Protocol
for Sharing Information
Between

- **NHS Dumfries and Galloway**
- **Dumfries and Galloway Council**
- **Dumfries and Galloway Constabulary**

This document has been supplied for use with the Public Records (Scotland) Act 2011
http://www.nas.gov.uk/recordKeeping/prsa/modelPlanGuidance.asp

Document History

For more information on the status of this document, please contact	Duncan Card Data Sharing Manager High Centre Crichton Hall Bankend Road Dumfries DG1 4TG t : 01387 244 237 e : Duncan.Card@nhs.net Duncan.Card@Dumgal.gov.uk

Revision History

Version	Date	Summary of Changes	Author
0.1	09/11/07	Generic version of protocol for children and adults created from IAF project gold standard original	SSA team
0.2	03/09/09	Protocol updated following consultation	DSM
1.0	17/12/09	Removal of reference to SCRA	DSM

Approvals

This document requires the following approvals

Name	Signature	Title	Date of Issue	Version

Distribution

Name	Title	Date of Issue	Version

Table of Contents

1. Introduction

1.1.1 Information sharing between partner agencies is vital to the provision of co-ordinated and seamless health and social care services. The Parties have developed a two level approach to Information Sharing consisting of this Protocol supported by a series of Guidance Procedures. This Protocol exists to ensure that information can be shared in a way, which satisfies both the legal and professional obligations of the Parties and their respective staff, and the legitimate expectations of service users. It extends to all types of information sharing relevant to the provision of both adult and children's health and social care services. It cannot therefore be used as an operational guidebook or manual. It simply defines, at a high level, general agreed principles for information sharing between the Parties. Each Information Sharing context will require a unique set of Guidance Procedures, which should be referred to for guidance on specific applications.

1.1.2 Whenever a subsequent agreement is made to share information between the local partners, further Guidance Procedures will need to be developed on that particular information sharing application, in line with this Protocol. In practice, this will allow additional projects to concentrate resources on the development of practical policies and procedures rather than wasting time redefining generally agreed principles.

1.1.3 Information is shared between the Parties, for a variety of purposes, mainly to assist them in complying with their respective statutory duties or to improve service delivery. A full description of the purposes of information exchange is provided in paragraph 4.1.

1.2 Parties to the Protocol

1.2.1 This Protocol is a legal contract between National Health Service Dumfries & Galloway, Dumfries & Galloway Council and Dumfries & Galloway Constabulary who are collectively referred to as "the Parties". This shall include any statutory successors to the named Parties (e.g. as a consequence of local government or NHS reorganisation).

1.3. Background

1.3.1 The aim of public policy is that citizens receive the health and social care services that they need and that the organisation of services should not impede or debase the service provided. This clearly requires agencies to work effectively and efficiently together to tailor services to the particular circumstance of each individual. Sharing information about a Service User between the Parties is vital to the provision of co-ordinated and seamless care to that Service User.

1.3.2 Attempts and proposals to exchange information previously have encountered both real and perceived barriers at both operational and managerial levels. These barriers may be linked to the legal requirements or ethical standards which must be satisfied but sometimes these impediments have focused on less relevant issues. The value of information sharing has often been reduced by such problems as different interpretations of the legal requirements, misunderstandings in the use of language or inefficiencies in communication channel. These barriers have led to concerns and to uncertainties about when, with whom and how information may be shared. This Protocol has been developed to address these concerns. The Protocol will need to be supported by training and procedures to ensure that boundary-crossing processes work smoothly and are managed

effectively. This Protocol is designed to ensure that the exchange of information which is necessary to permit multi-agency and multi-disciplinary service provision can proceed in a way which conforms with all applicable laws and safeguards the rights of the Parties and Service Users and in particular, provides a framework for secure and confidential storing of information which allows Service Users to be informed as to how and why their details will be exchanged between the Parties.

1.4 Development process

1.4.1 The Protocol has been developed by all the Parties. The Protocol adheres to the national model authorised by the Scottish Government's Health Department. The intention has been to develop an over-arching statement of law and policy for all information-sharing applications. This will be supplemented by Guidance Procedures for specific applications, which will adopt the common core procedures as their base line. The Guidance Procedures will set out the specific arrangements and responsibilities designated, any additional requirements, and the service level agreements for each application. This Protocol is expected to cut down the development time for Guidance Procedures.

