Cornwall General Protocol

Relating to the sharing of information

Version 1.3

CONTENTS

DOCUMENT HISTORY

This document has been distributed to:

Version	Date	Author	Released to	Comments
1.1	02/15	Simon Mansell	Public Sector Group	
1.2	02/16	Simon Mansell	Cornwall Executive Group	

This document requires the following approvals

Date	Version	Group
10/02/15	1.1	Public Sector Group
04/02/16	1.2	Cornwall Executive Group
18/01/2017	1.3	Cornwall Executive Group

INTRODUCTION

1 Background

1.1 The need to share information between Cornwall's partner agencies

1.1.1 While the public rightly expect that personal information held by Cornwall's statutory agencies will be properly protected, there is also a growing expectation that information will be shared in partnership where it is appropriate to do so.

1.1.2 Sometimes it is only when information held by different agencies is pulled together that a person is identified as needing additional or alternative services. Sharing information, therefore, is a key element to the delivery of high quality, cost effective and seamless public services.

1.1.3 In the past there have been both real and perceived barriers to the sharing of personal information. The Data Protection Act 1998 ('DPA') places an emphasis on protecting privacy which has, in the past, made agencies very reluctant to share information for fear of breaking the law. It also, however, meant that information which should have been shared was kept within one agency. There is a need to share information within the framework of clear understanding between agencies.

1.2 The need for a General Protocol

1.2.1 In the absence of specific statutory instruments enabling the sharing of personal information to take place, it is necessary that all partners concerned have a clearly defined framework to facilitate the sharing of personal information whilst respecting the rights of the individual.

1.2.2 The objective of this General Protocol is to provide a framework for professionals to facilitate the way in which personal and other information is shared to protect people who use public services in Cornwall. This is essential to enable public sector agencies to meet both their statutory obligations and the needs and expectations of the people they serve.

1.2.3 It is intended to assist both professionals and the public to feel confident that personal information is being shared in the right ways for the right reasons.

1.2.4 The purpose is to help agencies to work closer together, and provide the standards of service expected by both government and the public.

1.2.5 The following agencies are parties to this General Protocol and are referred to as the Parties throughout;

1. Cornwall Council;
2. Royal Cornwall Hospitals NHS Trust;
3. Plymouth Hospitals NHS Trust
4. NHS England South (South West)
5. Kernow Health Community Interest Company

6. Cornwall Voluntary Sector Forum
7. NHS Kernow;
8. Cornwall Partnership NHS Foundation Trust;
9. Department for Work and Pensions;
10. Devon and Cornwall Police;
11. Truro/Penwith College;
12. Cornwall College;
13. Corserv;
14. Environment Agency;
15. Homes and Communities Agency;
16. Highways Agency;
17. Skills Funding Agency
18. Coastline Housing
19. Falmouth University
20. Natural England
21. South West Ambulance Service NHS Foundation Trust
22. Cornwall and Isles of Scilly Local Enterprise Partnership
23. Council of the Isles of Scilly
24. Cornwall Association of Local Councils

2 Purpose

2.1 Overarching objectives

2.1.1 To set out a general framework for the secure and confidential sharing of personal information between public sector partner agencies to enable them to meet both their statutory obligations and the needs and expectations of the people they serve by helping the Parties to work closer together, and provide the standards of service expected by both government and the public.

2.1.2 The strategic purposes 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; and,

c) to enable parties to the General Protocol to review, account for, and learn how to improve what they do.

2.1.3 This General Protocol is an over-arching framework for sharing information between the Parties. It focuses on requirements for sharing personal information about customers, patients, clients or partners (' Service Users').

2.1.4 This General Protocol:

a) Clarifies the background on information sharing

b) Outlines the principles that need to underpin the process

c) Provides a framework within which the Parties can develop Individual Information Sharing Agreements (IISAs) for specific areas of service

d) Includes arrangements for monitoring and reviewing the use of the General Protocol and for responding to breaches

e) The General Protocol is not contractually binding but is to be used to set good practice standards that the Parties need to meet in order to comply with relevant duties in relation to the sharing of personal information

2.1.5 The General Protocol will be further supported by Individual Information Sharing Agreements (IISAs) between the individual partners which will set out the legal and/or statutory basis for sharing information, what information is to be shared and the formal obligations each of the partners undertakes to follow in sharing the information.

2.2 Helping to promote information sharing

2.2.1 The General Protocol is designed to help to remove barriers to effective information sharing and will assist in ensuring that service users receive integrated services which is a key principle of Government policy.

2.3 Helping to ensure compliance with legislation and guidance

2.3.1 In order to ensure compliance with the DPA, each of the Parties must satisfy themselves that the agencies they share information with have proper procedures in place in relation to the way in which they will hold and use that information.

2.3.2 The General Protocol includes procedural guidance to assist organisations in complying with legislation and guidance and in particular to:

a) help to ensure that consent to share personal information is obtained from the service user wherever this is necessary and this Protocol includes detailed procedural guidance on consent issues to assist staff in complying with legal requirements

b) help ensure that information is shared where there is a requirement to do so

c) help ensure that partner organisations have appropriate procedures in place to ensure compliance with legislation

The IISAs will require that these procedures are followed.

2.4 Raising awareness

2.4.1 The General Protocol seeks to raise awareness of the key information sharing issues and provides procedural guidance.

3 Status and Scope

3.1 Scope

3.1.1 This General Protocol sets out the way the agencies will deal in general terms with the sharing of personal information about service users and facilitate the development of IISA's. It does not relate to the sharing of personal information about staff.

3.1.2 The Protocol focuses on the sharing of "personal" and "sensitive" information about a data subject or subjects. This may also be referred to as "private" information in relation to the Human Rights Act 1998 (HRA) and "confidential" information.

