to work more closely and efficiently together and to tailor the services that they provide to meet the particular needs and circumstances of each individual. Sharing information, both within the Council and between agencies, is seen as a key imperative to the delivery of high quality, cost effective and seamless public services.
- 1.1.2. In the past there have been both real and perceived barriers to the sharing of personal information. These are often linked to legal requirements or ethical standards. However, sometimes these impediments have focused on personal, inter-professional and inter-organisational mistrust; sometimes on worries about responsibility and accountability for personal information; sometimes in the absence of enabling mechanisms; and sometimes because of technical matters.
- 1.1.3. To enable Solihull MBC and other agencies to work closer together, and provide the standards of service expected by both government and the public, it is essential that these barriers are minimised. In the absence of specific statutory instruments enabling the sharing of personal information to take place, it is necessary that all concerned have a clearly defined framework to facilitate the sharing of personal information whilst respecting the rights of the individual.
- 1.1.4. This General Protocol, and the underpinning Individual Protocols, have been developed in accordance with national guidelines to address these responsibilities and concerns.

1.2. Objectives of the General Protocol

- 1.2.1. To provide a robust framework for the legal, secure and confidential sharing of personal information between public sector agencies to enable them to meet both their statutory obligations and the needs and expectations of the people who they serve.
- 1.2.2. The strategic purpose of this General Protocol for the sharing of personal information are:-

- a) The delivery of integrated public sector services in line with government initiatives and public expectations.
- b) To facilitate the management and planning of cost effective and efficient services.
- c) To enable parties to the General Protocol to review, account for, and learn how to improve what they do.

1.3. The Document

1.3.1. The General Protocol defines:-

- a) The principles which underpin the exchange of personal information between the parties who have signed up to the General Protocol.
- b) The procedures which will ensure that information is disclosed in line with statutory obligations and responsibilities.
- c) The responsibilities of organisations to implement internal arrangements to meet the requirements of the General Protocol.
- d) The roles and structures which will support the exchange of personal information between parties to the General Protocol.
- e) The security procedures necessary to ensure that the confidentiality of personal information exchanged is maintained.
- f) How this protocol will be implemented, monitored and reviewed.

2. LEGISLATION

2.1. General

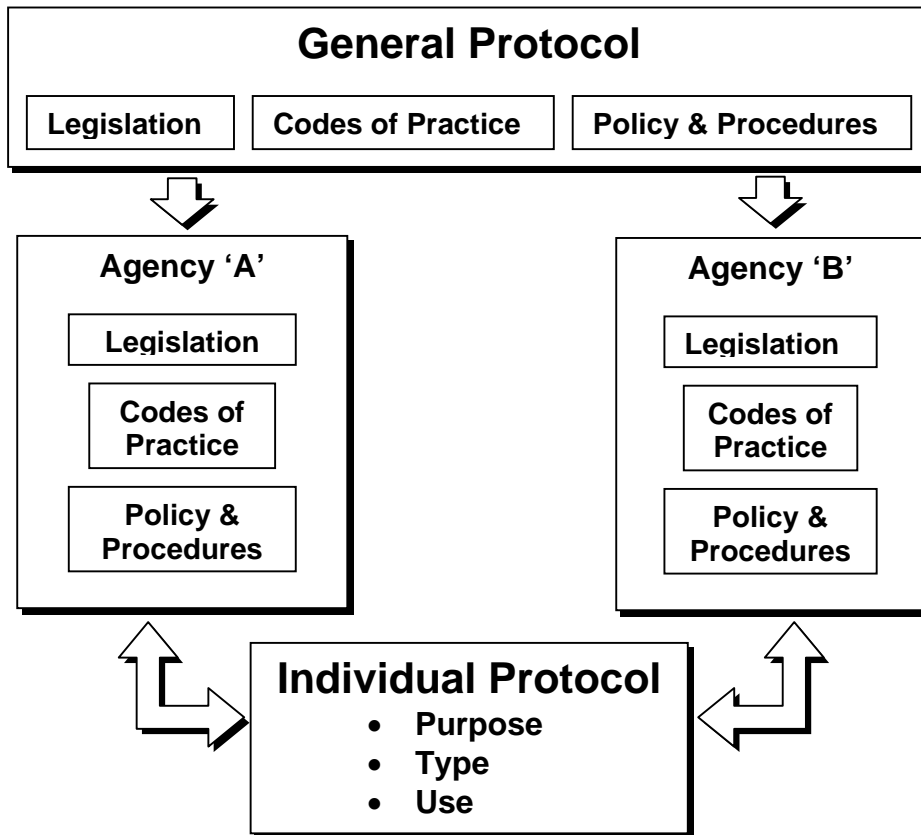
- 2.1.1. Legislation, under which most public sector agencies operate, defines the role, responsibility and power of the agency to enable it to carry out a particular function.
- 2.1.2. In many instances legislation tends to use broad or vague statements when it come to the matter of sharing personal information, for example: the agency is required to communicate.., or will co-operate with.. without actually specifying exactly how this may be done. This is because legislation that specifically deals with use of personal information (collection; use; storage; destruction; protection etc.) already exists namely, the Data Protection Act 1998.

- 2.1.3. The Data Protection Act 1998, in most cases, is the key to the use of personal information and links into most other legislation. The Act sets out to govern the collection, use, storage, destruction and protection of a living person's identifiable information (Personal Data) in most formats e.g. paper, electronic, images (photograph/video) etc.
- 2.1.4. The Data Protection Act 1998 does not set out to prevent the sharing of personal information. To the contrary, provide that the necessary conditions of the Act can be met, sharing is perfectly legal.
- 2.1.5. The key legislation governing the collection and use of personal information are:-
- a) The Data Protection Act 1998
 - b) The Human Rights Act 1998
 - c) The Crime and Disorder Act 1998
 - d) Common Law Duty of Confidentiality
- 2.1.6. In addition to the above mentioned legislation, consideration may also need to be given to the following when sharing personal information:-
- a) The Caldicott Committee Report
 - b) The Regulation of Investigatory Powers Act 2000
- 2.1.7. The principle elements of the above mentioned legislation are described in Appendix A.
- 2.1.8. Guidance notes on the interpretation of key factors are provided in Appendix B.