1.4.2 This Protocol supersedes an earlier Protocol for Sharing Information between NHS Dumfries & Galloway and Dumfries & Galloway Council. The earlier Protocol will be terminated on the 1st October 2009 when this Protocol comes into force.

1.5 Overarching Principles

1.5.1 It shall be a fundamental principle of this Protocol that, except in circumstances such as those outlined in section 7.4, all processing of Service User personal Data by the Parties shall be processed on the basis of the informed consent of the Service User.

1.5.2 The Parties shall apply the presumption that all Service Users aged 12 years or older possess the capacity to give, withhold or modify the consent referred to in Clause 1.5.1 and Section 7 of this Protocol.

1.5.3 The presumption of capacity referred to in Clauses 1.5.2 shall only be regarded as having been rebutted if the procedures for establishing incapacity laid down in Appendix 4 have been followed.

1.5.4 It shall be a fundamental principle of this Protocol that the confidentiality of Service User Personal Data is paramount, except where required by statute, or where this duty is overridden by a clear duty to disclose information to other Parties for example, to ensure the safety of a child or of a vulnerable adult, to prevent serious crime, to exercise a statutory function or to aid in the apprehension and/or prosecution of offenders who are suspected of serious crime. The Parties agree that no use shall be made of that data which is inconsistent with both the aims of providing health services, social care or other services to Service Users, and with Service User's rights of confidentiality; except to the minimum extent required by law or to the extent that the Service User has expressly consented to that further use. The Parties agree to use their best endeavours to safeguard the confidentiality of the Service User Personal Data.

1.5.5 The Department of Health and professional bodies responsible for setting ethical standards for health and social work professionals accept that the common law duty of

confidentiality extends to the deceased, and accordingly the provisions of this Protocol shall apply to Personal Data relating to deceased Service Users and former Service Users as it applies to Service User Personal Data, save as amended by Clauses 1.5.6 and 1.5.7.

1.5.6 The provisions of this Protocol shall not apply to personal information relating to the deceased to the extent that failure to disclose such data would be prejudicial to the apprehension or prosecution of offenders, or the prevention or detection of crime, or would preclude the exercise of a statutory function.

1.5.7 The provision of this Protocol shall not apply to personal information relating to deceased Service Users to the extent that the Access to Health Records Act 1990 (so far as relating to such Data) requires it to be disclosed.

2. Objectives and Purpose of this Protocol

2.1 This Protocol is intended to:

2.1.1 Set out the principles which underpin the exchange of information between the Parties detailed in section 1.2;

2.1.2 Define the specific purposes for which the Parties have agreed to share information to meet their responsibilities to protect, support and care for Service Users;

2.1.3 Describe the roles and structures which will support the exchange of information between the Parties;

2.1.4 Describe at a high level the procedures which will ensure that information is disclosed in line with statutory responsibilities. More detailed procedures for individual information sharing contexts will be covered in particular Guidance Procedures;

2.1.5 Describe the arrangements which have been agreed for exchanging information;

2.1.6 Describe the security procedures necessary to ensure that the confidentiality of information exchanged is maintained;

2.1.7 Set out the responsibilities of the Parties to implement internal arrangements to meet the requirements of the protocol; and

2.1.8 Describe how this Protocol will be implemented, monitored and reviewed.

3. General Principles

3.1 Key legislation and guidance

3.1.1 Since 1 March 2000, the key legislation governing the protection and use of identifiable Service User information (Personal Data) has been the Data Protection Act 1998 (referred to as "DP Act 1998" in the rest of this Protocol). Any information sharing by the Parties requires to be both 'intra vires' i.e. within their legal powers, and compliant with the DP Act 1998. If a Party acts outwith its legal powers, even compliance with the DP Act 1998 cannot render that act lawful. There is no general statutory power to share information. Express powers to share information are relatively rare and are usually restricted to specific activities. However, the Parties, as public authorities, have various general powers, which allow them to carry out their functions, from which power to share information can often be implied. In general, unless there is a specific prohibition or restriction on a particular information sharing exercise, the key consideration will be whether the information can be shared in accordance with the DP Act 1998.