Confidential information can be defined as;

- personal information of a private or sensitive nature; and
- information that is not already lawfully in the public domain or readily

available from another public source; and

- information that has been shared in circumstances where the person giving the information could reasonably expect that it would not be shared with others.

3.1.3 The Protocol comprises the common principles and procedures to be adopted wherever and whenever these organisations share information for these purposes.

3.2 Status

3.2.1 The Protocol is intended as guidance for staff in the performance of their duties with regard to the sharing of personal information about Service Users.

3.2.2 The Protocol applies to all staff directly employed by the Parties: such staff will be instructed that they must not share personal information except in accordance with the Protocol.

3.2.3 The Protocol does not constitute legal advice.

3.3 Governance and Review

3.3.1 This General Protocol will be governed by the Parties.

3.4 Formal approval, adoption, review and amendment

3.4.1 This Protocol will be formally signed off by all the Parties.

3.4.2 The Parties to this Protocol are to make their own internal arrangements to ensure this this Protocol is correctly signed.

3.4.3 Formal adoption will follow the signing of the document by the appropriate signatory of each partner agency.

3.4.4 This Protocol will initially be reviewed on an annual basis by the Parties.

3.4.5 This Protocol may only be amended in writing with any amendments signed by the all the Parties.

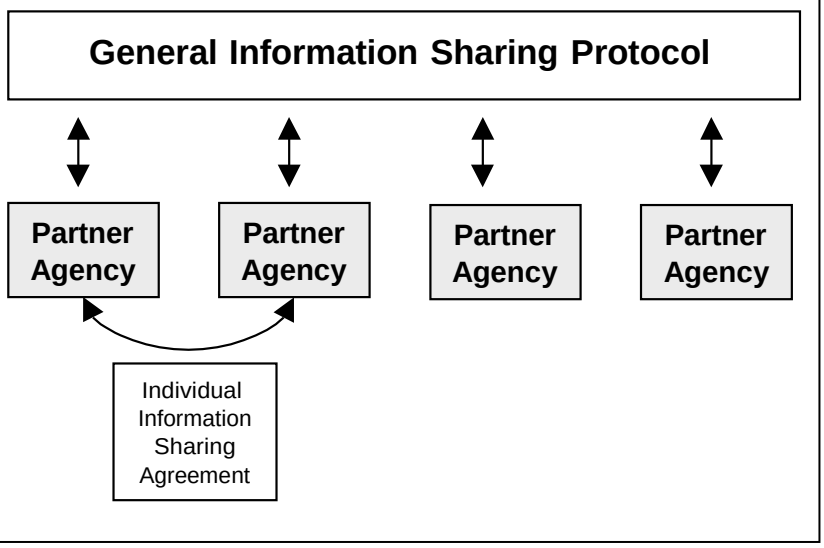
4 Protocols at two levels

4.1 Overview

4.1.1 The General Protocol (i.e. this document) provides the overall framework, common principles and procedures for the sharing of personally identifiable information between agencies. It will be supplemented and activated by IISA for specific areas of service between partner agencies (as indicated in Figure 1) that have signed this Protocol.

4.1.2 Each IISA will set out the detailed arrangements relevant to the proposed information sharing and, as a result, all IISAs will need to be fully compliant and consistent with this Protocol.

Figure 1:



5 The Individual Information Sharing Agreements

5.1 Working within the General Protocol

5.1.1 The IISA will specifically make reference to this Protocol and state that it is working within the framework of the Protocol.

5.2 Process for preparing an individual agreement

5.2.1 A specific process needs to be undertaken each time an IISA is set up. This is made up of a series of steps.

Figure 2: Process for preparing an Individual Information Sharing Agreement:

5.3 Proposal

5.3.1 The proposal is to define the key points of the agreement and provide an overall summary of the requirement for sharing the information. It should identify the legal, security and procedural matters relating to the proposed sharing.

5.4 Single point of contact

5.4.1 Each of the parties to the IISA need to nominate a designated officer who will serve as the single point of contact. This person will be responsible for day-to-day information sharing arrangements. In particular, this officer is responsible for:

a) Ensuring that the required information can be shared

b) Overseeing the sharing of the information

c) Ensuring the integrity of the information (that everything that needs to be disclosed is disclosed and that the quality of the data is appropriate for the purposes of the sharing)

d) Ensuring that the information is only received by authorised individuals or groups

e) Maintaining a record of disclosures

5.5 Legal Basis

5.5.1 The IISA must clearly indicate the legal basis for the proposed information sharing arrangements. This may be a statutory requirement or a statement of operational necessity.

5.6 Risk Assessment

5.6.1 A risk assessment needs to be undertaken by the parties to the IISA who need to agree specific measures relating to the handling of the information. The risk assessment will need to include:

a) an evaluation and statement around the nature of the information

b) detail how the information will be transferred

c) detail safeguards to protect the information during transit

d) detail safeguards for how this information will be held

e) highlight any risks and what can be done to mitigate these risks

5.7 Individual Information Sharing Agreement prepared and signed

5.7.1 The IISA must describe:

a) the process that was undertaken to prepare the agreement.

b) procedures for an annual review

6 Legal Basis for Sharing Information

6.1 Understanding the legal framework for information sharing

6.1.1 The legal framework within which public sector data sharing takes place is complex and overlapping and there is no single source of law that regulates public sector information sharing as set out at Appendix A.

6.2 How to approach questions around information sharing

6.2.1 In order to approach questions about information sharing the Protocol contains a checklist of considerations at Appendix B.