3. GENERAL PRINCIPLES

- 3.1.1. The General Protocol serves as the overarching principle to enable the legal and secure exchange of personal information between agencies who have common obligations to provide services within the community.
- 3.1.2. Each agency agrees to abide by the General Protocol and set in place policies and procedures to facilitate the collection, storage, processing and disposal of personal information in accordance with the guidelines.
- 3.1.3. In order to facilitate the exchange of personal information between agencies, Individual Protocols, as prescribed by the General Protocol, will be agreed between the participating agencies who may need to share personal information about their service user(s). These Individual Protocols will specify the purpose for the exchange of personal

information, the type of the information that may be exchanged and the purpose for which that information may be used and details of who else that information may be shared with.



4. THE PRINCIPLES GOVERNING THE SHARING OF PERSONAL INFORMATION

4.1. General

4.1.1. In seeking to share personal information in order to improve services and support individuals regardless of their age within the community, those agencies who are party to the General Protocol will adhere to the following principles:-

4.2. Lead Person

4.2.1. Agencies who are party to the General Protocol will nominate a lead person who will be responsible for the day to day management of the scheme within their agency and the approval of Individual Protocols.

4.2.2. The person nominated as 'Lead Person' should have sufficient seniority within the agency to influence policies and procedures at executive level.

It is anticipated that within NHS or Social Care agencies this person will be the Caldicott Guardian.

4.3. Individual Protocol

- 4.3.1. In order to maintain a consistent approach, all agencies who are party to the General Protocol will ensure that any Individual Protocol that they develop contains the following information:-
- a) The full details of the agencies who are party to the Individual Protocol e.g. names and addresses
 - b) The purpose(s) for the sharing of personal information.
 - c) The type(s) of personal information that will be shared.
 - d) Details of any other agencies/organisation to whom the personal information may also be shared by the recipient.
 - e) Details of any restrictions on the use of the personal information.
- 4.3.2. All Individual Protocols will be approved by the respective lead person nominated within each agency (see 4.2.).
- 4.3.3. A specimen Individual Protocol is given in Appendix C.
- 4.3.4. Where information sharing protocols exist between agencies prior to signing up to the General Protocol, such protocol will remain valid. However, such protocols should be reviewed and if necessary brought into line with the General Protocol at the earliest opportunity in order to maintain a consistent approach.

4.4. Confidentiality

- 4.4.1. Personal information held by an agency shall be deemed to have been provided in confidence, in the absence of explicit or implied confirmation, when it appears reasonable to assume that the provider of the information believed that this would be the case.
- 4.4.2. All agencies who are party to the General Protocol accept this duty of confidentiality and will not disclose personal information without the consent of the person concerned, unless there are statutory grounds or other overriding justification for so doing.
- 4.4.3. In requesting disclosure of personal information from another agency who are party to the General Protocol, those concerned will respect this responsibility and not seek to override the procedures which each agencies has in place to ensure that information is not disclosed illegally or inappropriately.

4.5. Compliance With The Data Protection Act

- 4.5.1. Agencies who are party to this General Protocol recognise their responsibilities with regard to legislation and the use of personal information which they have acquired and shall have in place appropriate policies and procedure to ensure that personal information within their care is used within the context of the relevant legislation, in particular the Data Protection Act 1998.
- 4.5.2. Agencies party to the General Protocol recognise the sensitivity of information about a person's racial or ethnic origin, political opinions, religious or other similar beliefs, trade union membership, physical and mental health, sexuality, the commission or alleged commission of any offence and any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings and will adhere to the requirements of Schedule 3 of the Data Protection Act 1998 in respect of such information.
- 4.5.3. An agency who has obtained information in any of the above mentioned categories about an individual, in the course of their direct contact with that person, will seek to obtain the explicit consent of that person to disclose that information to another agency. If consent is not given, because the person is either unable or unwilling to give that consent, then the information will only be released if there are legal grounds for doing so and one of the remaining conditions of Schedule 3 can be demonstrated or there is a statutory reason for doing so without the individual's consent.

4.6. Request for Access To Records

- 4.6.1. A service user making a valid request under section 7 of the Data Protection Act 1998 for access to his/her record will be fully informed, in accordance with the Act, about the information that is held about them by the agency approached.
- 4.6.2. Information that has been provided by another agency under an agreed Individual Protocol may be disclosed to the individual without the need for obtaining the provider's consent to disclose, with the following exceptions when consent must be obtained prior to disclosure:-
 - a) The provider has specifically stated that the information supplied must be kept confidential from the service user.
 - b) The information contains medical details.
 - c) The information contains information of a legal nature.
- 4.6.3. In the situation of two or more organisations having a joint (single) record on an individual, that individual may make their access to record request to any of the organisations. The organisation receiving the request will be responsible for processing the request for the whole record and not just

the part that they may have contributed, subject to the conditions for disclosure mentioned above (4.6.2.).

4.7. Consent

- 4.7.1. Unless statutory exemptions are applicable, all agencies who are party to the General Protocol will endeavour to seek **informed explicit consent** from the individual concerned to share their personal information in accordance with an agreed Individual Protocol.
- 4.7.2. Consent will normally be obtained at the earliest opportunity and should be sufficient to cover the needs for a particular 'piece of work' or situation. It is essential to avoid the need to repeatedly seek consent over minor issues.
- 4.7.3. In seeking consent to disclose personal information, the individual concerned will be made fully aware of the nature of the information that it may be necessary to share, who the information may be shared with, the purposes for which the information will be used and any other relevant details including their right to withhold or withdraw consent.
- 4.7.4. For further guidance on consent, see Appendix B.
- 4.7.5. A specimen consent form is given in Appendix D.
- 4.7.5. A specimen service user information leaflet is given in Appendix E.

4.8. Time Limit On Consent

- 4.8.1. Consent to disclose personal information, obtained under an Individual Protocol, will be limited to the duration of the 'piece of work'.
- 4.8.2. All agencies participating in the General Protocol agree that once the 'piece of work' for which consent was originally obtained has been completed, that consent will be deemed to have lapsed.
- 4.8.3. In the event that a similar, or subsequent additional work needs to be undertaken with that individual, a new consent to disclose will be obtained.

4.9. Recording Of Consent

- 4.9.1 The agency obtaining explicit consent to disclose an individual's personal information will:-
 - a) Retain the signed original consent form on the individual's manual record.
 - b) Provide the person giving consent with a copy.

- c) Provide a copy of the consent form to the other agency/agencies involved when the initial disclosure is made.