3.1.2 The DP Act 1998 does not apply to information relating to the deceased. However, this Protocol establishes measures to safeguard the details of those who are deceased, as set out in Clauses 1.5.5. to 1.5.7. Personal Data means any information relating to a living individual who can be identified from that information alone, or from that information and other information held or likely to come into the possession of the "data controller" and includes any expression of opinion and any indication of intention about the individual. The "data controller" is the Party responsible for determining how and why the data are processed.

3.1.3 The DP Act 1998 requires that the processing of personal data complies with the eight Data Protection Principles (See Appendix 1) and gives seven rights to individuals in respect of their own personal data held by others:-

- The right of subject access,
- The right to prevent processing likely to cause damage or distress,
- The right to prevent processing for the purposes of direct marketing,
- Rights in relation to automated decision taking,
- The right to take action for compensation if the individual suffers damage,
- The right to take action to rectify, block, erase or destroy inaccurate data
- The right to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.

3.1.4 The key principles of the DP Act 1998 are set out in Appendix 1. The 1st principle is one of the crucial principles when considering whether information can be shared. This states that the processing of personal data must be fair and lawful. Fair processing usually means that, at the point of collection, the Service User should be told about the purposes for which their personal data will be used. If personal data is to be used for purposes which were not spelled out to the data subject at the time it was collected, the "fair processing code" in Part II of the 1st Schedule to the DP Act 1998 requires that the data subject be advised of the purpose or purposes for which the data are, or are intended to be, processed; the identity of the data controller; and any other information required in the interests of fairness (e.g. it may include telling data subjects that they have the right to see the information held on them). In terms of this Protocol, the "data controller" will initially be whichever of the Parties acquires the information in question. The intention is that Service

Users will agree to information being shared between the Parties, in which case the Parties will become joint data controllers. In any case where information sharing means personal data will be used for a purpose other than the original purpose, it is for the data controller, who is using the data for a different purpose, to ensure that the fair processing code is complied with.

3.1.5 In order for processing of personal data to be lawful, at least one of the conditions listed in schedule 2 to the DP Act 1998 must be met, and if processing sensitive personal data, at least one additional condition from Schedule 3. Schedules 2 and 3 to the DP Act 1998 are set out in Appendix 2. Sensitive data, as defined by the Act, includes health data and information regarding a person's sexuality, ethnicity, religious beliefs and trade union membership. The Protocol proceeds on the basis that for most processing, consent of the Service User will be the appropriate Schedule 2 condition, and explicit consent of the Service User will be the appropriate Schedule 3 condition. However, although consent will be required for routine information sharing, there are also exceptional circumstances where information must be shared without consent, as detailed at Section 7.4 of this Protocol.

3.1.6 The third data protection principle states that personal data shall be adequate, relevant and not excessive for the purpose for which they are processed. The Parties must ascertain what information needs to be shared, as it is unlikely that each Party will need to disclose all personal data, which it holds, or indeed, be legally justified in doing so.

3.1.7 The DP Act 1998 supersedes the Access to Health Records Act 1990 apart from the sections dealing with access to information about the deceased. The Access to Health Records Act 1990 provides rights of access to the health records of deceased individuals for their personal representatives and others having a claim on the deceased's estate, insofar as they relate to the death of the deceased. In other circumstances, disclosure of health records relating to the deceased should satisfy common law duty of confidence requirements. This is reflected by the procedures outlined in paragraphs 1.5.5 to 1.5.7.

3.1.8 Article 8.1 of the European Convention of Human Rights, as given effect to by 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 and Article 8.2 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."

3.1.9 In the event of a claim arising under the Human Rights Act 1998, that a Party has acted in a way which is incompatible with the Convention rights, a key factor will be whether the Party can show, in relation to its decision on information sharing:-

- That it has taken these rights into account;
- That it considered whether any breach might result, directly or indirectly, from the action, or lack of action;
- If there was the possibility of a breach, whether the particular rights which might be breached were absolute rights or qualified rights;

If the right is qualified, an interference with that right can be justified but only if it can be shown that this is:-

- Lawful
- Necessary to pursue a legitimate aim e.g. protection of health or protection of the rights and freedoms of others and:
- Proportionate to that aim. Proportionality requires that any interference with rights, whether through action or inaction, is the least intrusive possible. Before interfering with rights, consideration should always be given to whether there is a less intrusive way of achieving the same benefits. Information sharing will be proportionate if there is no viable alternative and the information shared is limited to what the recipient Party needs to know.