6.2.2 This requires each party to the IISA to:

a) Establish whether there is power to carry out the function to which

the information sharing relates

b) Check whether there are express statutory restrictions on the information sharing activity proposed, or any restrictions which may be implied by the existence of other statutory, common law or other provisions

c) Decide whether the sharing of the information would interfere with rights under Article 8 of the European Convention on Human Rights in a way which would be disproportionate to the achievement of a legitimate aim

d) Decide whether the sharing of the information would breach any obligations of confidence

e) Decide whether the information sharing would be in accordance with the DPA, in particular the Data Protection Principles

6.3 Inter-authority Freedom of Information Act (FOIA) 2000 requests

6.3.1 From time to time, a request may be made under FOIA for information that has been shared under this Protocol. These "inter-authority requests" are to be handled in accordance with the procedures set out below. The party that receives the FOIA request is responsible for answering the request. In doing so they must comply with the procedural requirements of FOIA (for instance, the requirement to identify any exemptions relied upon, and where necessary to explain the basis on which those exemptions are thought to apply).

6.3.2 The party that received the request, and the party that originally disclosed the information that is sought in the request, must seek if at all possible to agree whether the information is to be disclosed. The fullest consideration will be given to either party's claim that an exemption applies. If there is a dispute between two parties as to whether or not information should be disclosed, then the party who received the information is guided to consider the option of non-disclosure of the information. This will enable the applicant, if not satisfied with the outcome, to proceed to the review stage of the request.

6.3.3 The legal obligation is clear – the party receiving a request for information that it holds has a duty to disclose that information unless an exemption applies – this ensures that cross party requests are dealt with in a manner that will provide the best service to the applicant and ensure that decisions on the disclosure or non- disclosure of information are dealt with in a co-ordinated approach.

6.3.4 The Code under s.45 FOIA outlines further responsibilities on a public body to transfer requests for information that it does not hold, where it is believed to be held by another organisation. The public body will consider whether to:

a) consult the other organisation with a view to establishing whether information is held

b) transfer the request, either in full or the part of the request that

relates to information held elsewhere, with the consent of both the applicant and the other agency

6.3.5 The party that received the request must still advise the applicant that it does not hold the information (or part of it), consider the appropriateness of advising the applicant that the information is held elsewhere and seek the applicant's consent to transfer the request, or advise the applicant they should approach the information holder. Information held by the party receiving the request that can be disclosed must be so disclosed whilst the remainder of the request is transferred.

6.3.6 When dealing with such requests it is for the parties to consider who is the Data Controller and who is the Data Processor for the requested information.

7 Key principles for information sharing

7.1 The sharing of information by organisations under the Protocol will be based on the following principles:

8.1 Commitment to sharing information

8.1.1 Partner organisations recognise that multi-agency initiatives require a commitment to sharing personal information about service users in compliance with guidance and legislation.

9.1 Statutory duties

9.1.1 Partner organisations are fully committed to ensuring that they share information in accordance with their statutory duties.

9.2 Duty of confidentiality

9.2.1 All organisations which are party to this Protocol recognise the importance of the legal duty of confidentiality.

9.3 Consent

9.3.1 Wherever possible organisations will seek consent from the service user to share personal information. Where consent to disclose information is requested, the service user will be made fully aware of the information it is proposed to share and the purposes for which it will be used. If a person is unwilling to give consent, information will only be shared in exceptional circumstances and where there are appropriate statutory grounds for doing so.

9.4 Sharing without consent

9.4.1 Organisations will put appropriate procedures in place to ensure that decisions to share personal information without consent have been fully considered and comply with the requirements of the relevant legislation.

9.5 "Need to know"

9.5.1 Where it is agreed necessary for information to be shared, this will be done on a "need-to-know" basis only i.e. the minimum information consistent with the purpose for sharing will be provided.

9.6 Information kept confidential from the service user

9.6.1 Where an organisation believes that information supplied by them should be kept confidential from a service user, the outcome of this request and the reasons for taking the decision will be recorded.

9.7 Specific purpose

9.7.1 Partners will not abuse information that is disclosed to them under the specific purposes set out in the protocol. Information shared with a member of another organisation for a specific purpose will not be regarded by that organisation as intelligence for the general use of the organisation.

9.8 Fact / opinion

9.8.1 When disclosing information about an individual, professionals will clearly state whether the information being supplied is fact, opinion, or a combination of the two.

9.9 Use of anonymised information where possible

9.9.1 Personal information will only be disclosed where the purpose for which it has been agreed to share clearly requires that this is necessary. For all other purposes, information about individual cases will be anonymised.

9.10 Access to information

9.10.1 In line with the DPA, people will be fully informed about the information that is recorded about them on request. They will be able to gain access to information held about them under Subject Access Request procedures and to correct any factual errors that may have been made. If an organisation has statutory grounds for restricting a person's access to information about them, they will be told that such information is held and the grounds on which it is restricted under the DPA. Where opinion about a service user is recorded and they feel the opinion is based on incorrect factual information, they will be given the opportunity to correct the factual error and record their disagreement with the recorded opinion.

9.11 Staff awareness

9.11.1 Partner organisations will ensure that all relevant staff are aware of and comply with their responsibilities in relation to:

a) the Protocol

b) the IISA

c) the confidentiality of information about service users

d) the commitment to share information in accordance with guidance and legislation

OBLIGATIONS OF THE PARTIES

10 General undertakings by each party

10.1 Nominated Person

10.1.1 Those who are party to the General Protocol will have in place a nominated person who will be responsible for the day-to-day management of the scheme within their agency and the approval of this Protocol.

10.1.2 The person so nominated will have sufficient seniority within the agency to influence policies and procedures at executive level.

10.2 To ensure minimum standards for all Individual Information Sharing Agreements

10.2.1 In order to maintain a consistent approach, all those who are party to the General Protocol will ensure that any IISA's contains the following information:-

a) The full details of those who are party to the agreement

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

10.2.2 All IISA's will be approved by the respective lead person nominated within each agency.

10.2.3 Where information sharing protocols exist between agencies prior to signing up to the General Protocol, such protocols will remain valid until an IISA is entered into between the parties.

10.3 To comply with a duty of confidentiality

10.3.1 Personal information held by an agency shall always 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.

10.3.2 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.