4.9.2. All agencies participating in the General Protocol will ensure that the details (including any conditions) of any consent, or refused consent, are recorded on their electronic systems in accordance with their agencies policies and procedures.

4.10. Withdrawal Of Consent/Add Or Amend Restrictions

4.10.1. In the event that an individual:-

- a) Withdraws his/her consent for their personal information to be shared, or
- b) Wishes to subsequently place/amend a restriction upon the personal information to that may be shared.

the agency receiving such a request will immediately inform all other agencies who are or may be affected and record the details on the individual's file.

4.10.2. In the case of consent being withdrawn, no further personal information should be disclosed unless there are statutory reasons for doing so, or a legal exemptions can be applied.

4.10.3. In the case of the person applying restrictions on the use of their personal information, these restrictions should be complied with unless there are statutory reasons for doing so, or a legal exemptions can be applied.

4.11. Disclosure Without Consent

4.11.1 Agencies who are party to the General Protocol will put in place procedures to ensure that decisions to disclose personal information without legal grounds or consent have been fully considered and that such a decisions can be audited and defended.

4.11.2. A decision to disclose personal information without the consent of the individual concerned should be authorised by a senior member of staff (nominated person) and the reason(s) recorded on the service user's record.

4.11.3. On disclosure of the information, the agency providing the information will make the receiving agency aware that disclosure is being made without consent and the reason(s) why.

4.11.4. Personal information will only be disclosed where the relevant agreed purpose for sharing clearly requires this. For all other purposes, information about individual cases will be anonymised.

4.12. Making Disclosure

- 4.12.1. Agencies who are party to the General Protocol will ensure that their staff, who are authorised to make disclosure of personal information, will clearly state whether the information that is being supplied is fact, opinion, or a combination of the two.
- 4.12.2. Unless it is specified to the contrary, all personal information that is provided under an agreed Individual Protocol will be made available to the individual should that individual make a valid request to the recipient for access to their record under section 7 of the Data Protection Act 1998 without the necessity of seeking the providers consent to disclose, subject to the exceptions specified in 4.6.2. It is therefore the responsibility of the person providing the information to clearly state that they do not wish the information to be disclosed without being consulted first.

4.13. Recording Disclosure

- 4.13.1. Agencies who are party to the General Protocol will ensure that all personal information that has been disclosed to them under an agreed Individual Protocol will be recorded accurately on the individual's manual or electronic record in accordance with their agencies policies and procedures.
- 4.13.2. Agencies who are party to the General Protocol will set in place procedures to record not only the details of the information, but who gave and who received that information.

4.14. Disclosure Of A Deceased's Personal Information

- 4.14.1. Agencies who are party to the General Protocol will exercise caution when contemplating the disclosure of personal information relating a deceased person. Although the Data Protection Act only applies to personal information of a living person, a duty of confidentiality may still apply after the person has died.

4.15. Complaints Procedure

- 4.15.1. Agencies who are party to the General Protocol shall put in place efficient and effective procedures to address complaints relating to the disclosure or the use of personal information that has been provided under an agreed Individual Protocol.
- 4.15.2. In the event of an complaint relating to the disclosure or the use of an individual's personal information that has been supplied/obtained under an agreed Individual Protocol, all agencies who are party to the Individual Protocol will provide co-operation and assistance in order to resolve the complaint.

- 4.15.3. All agencies will ensure that the service users will be provided with information about the complaints procedures when consent is obtained or upon request.

4.16. Staff Confidentiality Agreement

- 4.16.1. All agencies who are party to the General Protocol should require their staff (full/part time; temporary; agency; students etc) who have access to, or are likely to come into contact with, personal information should be required to sign a confidentiality agreement as part of their terms and conditions of employment.

4.17. Staff Awareness

- 4.17.1. Agencies who are party to the General Protocol will ensure that all staff are aware of, and comply with, their responsibilities and obligations with regard to:-
- a) The confidentiality of personal information about people who are in contact with their agency, and
 - b) The commitment of the organisations/agency to only share information legally and within the terms of an agreed Individual Protocol.
 - c) Information will be shared on a need-to-know basis only.
- 4.17.2. Staff will be made aware that disclosure of personal information which cannot be justified, whether inadvertent or intentional will be subject to disciplinary action.

4.18. Staff Training

- 4.18.1. All parties to the General Protocol will ensure that employees who need to share personal information under an Individual Protocol are given appropriate training to enable them to share information legally, comply with any professional codes of practice and comply with any local policies and procedures.
- 4.18.2. Staff who are not directly involved with sharing personal information should not be excluded from such training as it is possible that they may come across such information during the course of their duties. It may therefore be appropriate that such employees receive awareness training.

4.19. Storage Of Personal Information

- 4.19.1 All agencies who are party to the General Protocol will put in place policies and procedures governing the secure storage of all personal information retained within their manual and/or electronic systems.

4.20. Access To Personal Information

- 4.20.1. All agencies who are party to the General Protocol will put in place policies and procedures governing the access by their employees, and others, to personal information held within their manual and/or electronic systems and to ensure that access to such information is controlled and restricted to those who have a legitimate need to have access.

4.21. Retention Of Personal Information

- 4.21.1. All agencies who are party to the General Protocol will put in place policies and procedures governing the retention and destruction of records containing personal information retained within their manual and/or electronic systems.

4.22. Transfer Of Personal Information

- 4.22.1. All agencies who are party to the General Protocol will put in place policies and procedures that govern the secure transfer of personal information both internally and externally. Such policies and procedures must cover:-
- a) Internal and external postal arrangements.
 - b) Verbally; face-to-face and telephone.
 - c) Facsimiles (safe haven).
 - d) Electronic mail (secure network or encryption).
 - e) Electronic network transfer.

4.23. Compromise Of Confidentiality

- 4.23.1. All agencies who are party to the General Protocol will have in place appropriate measures to investigate and deal with the inappropriate or unauthorised access to, or use of, personal information whether intentional or inadvertent.
- 4.23.2. In the event of personal information that has been shared under the General Protocol having or may have been compromised, whether accidental or intentional, the agency making the discovery will without delay:-
- a) Inform the information provider of the details.
 - b) Take steps to investigate the cause.
 - c) If appropriate, take disciplinary action against the person(s) responsible.

d) Take appropriate steps to avoid a repetition.