Adherence to the terms of this Protocol should ensure that any infringement on the rights conferred by Article 8 will be in accordance with law; necessary; and proportionate.

3.1.10 All staff working in both the statutory and independent sector are aware that they are subject to a Common Law Duty of Confidentiality, and must abide by this. The duty of confidence only applies to 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.

3.1.11 The duty of confidentiality requires that unless there is a statutory requirement to use information that has been provided in confidence or a court orders the information to be disclosed, 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). The Scottish Government Health Department and professional bodies responsible for setting ethical standards for health professionals accept that the common law duty of confidence extends to the deceased. This Protocol proceeds on the basis of safeguarding information, which relates to deceased individuals.

3.1.12 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 (deceased individuals may have provided their consent prior to death). Schedules 2 and 3 to the DP Act 1998 apply whether or not the information was provided in confidence.

3.1.13 Where it is judged that an individual is unable to provide consent (for example due to mental incapacity or unconsciousness), other conditions in schedule 2 and 3 of the DP Act 1998 must be satisfied (processing will normally need to be in the vital interest of the individual); unless there is someone else who is lawfully entitled to consent on behalf of the individual and who does, in fact, consent. Any such proxy consents should be in writing for the avoidance of any later disagreements.

3.1.14 The Parties are subject to their own codes or standards relating to confidentiality although these should be seen as complementary rather than conflicting. This Protocol proceeds on the basis that the staff (including employees, contractors, agents and advisers) of the Parties who will have access to Service User personal data in terms of this Protocol, understand the confidential nature of this data and treat it accordingly. The Parties therefore undertake to ensure that all members of staff for whom they are

responsible are advised of and bound by a duty of confidentiality in respect of all Service User personal data.

3.1.15 NHS organisations who are Party to this Protocol are committed to the Caldicott principles when considering whether patient identifiable information should be shared. These principles are:

- Justify the purpose(s) for using confidential information
- Only use when absolutely necessary
- Use the minimum that is required
- Access should be on a strict need to know basis
- Everyone must understand his or her responsibilities
- Understand and comply with the law

Non-NHS Parties undertake to respect the Caldicott Principles in respect of patient-identifiable information, which they receive. However, the Parties also agree that whilst the Caldicott principles complement the DP Act 1998, they do not extend beyond its provisions. Therefore, if information can be shared in accordance with the DP Act 1998, the Caldicott principles should not be perceived as an obstacle to sharing of this information. The Caldicott Principles are set out in Appendix 7.

3.1.16 The Freedom of Information (Scotland) Act 2002 (FOI(S) Act 2002) does, as of 1 January 2005, provide a statutory right of access to all information held by Scottish public authorities, unless one of the fairly narrow exemptions to this new right of access is applicable. Public authorities will therefore require to have procedures in place to facilitate disclosure of information under this legislation. In responding to requests for information, which relates to matters covered by this Protocol, the Parties undertake to co-operate fully with each other. One of the exemptions in the FOI(S) Act 2002 relates to personal information, and requires that any disclosure of personal data to a third party must comply with the data protection principles contained in the DP Act 1988. The Parties anticipate that the personal and sensitive nature of much of the information exchanged under this Protocol could not be disclosed to a third party without breaching one or more of those principles and that as a result, the information may be exempt from the right of access provided by the FOI(S) Act 2002. However they also accept that any such request must be considered on a case basis at the time it is made.

3.1.17 Section 139 of the Anti Social Behaviour (Scotland) Act 2004 makes specific provision for information sharing between relevant authorities where this is necessary or expedient for the purposes of any provision of the Act or any other enactment relating to antisocial behaviour or its effects.

3.2 Principles governing the sharing of information in Dumfries and Galloway

3.2.1 In seeking to share information to improve services and support to the population of Dumfries and Galloway, the Parties will adhere to the following principles:

3.2.2 Non-NHS organisations recognise the requirements that Caldicott imposes on NHS organisations and will ensure that when requesting information from NHS organisations, such requests are made in a manner compatible with these requirements.