10.3.3 In requesting disclosure of personal information from another agencies who are party to the General Protocol, those concerned will respect this responsibility and not seek to override the procedures which each party has in place to ensure that information is not disclosed illegally or inappropriately.

10.4 To comply with legislation

10.4.1 Those 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 DPA.

10.4.2 Each party therefore recognises the sensitivity of information about a person's racial or ethnic origin, political opinions including trade union membership, religious or other similar beliefs, 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 DPA in respect of such information.

10.4.3 Agencies who have 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.

10.5 Access to partner records

10.5.1 A service user making a valid request under section 7 of the DPA for access to his/her records in the form of a subject access request, will be fully informed, in accordance with the Act, about the information that is held about them by the agency approached.

10.5.2 Information that has been provided by another agency under an agreed IISA 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

10.5.3 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.

10.6 Complaints Procedure

10.6.1 Those who are party to this General Protocol shall have 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 IISA.

10.6.2 In the event of a complaint relating to the disclosure or the use of an individual's personal information that has been supplied/obtained under an agreed IISA all those who are a party to the I ISA will provide co-operation and assistance in order to resolve the complaint.

10.6.3 All parties to the IISA will ensure that the service users will be provided with information about the complaints procedures when consent is obtained or upon request.

10.7 Dealing with Information Security Breaches

10.7.1 All those 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.

10.7.2 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 Data Controller of the details of the breach

b) Inform the service user of the details of the breach

c) Advise the SIRO of the breach, advise the ICO/NHS Digital (formerly the Health and Social Care Information Centre) of the breach if necessary and take steps to investigate the cause

d) Take appropriate steps to avoid a repetition

10.7.3 On being notified that an individual's personal information has / 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

10.8 Requests to use Personal Information other than for an agreed purpose

10.8.1 It is recognised that those 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.

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

10.8.3 Personal information that has been obtained under an agreed IISA will not be regarded or used by the receiving party as intelligence for the general use of that organisation.

10.8.4 Those wishing to use information given under the General Protocol for any purpose other than that defined in the IISA, 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

10.8.5 Parties 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.

11 Consent

11.1 To seek informed explicit consent

11.1.1 Unless statutory exemptions are applicable, all those 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 IISA.

11.1.2 Consent will normally be obtained at the earliest opportunity and should be sufficient to cover the specific needs for a particular 'piece of work' or situation that is the subject of the IISA. It is essential to avoid the need to repeatedly seek consent over minor issues.

11.1.3 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.

11.1.4 For further guidance on consent, see Appendix C.

11.2 Time Limit on Consent

11.2.1 Consent to disclose personal information, obtained under an IISA, will be limited to the duration of the piece of work it relates to.

11.2.2 All those who are a party to General Protocol agree that once the named piece of work for which consent was originally obtained has been completed, that consent will be deemed to have lapsed.

11.2.3 In the event that similar, or subsequent additional work needs to undertaken with that individual, new consent to disclose will be obtained.

11.3 Recording consent

11.3.1 The party obtaining explicit consent to disclose an individual's personal information will retain the original consent, in whatever form is retained on the service users record.

11.3.2 The party obtaining explicit consent to disclose an individual's personal information will provide the person giving consent with a copy.

11.3.3 The party obtaining explicit consent to disclose an individual's personal information will provide a copy of the consent form to the other agency/agencies involved when the initial disclosure is made.

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

11.4 Amendment or Withdrawal of Consent

11.4.1 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 party 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.

11.4.2 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 exemption can be applied.

11.4.3 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 not doing so, or a legal exemption can be applied.

12 Disclosure

12.1 Disclosure Without Consent

12.1.1 All those who are party to the General Protocol will put in place procedures to ensure that decisions to disclose personal information without consent have been fully considered and that such decisions can be audited and defended.

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

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

12.1.4 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.

12.2 Disclosure of Information

12.2.1 Those 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.

12.2.2 Unless it is specified to the contrary, all personal information that is provided under an agreed IISA will be made available to the requestor record under section 7 of the DPA without the necessity of seeking the providers consent to disclose, subject to the exceptions as may be appropriate. 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.

12.3 Recording of Information Disclosed.

12.3.1 Those who are a party to the General Protocol will ensure that all personal information that has been disclosed to them under an agreed IISA will be recorded accurately on the individual's manual or electronic record in accordance with their agencies policies and procedures.

12.3.2 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.

12.4 Deceased person(s)

12.4.1 Agencies who are party to the General Protocol will exercise caution when contemplating the disclosure of personal information relating to a

deceased person. Although the DPA only applies to personal information of a living person, a duty of confidentiality may still apply after the person has died.

13 Storage

13.1 Storage of personal information

13.1.1 All those who are a 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.

13.2 Policies and Procedures relating to Access

13.2.1 All those who are a 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 it.

13.3 Destruction policies and procedures

13.3.1 All those who are a 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.

13.4 Secure Transfer

13.4.1 All those who are a 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) Verbal face-to-face and telephone

c) Facsimiles (safe haven)

d) Electronic mail (secure network or encryption)

e) Electronic network transfer

14 Staff awareness and training

14.1 Compliance with the Protocol

14.1.1 Those who are a party to the General Protocol will ensure that all staff are aware of, and comply with, their responsibilities and obligations with regard to the confidentiality of personal information about people who are in contact with their agency.

14.1.2 That all staff are aware of, and comply with the commitment of the organisations/agency to only share information legally and within the terms of an agreed IISA.

14.1.3 That all staff are aware of, and comply with the commitment that information will be shared on a need-to-know basis only.

14.1.4 That staff will be made aware that disclosure of personal information which cannot be justified, whether inadvertent or intentional may be subject to disciplinary action.

14.2 Training

14.2.1 All parties to the General Protocol will ensure that employees who need to share personal information under an IISA 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.

14.2.2 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.