4.23.3 On being notified that an individual's personal information has or may have been compromised, the original provider will assess the potential implications for the individual whose information has been compromised and if necessary:-

a) notify the individual concerned,

b) advise the individual of their rights,

c) provide the individual with appropriate support.

4.24. Use Of Personal Information Other Than For An Agreed Purpose

4.24.1. It is recognised that agencies who are party to the General Protocol may fulfil a number of roles. In fulfilling one particular role, they may be given privileged access to personal information which they may subsequently believe may assist them in another role or be of wider interest to their organisation.

4.24.2. Personal information shared under this General Protocol will have been disclosed for a specific purpose, as defined in the Individual Protocol, and as such must only be used for that purpose.

4.24.3. Personal information that has been obtained under an agreed Individual Protocol will not be regarded or used by the receiving agency as intelligence for the general use of that organisation.

4.24.4. Agencies wishing to use information given under the General Protocol for any purpose other than that defined in the Individual Protocol, or who may wish to disclose that information to any person other than those authorised to receive that information, must:-

a) inform the originator of the information of their intention to use the information provided for a different purpose, and

b) Obtain explicit consent from the individual(s) concerned before processing such information.

4.24.5. Agencies who wish to use information that has been provided to them under the General Protocol for research or statistical purposes must ensure that policies and procedures are in place to guarantee that such personal information is anonymised.

5. INDEMNITY

- 5.1. Disclosure of personal information without consent must be justifiable on statutory grounds, or meet the criterion for claiming an exemption under the Data Protection Act. Without such justification, both the agency and the member of staff expose themselves to the risk of prosecution and liability to a compensation order under the Data Protection Act or damages for a breach of the Human Rights Act.

6. AGREEMENT

In consideration of the provision of information in accordance with this General Protocol for Inter-Agency Information Sharing within Solihull each person or authority being a Signatory as set out in Section 7 undertakes to indemnify each of the other Signatories against any liability which may be incurred such Signatory as a result of the provision of such information.

Provided that this indemnity shall not apply:-

1. in the event of the liability arising from information supplied which is incomplete or incorrect and where the error or omission was due to the wilful wrongdoing or negligence of any member or employee of the Signatory providing the information;
2. unless the Signatory claiming the benefit of this indemnity notifies a Signatory by notice in writing to its Chief Officer providing information or notice as soon as possible of any action claim or demand to which this indemnity applies and permits such Signatory to deal with the action claim or demand by settlement or otherwise and renders to such Signatory all reasonable assistance in so doing.
3. to the extent that a Signatory claiming the benefit of this indemnity makes any admission which may be prejudicial to the defence of the action claim or demand.

7. SIGNATORIES AND PRODUCTION OF DOCUMENTS

7.1. Solihull Metropolitan Borough Council undertakes:-

1. to hold the original of this Protocol as signed by all persons who agree to be bound by its provisions and to produce the original to any signatory who may require it for the purpose of enforcing the Protocol against any other person;
2. to provide each party to this Protocol with a copy of this Protocol signed on behalf of the Council;

3. to publish this Protocol on the Council's web site with the names of all current signatories and to make amendments as required; and
 4. to hold a list of all past and present signatories with details of the period during which such signatories were bound by the Protocol.
- 7.2. Any person who is a signatory to this Protocol may give 28 days notice to Solihull Metropolitan Borough Council and the name of that signatory shall be removed from the list of current signatories at the expiry of that period but without prejudice to the enforcement of any provision of the Protocol by any past or present signatory in respect of any period during which a person was a signatory to the Protocol.

8. SIGNATORIES

Signed: _____ Date: _____

Chief Executive Solihull Metropolitan Borough Council

Signed: _____ Date: _____

On behalf of: _____

Signed: _____ Date: _____

On behalf of: _____

Signed: _____ Date: _____

On behalf of: _____

Signed: _____ Date: _____

On behalf of: _____

Signed: _____ Date: _____

On behalf of: _____

INTENTIONALLY LEFT BLANK

General Protocol for Inter-agency Information Sharing

Appendix A - LEGISLATION

1. Introduction

- 1.1. Legislation, under which most public sector agencies operate, defines the role, responsibility and power of the agency to enable it to carry out a particular function.
- 1.2. In many instances legislation tends to use broad or vague statements when it come to the matter of sharing personal information, for example: the agency is required to communicate.., or will co-operate with.. without actually specifying exactly how this may be done. This is because legislation that specifically deals with use of personal information (collection; use; storage; destruction; protection etc.) already exists namely, the Data Protection Act 1998.
- 1.3. The Data Protection Act 1998, in most cases, is the key to the use of personal information and links into most other legislation. The Act sets out to govern the collection, use, storage, destruction and protection of a living person's identifiable information (Personal Data) in most formats e.g. paper, electronic, images (photograph/video) etc.
- 1.4. The Data Protection Act 1998 does not set out to prevent the sharing of personal information. To the contrary, provide that the necessary conditions of the Act can be met, sharing is perfectly legal.

2. Data Protection Act 1998

- 2.1. The key principles of the Data Protection Act are:-
 - (1) Personal Data must be processed (e.g. collected, held, disclosed) fairly and lawfully and that processing must satisfy one of the conditions in schedule 2 of the Act. The processing of sensitive data is further protected in that processing must also satisfy at least one of the conditions in schedule 3 of the Act.
 - (2) Personal Data shall be obtained and processed for only one or more specific and lawful purpose(s).
 - (3) Personal Data shall be adequate, relevant and not excessive in relation to the specified purpose(s).
 - (4) Personal Data shall be accurate and kept up to date.
 - (5) Personal Data shall not be held for longer than is necessary.

Appendix A – LEGISLATION (continued)

- (6) Processing of Personal Data must be in accordance with the rights of the individual.
- (7) Appropriate technical and organisational measures should protect Personal Data.
- (8) Personal data should not be transferred outside the European Union unless adequate protection is provided by the recipient.

- 2.2. With few exceptions the Data protection Act 1998 requires anyone processing personal information to register with the Information Commissioner.

The registration details include the type of information held, the purpose of use and who the information may be disclosed to. It is therefore essential that anyone considering sharing personal information establishes that their registration covers who they may disclose information to, or what information they may collect (when receiving shared information). If their registration does not cover these matters adequately, amendments must be registered with the Information Commissioner.

- 2.3. The first and second principles of the Data Protection Act are crucial when considering information sharing. In basic essence, these require that personal information should be obtained and processed fairly and lawfully and that personal information should only be used for the purpose(s) that it was originally obtained.