3.2.3 Information is provided in confidence when it appears reasonable to assume that the provider of the information believed that this would be the case. It is generally accepted that most (if not all) information provided by Service Users is confidential in nature. The Parties to this Protocol accept this duty of confidentiality and will not disclose such information without the consent of the person concerned, unless there are statutory grounds and an overriding justification for so doing. In requesting release and disclosure of information from the other Party, staff making the request 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.

3.2.4 The Parties will not abuse information which, in terms of this Protocol, is disclosed to them only for the specific purposes set out in this Protocol. Information shared with the other Party for a specific purpose will not be regarded by that Party as intelligence for general use.

3.2.5 The Parties are fully committed to ensuring that they share information in accordance with their statutory duties. They will seek to put in place procedures which ensure that the principles of the DP Act 1998 are adhered to and underpin the sharing of information between them and in particular, will adhere to the requirements of Schedule 3 to the DP Act 1998 in circumstances where information to be shared includes sensitive personal data. The Parties will seek to streamline such procedures, where possible. Parties which have obtained sensitive personal data relating to a Service User, in the course of their direct contact with that person, will seek to obtain the explicit consent of the Service User to disclose that information to another organisation. 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 statutory grounds for doing so and one of the remaining conditions of Schedule 3 can be satisfied. The Parties may seek to avoid asking for consent from a service user to disclose information to another person or Party when it is clearly envisaged that the information will be disclosed, irrespective of consent, and there are clear overriding circumstances (e.g. for certain criminal investigations which could be prejudiced if a suspect knew that he was under suspicion). This will be a rare event and should be authorised by the Data Controller or Caldicott Guardian of the Party involved.

3.2.6 Service Users in contact with any or all of the Parties will be fully informed about information which is recorded about them. If a Party has statutory grounds for restricting a Service User's access to information relating to them, then the individual will be told that such information is held and on what grounds it is restricted. (Unless, exceptionally, the information is such that the Party is entitled to withhold even the fact that it holds information at all). Other than this, they will be given every opportunity to gain access to information held about them and to correct any factual errors that have been made. Similarly, where opinion about them has been recorded and the Service User feels this opinion is based on incorrect factual information, they will be given every opportunity both to correct the factual error, and to record their disagreement with the recorded opinion. The Parties will, so far as possible, ensure that any such factual correction, or recording of disagreement, is notified to any of the other Parties to whom the information, so corrected or disagreed with, had previously been disclosed.

3.2.7 Where professionals request that information supplied by them be kept confidential from the Service User, the outcome of this request and the reasons for taking the decision will be recorded. Such decisions will only be taken on statutory grounds. Such grounds are

very limited. For example, the Orders detailed in paragraph 6.1.4, allow information to be withheld from the Service User if a health professional expresses the opinion that failure to do so would be likely to cause serious harm to the physical or mental condition of the Service User or another person. The data controller is not however entitled to withhold data supplied by the health professional simply on the basis that he would prefer this to remain confidential.

3.2.8 In seeking consent from a Service User to disclose this information, the Service User will be made fully aware of the information that will be shared and the purposes for which it will be used.

3.2.9 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.

3.2.10 When disclosing information about a Service User, professionals will clearly state whether the information being supplied is fact, opinion, or a combination of the two. Professionals should be aware that the definition of personal data in the DP Act 1998 expressly covers opinions and so, Service Users may exercise their rights of access to opinion as well as factual information. Use of professional jargon and organisation-specific acronyms or abbreviations should be avoided, particularly when the information is to be released to the other Party whose staff may not understand the jargon, or where the acronym or abbreviations in question may have a completely different meaning for them.

3.2.11 Careful consideration will be given to the disclosure of information concerning a deceased person and if necessary, legal advice will be sought on each individual case to ensure that both obligations of confidentiality and statutory rights to access such information are duly accepted.

3.2.12 The Parties are committed to putting in place efficient and effective procedures to address complaints relating to the disclosure of information, and will provide Service Users with information about these procedures.

3.2.13 The Parties will ensure that all relevant staff are aware of, and comply with, their responsibilities in regard both to the confidentiality of information about Service Users and to the commitment of the Parties to share information.