15 Purposes for which information will be shared

15.1.1 Information will only be disclosed where the relevant agreed purpose for sharing clearly requires this. However, each party must have regard to its legal power in deciding whether they can share information for that particular purpose. The following range of purposes are agreed as justifiable for the transfer of personal information between the Parties as defined within the remit of this Protocol:

a) assessment of need, service delivery and treatment

b) assuring and improving the quality of care and treatment

c) monitoring, reporting and protecting public health

d) managing and planning future services

e) contracting for NHS and other services

f) training of staff

g) auditing agencies' accounts and performance

h) statutory notification of births, deaths and infectious diseases

i) medical, health or social care research (subject to ethical approval)

j) risk management

k) statistical analysis

l) compliance with court orders

m) prevention of crime or disorder

n) investigation of complaints or potential legal claims

o) medical reports/insurance requests

p) drug research/ trials

15.2 Relevant information

15.2.1 Consideration must be given to the extent of any personal information that is proposed to be disclosed, taking into account the circumstances of the proposed disclosure. It may not be necessary to disclose all information held regarding a service user and only such information as is relevant for the purpose for which it is disclosed should be released under the IISA to the recipient(s).

16 Agreement

16.1 The Parties hereby agree to:

16.1.1 Promote good practice in the sharing of personal information by ensuring compliance with the principles, purposes and processes of this Protocol

16.1.2 Take necessary action to identify and rectify any breaches of the Protocol and to have established policies and practices for dealing with complaints about the sharing of information

16.1.3 Facilitate the exchange of information where necessary to promote good quality services.

16.1.4 Ensure that no restrictions are placed on sharing personal information other than those that are specified in this Protocol

16.1.5 Ensure that service users are informed of their rights in respect of personal information, including right of access and the complaints procedure

16.1.6 Develop systems of implementation, dissemination, guidance, training and monitoring to ensure that the Protocol is known, understood and followed by all professionals who need to share personal information

16.1.7 Establish processes to review the use of the Protocol, in order to ensure that practice is in accordance with the requirements of the Protocol, and to take corrective action as needed

16.1.8 Develop and amend the Protocol according to any changes to the law or future national guidance

16.1.9 Develop data processing systems that ensure collected information is complete, accurate, kept up-to-date and relevant

16.1.10 Ensure that collected information is stored and transmitted securely

16.2 Indemnity

16.2.1 Disclosure of personal information without consent must be justifiable on

statutory grounds, or a meet the criterion for claiming an exemption under the DPA. Without such justification, both the party who has disclosed the data and the member of staff expose themselves to the risk of prosecution and liability to a compensation order under the DPA or damages for a breach of the HRA.

16.2.2 Where a disclosing party provides information to a requesting party both parties shall assume that both the request and the disclosure are compliant with the requirements of the DPA.

16.2.3 If subsequently it is found that either the request for, or the disclosure of, information is in contravention of the requirements of the DPA, the agency that originally breached the requirements of the DPA, either in requesting or disclosing information, shall indemnify the other agency against any liability, cost or expense thereby reasonably incurred, provided that this indemnity shall not apply:

a) Where one party originally found to be in breach of the DPA did not know and, acting reasonably had no reason to know, that it had acted in breach of the DPA either in requesting or disclosing information

b) unless either party notifies the other as soon as reasonably practical of any action, claim or demand against itself to which it considers this indemnity may apply, permits the other party to deal with the action, claim or demand by settlement or otherwise, and renders all reasonable assistance in doing so

16.3 Agreement

16.3.1 In consideration of the provision of information in accordance with this General Protocol within Cornwall each person or authority being a Party undertakes to indemnify each of the other Parties against any liability which may be incurred as a result of the provision of such information.

16.3.2 Provided that this indemnity shall not apply:-

a) 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 Party providing the information

b) unless the Party claiming the benefit of this indemnity notifies a Party 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 Party to deal with the action claim or demand by settlement or otherwise and renders to such Party all reasonable assistance in so doing

c) to the extent that a Party claiming the benefit of this indemnity makes any admission which may be prejudicial to the defence of the action claim or demand

17 Signatories

a. Signed on behalf of Cornwall Council by;

Name:

Signature:

b. Signed on behalf of Royal Cornwall Hospitals NHS Trust by:

Name:

Signature:

c. Signed on behalf of Plymouth Hospitals NHS Trust by:

Name:

Signature:

d. Signed on behalf of NHS England South (South West) by:

Name:

Signature:

e. Signed on behalf of Kernow Health Community Interest Company by:

Name:

Signature:

f. Signed on behalf of Cornwall Voluntary Sector Forum by:

Name:

Signature:

g. Signed on behalf of NHS Kernow by;

Name:

Signature:

h. Signed on behalf of Cornwall Partnership NHS Foundation Trust by;

Name:

Signature:

i. Signed on behalf of Job Centre Plus by;

Name:

Signature:

j. Signed on behalf of Devon and Cornwall Police by;

Name:

Signature:

k. Signed on behalf of Truro/Penwith College by;

Name:

Signature:

l. Signed on behalf of Cornwall College by;

Name:

Signature:

m. Signed on behalf of Corserv by;

Name:

Signature:

n. Signed on behalf of the Environment Agency by;

Name:

Signature:

o. Signed on behalf of the Homes and Communities Agency by;

Name:

Signature:

p. Signed on behalf of Highways England by:

Name:

Signature:

q. Signed on behalf of the Skills Funding Agency by:

Name:

Signature:

r. Signed on behalf of Falmouth University by:

Name:

Signature:

s. Signed on behalf of Natural England by:

Name:

Signature:

t. Signed on behalf of South West Ambulance Service NHS Foundation Trust by:

Name:

Signature:

u. Signed on behalf of Cornwall and Isles of Scilly Local Enterprise Partnership by:

Name:

Signature:

v. Signed on behalf of the Council of the Isles of Scilly by:

Name:

Signature:

w. Signed on behalf of Cornwall Association of Local Councils

Name:

Signature:

APPENDICES

18 APPENDIX A - Legislation

18.1 Introduction

18.1.1 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.