- 2.4. Schedules 2 and 3 of the Act set out conditions that must be met before personal information can be processed fairly and lawfully – Schedule 2 for all personal information; Schedule 3 as an additional test for sensitive information.

Sensitive information, as defined by the Act, includes information concerning a person's physical or mental health; sexual life; ethnicity or racial origin; political opinion; trade union membership; criminal record or details of alleged offences etc.

- 2.5. In order for there to be no misunderstanding, on anyone's part, it is always advisable for the 'collector' of the information to ensure that the person is made fully aware of why the information is needed, what will be done with it, who will have access to it, their rights and if appropriate seek the informed consent of the individual concerned before sharing that information.
- 2.6. If informed consent to a proposed disclosure is not forthcoming, compliance with the Schedule 2 or 3 of the Act alone will not permit a disclosure. However, there are circumstances where disclosure would still be possible, namely:-

Appendix A – LEGISLATION (continued)

- a) Section 29 of the Act permits disclosure for the purposes of prevention or detection of crime, or apprehension or prosecution of offenders, and where those purposes would be likely to be prejudiced by non-disclosure.
 - b) Disclosure is also permitted where information has to be made public, or where disclosure is required by law.
- 2.7. For the purposes of the common law duty of confidentiality, if there is no informed consent, this is the point where the need for confidentiality would have to be balanced against countervailing public interests – again preventing crime is accepted as one of those interests.
- 2.8. For the purposes of the Human Rights Act 1998, Article 8 – Right to respect for private and family life, would need to be considered.
- 2.9. The Data Protection Act gives individuals various rights in respect of their own personal data held by others, namely the right to:-
- a) access their own information (subject access request).
 - b) take action to rectify, block, erase or destroy inaccurate data.
 - c) prevent processing likely to cause unwarranted substantial damage or distress.
 - d) prevent processing for the purposes of direct marketing.
 - e) to informed about automated decision taking processes.
 - f) take action for compensation if the individual suffers damage.
 - g) apply to the Information Commissioner or the court to have their rights under the Act enforced.
- 2.10. Section 7 of the Act, gives an individual have the right to access the information held about themselves, irrespective of when the information was recorded or how it is stored (manual or electronic).
- 2.11. Disclosure of information held on an individual's record that identifies or has been provided by a third party is subject to certain restrictions.
- 2.12. The Act provides the holder of the information a limited of exemptions to decline/refuse access to an individual's record which are set out under Part IV of the Act.
- 2.13. The Data Protection Act 1998 does not apply to personal information relating to the deceased person.

Appendix A – LEGISLATION (continued)

- 2.14. The Data Protection Act 1998 supersedes the Access to Health Records Act 1990 apart from section 3.1.(f) which continues to provide a right of access to the health records of deceased person made by their personal representatives and others having a claim on the deceased's estate.

In all other circumstances, disclosure of records relating to the deceased person should satisfy common law duty of confidence.

- 2.15. **Schedule 2** of the Data Protection Act 1998 specifies conditions relevant for the processing of any personal data, namely:-
- a) The data subject has given his/her consent to the processing, or
 - b) The processing is necessary for the performance of a contract to which the data subject is a party, or for the taking of steps at the request of the data subject with a view to entering into a contract, or
 - c) The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract, or
 - d) The processing is necessary to protect the vital interests of the data subject.
 - e) The processing is necessary-for the administration of justice for the exercise of any functions conferred on any person by or under any enactment for the exercise of any functions of the Crown, a Minister of the Crown or a government department for the exercise of any other functions of a public nature exercised in the public interest by any person, or
 - f) The processing is necessary for the purpose of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject. The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

- 2.16. **Schedule 3** of the Data Protection Act 1998 specifies additional conditions relevant for the processing of sensitive personal data, namely:-

- a) The data subject has given his/her consent, or
- b) Processing of sensitive personal data is necessary:-
 - By right or obligation under law, or

Appendix A – LEGISLATION (continued)

- ❑ To protect specific vital interests of the individual or other persons, where consent cannot be given by or on behalf of the individual, or
- ❑ In the course of legitimate activities of specified non-profit organisations, with extra safeguards, or
- ❑ Information already publicly released by the individual.
- ❑ Legal, judicial, government or crown reasons, or
- ❑ Medical purposes, or
- ❑ To monitor equality or opportunity, or
- ❑ By order of the Secretary of State.

3. Human Rights Act 1998

- 3.1. Article 8.1. of the **European Convention on Human Rights** (*given effect via the Human Rights Act 1998*), provides that “everyone has the right to respect for his private and family life, his home and his correspondence.”

This is however, a qualified right i.e. there are specified grounds upon which it may be legitimate for authorities to infringe or limit those rights.

- 3.2. Article 8.2 of the European Convention on Human Rights provides “there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

- 3.3. In the event of a claim arising from the Act that an organisation has acted in a way which is incompatible with the Convention rights, a key factor will be whether the organisation can show, in relation to its decision(s) to have taken a particular course of action:-

- a) that it has taken these rights into account;
- b) that it considered whether any breach might result, directly or indirectly, from the action, or lack of action;
- c) if there was the possibility of a breach, whether the particular rights which might be breached were absolute rights or qualified rights;
- d) (if qualified rights) whether the organisation has proceeded in the way mentioned below.

Appendix A – LEGISLATION (continued)

“Evidence of the undertaking of a 'proportionality test', weighing the balance of the individual rights to respect for their privacy, versus other statutory responsibilities e.g. protection of others from harm, will be a significant factor for an organisation needing to account for its actions in response to claims arising from the Act”.

4. Crime and Disorder Act 1998

- 4.1. The Crime and Disorder Act 1998 introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in the local area.
- 4.2. Section 115 of the Act provides that any person has the power to lawfully disclose information to the police, local authorities, probation service or health authorities (or persons acting on their behalf) where they do not otherwise have the power, but only where it is necessary and expedient, for the purposes of the Act.
- 4.3. Whilst all agencies have the power to disclose, section 115 does not impose a requirement on them to exchange information, and responsibility for the disclosure remains with the agency that holds the information. It should be noted, however, that this does not exempt the provider from the requirements of the second Data Protection principle.

5. Common Law Duty of Confidentiality

- 5.1. All staff working in both the public and private sectors should be aware that they are subject to a Common Law Duty of Confidentiality, and must abide by this.

‘In Confidence’... Information is said to have been provided in confidence when it is reasonable to assume that the provider of that information believed that this would be the case, in particular where a professional relationship may exist e.g. doctor/patient, social worker/client; lawyer/client etc.

- 5.2. The duty of confidence only applies to person identifiable information and not to aggregated data derived from such information or to information that has otherwise been effectively anonymised i.e. it is not possible for anyone to link the information to a specific individual.
- 5.3. The duty of confidentiality requires that unless there is a statutory requirement or other legal reason to use information that has been provided in confidence, it should only be used for purposes that the subject has been informed about and has consented to. This duty is not absolute, but should only be overridden if the holder of the information can justify disclosure as being in the public interest (e.g. to protect others from harm).

Appendix A – LEGISLATION (continued)

- 5.4. Whilst it is not entirely clear under law whether or not a common law duty of confidence extends to the deceased, the Department of Health and relevant professional bodies accept that there is an ethical duty to respect the confidentiality of the dead.
- 5.5. Unless there is a sufficiently robust public interest justification for using identifiable information that has been provided in confidence then the consent of the individual concerned should be gained before disclosure of their information. Schedules 2 and 3 of the Data Protection Act 1998 apply whether or not the information was provided in confidence.
- 5.6. Where it is judged that an individual is unable to provide informed consent (due to age or condition), schedule 2 and 3 of the Data Protection Act 1998 must be satisfied (processing will normally need to be in the *vital interest* of the individual). 'Public functions' as outlined in schedule 2 , and 'medical purposes' as outlined in schedule 3 of the Data Protection Act 1998 are also likely to be very relevant.

6. Regulation of Investigatory Powers Act 2000

- 6.1. The Regulation of Investigatory Powers Act 2000 primarily deals with the acquisition and disclosure of information relating to the interception of communications, the carrying out of surveillance and the use of covert human intelligence. It is unlikely that this Act will have any implications on the sharing of personal information.

7. Caldicott

- 7.1. Although not a statutory requirement, NHS and Social Care organisations are committed to the Caldicott principles which encapsulate the above mentioned statutes when considering whether confidential information should be shared. These are:-
 - a) Justify the purpose(s) for using personal information.
 - b) Only use personal information when absolutely necessary.
 - c) Use the minimum amount of personal information that is required.
 - d) Access to personal information should be on a strict need to know basis.
 - e) Everyone with access to personal information must be aware of his/her responsibilities.
 - f) Everyone with access to personal information must understand and comply with legislation that governs personal information.

INTENTIONALLY LEFT BLANK

General Protocol for Inter-agency Information Sharing

Appendix B - GUIDANCE NOTES

1. Consent

- 1.1. In the past consent has all too often either been 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 explicit e.g. in writing.
- 1.2. In order to facilitate the sharing of personal information (without statutory grounds) it is essential that careful consideration should be given to obtaining explicit consent whenever possible, regardless of the person's age.
- 1.3. The key criterion that must be satisfied when obtaining consent is:

'that the person concerned should be mentally and emotionally capable of giving informed consent of his/her own free will'.
- 1.4. For the consent to be valid, the person concerned must:-
 - a) Have the capacity to take a particular decision, and
 - b) Have received sufficient information to make a decision, and
 - c) Not be acting under duress.
- 1.5. Consent may be given non-verbally, orally or in writing. In order to avoid any confusion or misunderstanding at a later date, non-verbal or oral consent should be witnessed and the details of the witness recorded.
- 1.6. To give valid informed consent, the person needs to understand in broad terms why their information needs to be shared, what type of information may be involved and who that information may be shared with.
- 1.7. The person should also be advised of their rights with regard to their information, namely:-
 - a) The right to withhold their consent.
 - b) The right to place restrictions on the use of their information.
 - c) The right to withdraw their consent at any time.
 - d) The right to have access to their records.

Appendix B – GUIDANCE NOTES (continued)

- 1.8. As well as discussing consent with the person, it is seen as good practice that the person should also be given such information in written form, in an appropriate format e.g. language, Braille.
- 1.9. To be valid, consent must be given voluntarily and freely, without any pressure or undue influence being exerted on the person by those seeking consent or family and friends of the person whose consent is being sought.
- 1.10. In general once a person has given consent, that consent may remain valid for an indefinite duration unless the person subsequently withdraws that consent.

For the purpose of the General Protocol, the consent duration should be time limited to the specific 'piece of work' that is being proposed.

It should be considered good practice to seek 'fresh' consent once the original piece of work is completed or there are significant changes in the circumstances of the person or work being undertaken.

- 1.11. If a person makes a voluntary and informed decision to refuse consent for their personal information to be shared, this decision must be respected unless there are sound legal grounds for not doing so.
- 1.12. A person, having given their consent, is entitled at any time to subsequently withdraw that consent. Like refusal, their wishes must be respected unless there are sound legal grounds for not doing so.
- 1.13. If a person refuses or withdraws consent, the consequences should be explained to them, but care must be exercised not to place the person under any undue pressure.

2. Capacity

- 2.1. For a person to have capacity, he/she 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.
- 2.2. The BMA has published guidance on the assessment of capacity.

3. Young Persons

- 3.1. Section 8 of the Family Law Reform Act entitles young people aged 16 or 17, having capacity, to give informed consent.
- 3.2. Following the case of Gillick v West Norfolk and Wisbech AHA [1986] AC 122, 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 capacity to consent.

Appendix B – GUIDANCE NOTES (continued)

- 3.3. It should be seen as good practice to involve the parent(s) of the young person in the consent process, unless this is against the wishes of the young person.

4. Parental Responsibility

- 4.1. The Children Act 1989 sets out persons who may have parental responsibility, these include:-
- a) The child's parents if married to each other at the time of conception or birth;
 - b) 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;
 - c) The child's legally appointed guardian;
 - d) A person in whose favour the court has made a residence order in respect of the child;
 - e) A local authority designated in a care order in respect of the child;
 - f) A local authority or other authorised person who holds an emergency protection order in respect of the child.

Note: Foster parents or guardians do not automatically have parental responsibility.

- 4.2. Whilst, 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, the provision of care, 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.

5. Obtaining Consent

- 5..1. For consent to be valid a number of criterion must be satisfied (see Consent 1. above). In order for consent to be obtained lawfully it is essential that all persons who may be expected to obtain consent for the sharing of personal information receive appropriate training and that under normal circumstances only those employees who have received training and been approved by management should seek consent.