18.1.2 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 the use of personal information (collection; use; storage; destruction; protection etc.) already exists namely, the Data Protection Act 1998 ('DPA').

18.1.3 The DPA, in most cases, is the key to the use of personal information and links into most other legislation. The DPA sets out to govern the collection, use, storage, destruction and protection of a living person's identifiable information (Personal Data). In general, recorded information held by public authorities about identifiable living individuals will be covered by the DPA. It is important to take account of whether the information is held in paper records or in automated form (such as on computer or on a CCTV system): some of the provisions of the DPA do not apply to certain paper records held by public authorities. Broadly speaking, the eight data protection principles set out in Schedule 1 to the DPA, and discussed further below, will apply to records held in a "relevant filing system" or an "accessible record".

18.1.4 The DPA does not set out to prevent the sharing of personal information. To the contrary, providing that the necessary conditions of the DPA can be met, sharing is perfectly legal.

18.2 Administrative Law

18.2.1 The principles of administrative law regulate the activities of public bodies; these principles are mainly enforced by way of claims for judicial review in the courts. Local authorities derive their powers entirely from statute and cannot act outside those limited statutory powers. Most of these statutory powers relate to specific local authority functions.

18.2.2 There is no general statutory power to disclose information, and there is no general power to obtain, hold or process information. As a result, it is necessary to consider the legislation that relates to the policy or service that the information sharing supports. From this, it will be possible to determine whether there are express powers to share information, or whether these can be implied. Express powers to share information are relatively rare and tend to be confined to specific activities and be exercisable only by named bodies.

18.3 Administrative powers

18.3.1 If a public body does not have the power or vires to collect, use or share information it will be acting unlawfully and the fact that an individual may have consented would not make the activity lawful.

18.3.2 Express statutory powers: Express statutory powers can be permissive or mandatory. Express permissive statutory powers (or gateways) to share information include, for example, section 115 of the Crime and Disorder Act 1998 (which allows persons to share information with relevant authorities where disclosure is necessary or expedient for the purposes of the Act) and regulation 27 of the Road Vehicles (Registration and Licensing) Regulations 2002 (which, among other things, permits the Secretary of State to make particulars in the vehicle registration register available for use by a local authority for any purpose connected with the investigation of an offence or of a decriminalised parking contravention). Examples of mandatory statutory gateways include: section 17 of the Criminal Appeal Act 1995, which makes it obligatory for a public body to provide information, when requested, to the Criminal Cases Review Commission in connection with the exercise of its functions; and section 6 of the Audit Commission Act 1998, which imposes a legal obligation on the Council to provide relevant information to the Audit Commission.

18.4 Data Protection Act 1998

18.4.1 The key principles of the DPA are:-

a) 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

b) Personal Data shall be obtained and processed for only one or more specific and lawful purpose(s)

c) Personal Data shall be adequate, relevant and not excessive in relation to the specified purpose(s)

d) Personal Data shall be accurate and kept up to date

e) Personal Data shall not be held for longer than is necessary

f) Processing of Personal Data must be in accordance with the rights of the individual

g) Appropriate technical and organisational measures should protect Personal Data

h) Personal data should not be transferred outside the European Union unless adequate protection is provided by the recipient

18.4.2 With few exceptions the DPA requires anyone processing personal

information to register with the Information Commissioner.

18.4.3 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's Office.

18.4.4 The first and second principles of the DPA are crucial when considering information sharing. In essence, these require that personal information should be obtained and processed fairly and lawfully and that personal information should not be used for a purpose(s) incompatible with the original purpose.

18.4.5 Schedules 2 and 3 of the Act set out conditions that must be met before personal information can be processed fairly and lawfully. For personal information to be processed lawfully, one of the conditions in Schedule 2 must be met. For sensitive personal information, one of the conditions in Schedule 3 must also be met.

18.4.6 Sensitive information, as defined by the DPA, 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.

18.4.7 In order for there to be no misunderstanding, on anyone's part, it is 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.

18.4.8 There are circumstances where information can be shared even if informed consent has not been given. These include the following:

a) Section 29 of the DPA 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

18.4.9 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.

18.4.10 For the purposes of the Human Rights Act 1998, Article 8 – Right to respect for private and family life, would need to be considered.

18.4.11 The DPA 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 be 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 DPA enforced

18.4.12 Section 7 of the Act, gives an individual the right to access the information held about themselves, via a subject access request, irrespective of when the information was recorded or how it is stored (manual or electronic).

18.4.13 Disclosure of information held on an individual's record that identifies or has been provided by a third party is subject to certain restrictions.

18.4.14 The DPA provides the holder of the information a limited number of exemptions to decline/refuse access to an individual's record which are set out under Part IV of the DPA.

18.4.15 The DPA does not apply to personal information relating to a deceased person.

18.4.16 The DPA 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.

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

18.4.18 **Schedule 2** of the DPA 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, or

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.

18.4.19 **Schedule 3** of the DPA 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:-

c) By right or obligation under law, or

d) To protect specific vital interests of the individual or other persons, where consent cannot be given by or on behalf of the individual or,

e) In the course of legitimate activities of specified non-profit organisations, with extra safeguards, or

f) Information already publicly released by the individual.

g) Legal, judicial, government or crown reasons, or

h) Medical purposes, or

i) To monitor equality of opportunity, or

j) By order of the Secretary of State.

18.5 Human Rights Act 1998 and European Convention on Human Rights

18.5.1 The Human Rights Act 1998(the HRA) gives further effect to the principal rights guaranteed by the European Convention on Human Rights (the Convention). In general, it is unlawful under the HRA for a public authority to act inconsistently with any of the Convention rights.

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

18.5.3 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.

18.5.4 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.”