Appendix B – GUIDANCE NOTES (continued)

6. Disclosure of Personal Information

- 6.1. The passing of personal information without either statutory cause or the consent of the person concerned, places both the agency and the individual member of staff at risk of prosecution.
- 6.2. It is therefore essential that all agencies who are party to the General protocol have in place policies and procedures governing who may disclose personal information and that such policies/procedures are communicated to all of their employees.

7. Disclosure with consent

- 7.1. Only staff who have been authorised to do so should disclose personal information about an individual service user.
- 7.2. Prior to disclosing personal information about an individual, the authorised member of staff should check the individual's file/record in order to ascertain:-
 - a) that consent to disclose has been given, and
 - b) the consent is applicable for the current situation, and
 - c) any restrictions that have been applied.
- 7.3. On the first instance of disclosure with respect to the particular situation, the person making the disclose should forward a copy of the individual's consent form to the receiving agency.
- 7.4. Disclosure of personal information will be strictly on a need to know basis and in accordance with any agreed Individual Protocol.
- 7.5. All information disclosed should be accurate and factual. Where opinion is given, this should be made clear to the recipient.
- 7.6. On disclosing personal information to another agency, a record of that disclosure should be made on the individual's file/record, this should include:-
 - a) When the disclosure was made.
 - b) Who made the disclosure.
 - c) Who the disclosure was made to.
 - d) How the disclosure was made.
 - e) What was disclosed.

Appendix B – GUIDANCE NOTES (continued)

7.7. The recipient of information should record:-

- a) The details of the information received.
- b) Who provided it.
- c) Any restrictions placed on the information that has been given e.g. 'not to be disclosed to the service user'.

8. Disclosure without consent

- 8.1. It is recognised that in certain emergency situations, such as vulnerable person investigations, speed is of the essence and inter-agency communication is of paramount importance and obtaining consent to disclose may be neither practical or expedient.
- 8.2. Staff involved in such situations all too often become completely focused on the core issue and often lose sight of the need to exercise caution when disclosing personal information.
- 8.3. Frequently staff are under the impression that the statute which enables them to undertake a particular duty also gives them the automatic right to collect, process and disclose whatever information they need. With very few exceptions, this is not the case.
- 8.4. The Data Protection Act 1998 is the key legislation governing the collection, processing and disclosure of personal information and almost all other statutes refer to it.
- 8.5. Disclosure of personal information without consent must be justifiable on statutory grounds, or a meet the criterion for claiming an exemption under the Data Protection Act. Without such justification, both the agency and the member of staff expose themselves to the risk of prosecution and liability to a compensation order under the Data Protection Act or damages for a breach of the Human Rights Act.
- 8.6. All agencies who are party to the General Protocol should set in place policies and procedures that deal specifically with the sharing of information under emergency situations e.g. major disaster.
- 8.7. All agencies should designate a person who has the knowledge and authority to take responsibility for making decisions on disclosure without consent. This person should hold sufficient seniority within the agency with influence on policies and procedures. Within the health and social care agencies it is expected that this person will be the Caldicott Guardian.
- 8.8. If disclosure is made without consent, the person making the disclosure must:-

Appendix B – GUIDANCE NOTES (continued)

- a) Advise the recipient accordingly.
 - b) Record the full details of the disclosure that has been made, including the reason why the decision to disclose was taken (statute or exemption); who made the disclosure and to who it was disclosed to.
- 8.9. The recipient of information that has disclosed without consent should record:-
- d) The details of the information received.
 - e) Who provided it.
 - f) Any restrictions placed on the information that has been given e.g. 'not to be disclosed to the service user'.
 - g) That the information was provided without consent, and the reason(s) why (if known).

9. Recording Consent

- 9.1. All agencies should have in place a means by which an individual, or their guardian/representative, can record their explicit consent to personal information being disclosed and any limitations, if any, they wish to place on that disclosure.
- 9.2. The consent form should indicate the following:-
- a) Details of the agency and person obtaining consent.
 - b) Details to identify the person whose personal details may/will be shared.
 - c) The purpose for the sharing of the personal information.
 - d) The organisation(s)/agency(ies) with whom the personal information may/will be shared.
 - e) The type of personal information that will be shared.
 - f) Details of any sensitive information that will be shared.
 - g) Any time limit on the use of the consent.
 - h) Any limits on disclosure of personal information, as specified by the individual.
 - i) Details of the supporting information given to the individual.

Appendix B – GUIDANCE NOTES (continued)

- j) Details of the person (guardian/representative) giving consent if appropriate.
- 9.3. The individual or their guardian/representative, having signed the consent, should be given a copy for their retention.
- 9.4. The consent form should be securely retained on the individual's file/record and that relevant information is recorded on any electronic systems used in order to ensure that other members of staff are made aware of the consent and any limitations.

10. Use Of Personal Information For Purposes Other Than Agreed

- 10.1. It is recognised that agencies who are party to the General Protocol may fulfil a number of roles. In fulfilling one particular role, they may be given privileged access to personal information which they may subsequently find could assist them in another role or be of wider interest to their organisation.
- 10.2. Personal information shared under this General Protocol will have been disclosed for a specific purpose, as defined in the Individual Protocol, and as such must only be used for that purpose.
- 10.3. Agencies wishing to use personal information given to them under the General Protocol for any purpose other than that defined in the Individual Protocol, or who may wish to disclose that information to any person other than those authorised to receive that information, must:-
- a) Inform the originator of their intention to use the information provided for a different purpose.
 - b) Obtain explicit consent from the individual(s) concerned before processing such information.
- 10.4. If the originator of the personal information considers that the purpose for which the information is proposed to be used is likely to be detrimental to their agency, or the individual(s) whose personal information it is proposed to use object, then that information should not be used for the proposed purpose.
- 10.5. Agencies wishing to use personal information that has been provided to them under the General Protocol for research or statistical purposes should ensure that policies and procedures are in place to guarantee that such personal information is anonymised.

INTENTIONALLY LEFT BLANK

General Protocol for Inter-agency Information Sharing

Appendix C - SPECIMEN INDIVIDUAL PROTOCOL

This Individual Protocol is made under the General Protocol for Inter Agency Information Sharing between:

Details of Agency 'A'

and

Details of Agency 'B'

1. Purpose for the sharing of personal information:

Statement defining the purpose(s) for the sharing of personal information.