18.5.5 In the event of a claim arising from the HRA 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. "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".

18.6 Crime and Disorder Act 1998

18.6.1 The Crime and Disorder Act 1998 (the 'CDA') 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.

18.6.2 Section 115 of the Act provides a power (not a statutory duty) to exchange information between partners where disclosure is necessary to support the local Community Safety Strategy or other provisions in the CDA. This power does not over ride other legal obligations such as compliance with the DPA, the HRA or the common law of confidentiality.

18.6.3 Section 115 of the CDA 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 CDA.

18.6.4 Whilst all agencies have the power to disclose, section 115 of the CDA 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.

18.7 Common Law Duty of Confidentiality

18.7.1 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.

18.7.2 '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 were a professional

relationship may exist e.g. doctor/patient, social worker/client; lawyer/client etc.

18.7.3 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.

18.7.4 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, just making the information as confidential does not necessarily mean it is under law.

18.7.5 Whilst it is not entirely clear under law whether or not a common law duty of confidence extends to the deceased, and all relevant professional bodies accept that there is an ethical duty to respect the confidentiality of the dead.

18.7.6 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. In addition, the data protection principles (including the requirements of Schedules 2 and 3 of the DPA) apply whether or not the information was provided in confidence.

18.7.7 Where it is judged that an individual is unable to provide informed consent (due to age or condition), then in order to avoid a breach of the common law duty of confidentiality it will usually be necessary to consider whether, a Schedule 2 and (in the case of sensitive personal data) Schedule 3 condition of the DPA will be satisfied, notwithstanding the absence of consent. Processing might for instance be lawful as being in the vital interest of the individual. 'Public functions' as outlined in Schedule 2, and 'medical purposes' as outlined in schedule 3 of the DPA are also likely to be very relevant.

18.8 Regulation of Investigatory Powers Act 2000

18.8.1 The Regulation of Investigatory Powers Act 2000 ('RIPA') 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.

18.9 The Children Act 2004

18.9.1 The Children Act 2004 created the legislative framework for developing more effective and accessible services focused around the needs of children, young people and families by ensuring co-operation, clearer accountability and safeguarding of children.

18.9.2 Main provisions of the Act:

a) A Children's Commissioner

b) A new duty on agencies to co-operate to improve the well-being of children and young people

c) A duty to safeguard and promote the welfare of children

d) A power to set up a new database with information about children

e) Local Safeguarding Children Boards

f) Children and young people's plans

g) Director of Children's Services and Lead Member

h) A framework for inspection and joint area reviews

i) New powers of intervention in failing authorities

j) A duty to promote the educational achievement of looked after children

k) Ascertaining children's wishes

l) Additional items include: private fostering, child minding and day care, adoption review panels, grants in respect of children and families and Child Safety Orders.

19 APPENDIX B - Checklist of considerations

19.1 Purpose

19.1.1 This part of the Protocol is designed as a guide to assist in determining how to establish the basis for information sharing. A new information sharing initiative may involve two or more public bodies who wish to share information with each other in order to set up a central database of useful information that they may each access. This information could be, for example, limited to up-to-date client names and addresses. Alternatively, it could be information about children thought to be at risk of serious physical harm. Consideration will need to be given to the following issues:

- Does the body that intends to hold and administer the database have the power to do so?
- Is the existing data that is to be shared subject to statutory prohibitions, whether express or implied?
- Is Article 8 of the ECHR engaged in that will the proposed data sharing interfere with the right to respect for private and family life?
- If Article 8 of the ECHR is engaged, is the interference (a) in accordance with the law; (b) in pursuit of a legitimate aim; and (c) necessary in a democratic society?
- Is the information confidential i.e. does it (a) have the necessary quality of confidence; (b) was the information in question communicated in circumstances giving rise to an obligation of confidence?; (c) has there been an unauthorised use of that material?
- If the information is confidential is there an overriding public interest that justifies its disclosure?
- Do the eight principles in Schedule 1 of the DPA apply i.e. is the information personal data held on computer or as part of a relevant filing system or an accessible record?
- If Schedule 1 of the DPA applies, can the requirement of fairness in the First Data Protection Principle be satisfied?
- Can one of the conditions in Schedule 2 be satisfied?
- Can the requirement of compatibility that is in the Second Data Protection Principle be complied with?
- Do any of the exemptions that are set out in the DPA apply?

20 APPENDIX C - Consent: Guidance notes

20.1 Consent

20.1.1 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.

20.1.2 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.

20.1.3 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'.

20.1.4 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.

20.1.5 Consent may be given non-verbally, orally or in writing. In order to avoid any confusion or misunderstanding at later date, non-verbal or oral consent should be witnessed and the details of the witness recorded.

20.1.6 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.

20.1.7 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

20.1.8 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.

20.1.9 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.

20.1.10 In general once a person has given consent, that consent may remain valid for an indefinite duration unless the person subsequently withdraws that consent.

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

20.1.12 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.

20.1.13 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.

20.1.14 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.

20.1.15 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.

20.2 Capacity

20.2.1 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.

20.3 Young Persons

20.3.1 Section 8 of the Family Law Reform Act entitles young people aged 16 or 17, having capacity, to give informed consent.

20.4 Parental Responsibility

20.4.1 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)

20.4.2 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.

20.5 Obtaining Consent

20.5.1 For consent to be valid a number of criterion must be satisfied. 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.

20.6 Disclosure of Personal Information

20.6.1 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.

20.6.2 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.

20.7 Disclosure with consent

20.7.1 Only staff who have been authorised to do so should disclose personal information about an individual service user.

20.7.2 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

20.7.3 On the first instance of disclosure with respect to the particular situation, the person making the disclosure should forward a copy of the individual's consent form to the receiving agency.

20.7.4 Disclosure of personal information will be strictly on a need to know basis and in accordance with any agreed IISA.

20.7.5 All information disclosed should be accurate and factual. Where opinion is given, this should be made clear to the recipient.

20.7.6 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

20.7.7 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'

20.8 Disclosure without consent

20.8.1 It is recognised that in certain emergency situations, such as safeguarding investigations, speed is of the essence and inter-agency communication is of paramount importance and obtaining consent to disclose may be neither practical nor expedient.

20.8.2 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.

20.8.3 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.

20.8.4 The DPA is the key legislation governing the collection, processing and disclosure of personal information and almost all other statutes refer to it.

20.8.5 Disclosure of personal information without consent must be justifiable on statutory grounds, or a meet the criterion for claiming an exemption under the DPA. 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 DPA or damages for a breach of the HRA.

20.8.6 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.

20.8.7 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 heath and social care agencies it expected that this person will be the Caldicott Guardian.

20.8.8 If disclosure is made without consent, the person making the disclosure must:-

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

20.8.9 The recipient of information that has disclosed without consent 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'

d) That the information was provided without consent, and the reason(s) why (if known)

20.9 Recording Consent

20.9.1 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.

20.9.2 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

j) Details of the person (guardian/representative) giving consent if appropriate

20.9.3 The individual or their guardian/representative, having signed the consent, should be given a copy for their retention.

20.9.4 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.

20.10 Use Of Personal Information For Purposes Other Than Agreed

20.10.1 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.

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

20.10.3 Agencies wishing to use personal information given to them under the General Protocol for any purpose other than that defined in the IISA, 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

20.10.4 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.

20.10.5 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.

21 APPENDIX D - Protocol Management Procedures

21.1 Circulation of the Protocol

21.1.1 This Protocol and the IISA will be introduced to managers, front line and field workers following internal training plans and procedures.

21.1.2 Copies of the Protocol will be circulated to all relevant staff, in line with each organisation's internal distribution procedures and guidelines. Wherever possible, the document will be available to staff online.

21.1.3 A strategy for disseminating the Protocol to the public will be developed in line with the need to ensure that members of the public are fully informed about their rights in relation to disclosure of information.

21.1.4 The Protocol will be published, wherever possible, on the web sites of the organisations party to the protocol and made available at public information points. Each partner organisation will keep sufficient copies to enable the document to be readily available to members of the public who require it.

21.2 Monitoring and Reviewing procedures

21.2.1 The Protocol will be subject to annual review.

21.2.2 Following the introduction of this Protocol, its use and application will be closely monitored until the date of the first formal review. During this period, changes will only be considered if the issues and problems identified are felt to be a significant barrier to information exchange.

21.3 Evaluation of the Protocol

21.3.1 Staff in all organisations will be required to log and report responses and behaviour that they believe are not in accordance with the Protocol. Breaches will be analysed to ensure that problems with the implementation of the Protocol are addressed before they become a major issue.

21.3.2 The Parties to this Protocol will be responsible for ensuring that their own staff are advised of both this Protocol and IISA's made under it which are relevant to their role.

21.3.3 Complaints received by organisations will be analysed to determine whether they relate to a breakdown or inadequacy of the Protocol or the IISA. All organisations party to the Protocol will establish a procedure by which complaints regarding inappropriate use or disclosure of information are reported to the body responsible for the security of that information.

21.4 Reporting Breaches of the Protocol

21.4.1 All breaches are to be logged, investigated, and the outcome noted.

21.4.2 The following sets out the types of incidents will be logged and investigated however, it should be noted that this list is not exhaustive and the Parties to this Protocol will be responsible for determining if a matter should be logged and investigated;:

- Refusal to disclose information
- Conditions being placed on disclosure
- Delays in responding to requests
- Disclosure of information to members of staff who do not have a legitimate reason for access
- Non-delivery of agreed reports
- Inappropriate or inadequate use of procedures e.g. insufficient information provided
- Disregard for procedures
- The use of data/information for purposes other than those agreed in the protocol
- Inadequate security arrangements.

21.4.3 In the event that a potential breach is logged all Parties to this Protocol will;

- Report the potential breach to those parties to the protocol directly affect by it
- Keep these parties informed as the investigation proceeds
- Report all matter that are logged on a quarterly basis to Public Sector Group

21.5 Breaches noted by members of staff:

21.5.1 A member of staff working on behalf of any organisation party to the Protocol who becomes aware that the procedures and agreements set out in the Protocol are not being adhered to, whether within their own or a partner organisation, should first raise the issue with the line manager responsible for the day-to-day management of the Protocol.

21.5.2 The manager should record the issue and check whether the concern is justified. If the manager concludes that the Protocol is being breached, he or she should first try to resolve it informally. If the matter can be resolved in this way, the outcome should be noted and forwarded to the designated person (the person responsible for monitoring the protocol during the pilot phase) who should file the details in a 'breaches log'.

21.5.3 The line manager should inform the member of staff who raised the issue of the outcome prior to submitting the issue to the designated

person. If the member of staff is not satisfied with the response they should be able to record their comments on the form prior to submission.

21.5.4 A time limit of 10 days should be allowed for informal negotiation. At the end of this period, the details of any actions and the outcome of negotiations should be noted and passed to the designated person for logging and for reporting.

21.6 Breaches alleged by a member of the public:

21.6.1 Any complaint received by, or on behalf of, a member of the public concerning allegations of inappropriate disclosure of information will be dealt with via the internal complaints procedures of the organisation who received the complaint: Any disciplinary action will be an internal matter for the organisation concerned.

21.6.2 In order to monitor adherence to and use of the Protocol, procedures should be established within each organisation by which complaints relating to the inappropriate disclosure of information is passed by the complaints officer to the officer designated to deal with breaches of the Protocol. The designated officer should report any complaints of this nature to the equivalent officer in each agency.

21.6.3 All alleged breaches of the Protocol, whether proven or not, should be analysed as part of the formal review of the Protocol.