2. Type of information that may be shared:

List in broad category terms the type of information that may need to be shared e.g.

'Basic' person details = name, address, date of birth etc.

Sensitive information = ethnic origin, criminal offences etc.

Relationships = next of kin, doctor etc.

3. Who else this information may be shared with:

The receiver of the personal information should list details of who else the person's information may need to be shared with e.g. not party to this Individual Protocol.

4. Restrictions on information shared:

If the provider agency of the personal information requires to place any additional restriction on the use of the information, these should be indicated here.

Signed: _____
For Agency 'A'

Date: _____

Signed: _____
For Agency 'B'

Date: _____

General Protocol for Inter-agency Information Sharing

Appendix D - SPECIMEN CONSENT FORM

Person Details
Family Name: _____
First Name(s): _____
Date of Birth: _____
System ID Number: _____

Responsible Worker
Worker's name: _____
Team: _____
Location: _____

The original document must be retained on the person's file

A copy of this document has been given/sent to the person on _____

Appendix D – SPECIMEN CONSENT FORM

Statement of responsible worker

I have explained to the person:-

- The reasons why we need their information.
- Who will have access to their information.
- How their information will be kept.
- How long their information will be kept for.
- Their rights under the Data Protection Act to access their records.
- Why we may need to share their information.
- Who we may need to share their information with.
- What information we may share.
- The restriction on the use of their information.
- Their right to decline the sharing of their information.
- Their right to withdraw consent to share information.
- The complaints procedure.

I have provided the person with copies of the following information booklets/leaflets.

(list with check boxes)

Remarks: _____

I am satisfied that the person mentioned on page 1 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.

Signed: _____ Date: _____

Name(PRINT): _____

Appendix D – SPECIMEN CONSENT FORM

Statement of person

Please read this form carefully, if you have any concerns please discuss them with the responsible worker before you sign – we are here to help you.

I have been given the information indicated on page 2 concerning the possible sharing of my information with those organisations listed for the purpose(s) described to me.

I understand that I have the right to restrict what information may be shared and with whom.

I understand that I have the right to withdraw my consent at any time.

I consent to Agency 'A' sharing my information on a need to know basis with 'partner' agencies listed below as they consider appropriate to my best interests.

(list organisations with check boxes)

Signed: _____ Date: _____

Person's Name:(please print) _____

If the person wishes to restrict the nature of the information which may be shared or with whom, those wishes should be indicated here:

If the person is unable to sign but has indicate their consent by other means, a witness should sign below to confirm consent. Young people may also wish their parent to sign here.

I confirm that the person mentioned on the front cover has indicated their consent for Agency 'A' to share their information.

Witness
Signature: _____ Date: _____

Witness Name:(please print) _____

General Protocol for Inter-agency Information Sharing

Appendix E - SPECIMEN INFORMATION LEAFLET

INTRODUCTION

In trying to help you, we may find that you will also need assistance from other organisations or agencies who we work with.

In the past we would have contacted the appropriate organisation and given them very basic information about you for example, your name and address. This has meant that the other organisation has had to contact you and often ask you the same questions that we have.

We appreciate that being asked the same questions by different people can be extremely frustrating, particularly if several organisations are involved, and that this often results in delays in getting you the right help.

It would be helpful if we could give other organisations who we may need to work very closely with more information about you. In many cases we can only do this if we have your permission.

WHO WILL YOU GIVE MY INFORMATION TO?

This will very much depend upon the type of help that you may need. For example if you need help with:-

A housing problem - we may need to contact the local authority housing section.

Care after leaving hospital - we may need to contact your GP or the local social services.

Advice on further education or careers - we may need to contact Connexions.

In most cases, we will tell you before we contact an organisation.

WHAT INFORMATION WILL WE GIVE?

Again this will also very much depend upon the type of help that you may need. Obviously we will need to give the other organisation your basic details (name, address, date of birth telephone number etc.). Any other personal information that you have given to us will only be passed on to the other organisation if we feel that it is:-

- directly relevant to your needs, and
- the other organisation needs to know it in order to help you, and

Appendix E – SPECIMEN INFORMATION LEAFLET

- it is in your best interest.

In most cases we will tell you what sort of information we may pass on to the other organisation before we actually do so.

WHAT SAFEGUARDS DO YOU HAVE?

All of the organisations with whom we work closely have signed something called an **Information Sharing Protocol**. This is an agreement that they will treat all information that we may give them about you as confidential, and they will only use it in connection with the help that we are trying to give you. If they want to use it for any other purpose they will need to ask your permission. All organisations who have signed the Information Sharing Protocol have in place strict rules governing the safe storage of and restricted access to your personal information.

HOW LONG DOES THE PERMISSION LAST?

If you give us permission to share your personal information, we will only do so whilst we are helping you with the current problem - however long that may take. Once we have finished working with you we will stop sharing your personal information.

If you need our help again at a later date we would ask for your permission again.

WHAT IF I SAY NO?

You are perfectly within your rights to say that you do not want us to pass your personal information onto another organisation at any time. You can refuse from the beginning or if you give your permission you can change your mind later.

We can only pass your personal information onto another organisation if we have your permission or we have a legal reason for doing so.

Please bear in mind, if we are unable to provide the other organisation with the information they may need this may delay you getting the help that you need.

CAN I LIMIT WHAT INFORMATION YOU CAN PROVIDE?

Yes. In most cases we will tell you the type of personal information that we feel we may need to pass on to the other organisation and who those organisations are likely to be. If there is something that you do not want us to pass on about you, we will make a note of it and respect your wishes.

CAN I SEE WHAT INFORMATION HAS BEEN PASSED ON?

All organisations that have signed up to the Information Sharing Protocol are bound by the Data Protection Act 1998 which gives you the legal right to see what information that organisation holds about you.

Appendix E – SPECIMEN INFORMATION LEAFLET

You will be given a copy of a leaflet which tells you how you may apply to see your record.

WHAT IF I FEEL MY INFORMATION IS BEING MIS-USED?

If you feel that your personal information is being mis-used, or you are not happy about the service you are getting, please tell us as quickly as possible so that we can take steps to correct the situation.

All organisations who have signed up to the Information Sharing Protocol have a complaints procedure that can deal with your concerns.

You will be given a copy of a complaints procedure leaflet which will explain how to make a complaint.