3.2.14 Procedures will be put in place to ensure that decisions to disclose personal information without consent have been fully considered in terms of applicable legislation and Schedule 2 and, in the case of sensitive information, Schedule 3 of the DP Act 1998, and that these decisions can be audited and defended. All relevant staff will be provided with training in these procedures. This will often require the relevant staff to make difficult professional judgements about what level of information sharing, if any is necessary to protect the vital interests of the Service User or the public. Any risk assessment should show that staff have taken all relevant factors into consideration before reaching a decision. Any decision made about the sharing of information without consent should be proportionate. This means that the overall benefit achieved by the decision should outweigh any interference with the rights of an individual. This may involve balancing the wishes of the Service User with what is considered to be a more pressing need. Guidance

Procedures should provide staff with detailed information on how to carry out risk assessments.

3.2.15 The Parties undertake to stress the need for staff to carefully consider whether disclosures of information can be justified. Staff will be made aware that disclosure of personal information which cannot be justified on statutory grounds and under Schedule 2 and, in the case of sensitive information, Schedule 3 of the DP Act 1998, whether disclosure is inadvertent or intentional, may expose the Parties to legal liability and staff to disciplinary action. This statement should not discourage staff from disclosing suspicions relating to suspected abuse or other criminal activity to the appropriate agencies, and in all cases local Child/Vulnerable Adult Protection Procedures or other means of alerting the authorities to criminal activity MUST be adhered to. It is the responsibility of each Party to ensure that relevant staff are given appropriate training on information sharing and that the procedures detailed in 7.4.2. are followed to avoid over caution on the part of staff, anxious to avoid legal action. Fear of legal implications and/or disciplinary action must not be a barrier to effective information sharing. The DP Act 1998 does not preclude the sharing of information in circumstances where this is necessary for the protection of an individual.

3.2.16 Where it is agreed to be necessary for information to be shared, information will be shared on a need-to-know basis only.

4. Purposes for which Information will be Shared

4.1 The purpose for Information Sharing is as follows:

- To support national initiatives on multi-agency working and information exchange
- To support joint care planning and commissioning.
- To support statutory reporting functions and effective use of resources.
- To assist the management teams of the Parties with planning and management information.
- To improve the quality of services for Service Users in Dumfries and Galloway
- To provide professionals with the information they need to deliver integrated services.
- To produce consistent services and information.
- To support a single point of access and out of hours services for the community.
- To enhance the robustness and effectiveness of systems to protect Service Users from harm.
- Other purposes may emerge from time to time which were not foreseen at the time this Protocol was being drafted. Provided the Parties agree that such further uses are beneficial and the information exchange underpinning such purposes is consistent with the over-reaching principles of this Protocol, then this Protocol shall also apply to such other purposes. As detailed by Clause 1.1.2, further Guidance Procedures should be developed.

4.2 Use and control of Service User Personal Data

4.2.1 The Parties agree that the exchange of Service User Personal Data under this Protocol is for the principal purpose of enabling them to carry out their statutory duties in relation to Service Users in terms of the relevant legislation.

4.2.2 The Parties may additionally use Service User Personal Data for their own research and statistical purposes (but only to the extent that such uses are permitted in law and where required, subject to ethical approval) provided that the Party wishing to make such use has taken all appropriate steps to inform the Service User concerned of this use (in line with the recommendations of the Scottish Government, Health Department, Confidentiality and Security Advisory Group for Scotland, Protecting Patient Confidentiality Report 2002) at the point of consent and has notified the other Parties of their intention to do so.

4.2.3 Insofar as Service User Personal Data is mainly stored, or to be stored, on a computer system belonging to one Party, the Party which owns the system shall have responsibility for maintaining system security and integrity, data back-up and archiving.

4.2.4 Where Service User Personal Data is stored in a system (manual or electronic) which belongs to, and is under the control of, one Party, the other Party may add to that Data to the extent permitted by any applicable Guidance Procedures. Any deletion of such Data may only be done with the approval of the Party which owns and controls the system in question.

4.2.5 Where Service User Personal Data is stored in a joint system (manual or electronic), being a system which either belongs to both Parties jointly or is expressly controlled by the Parties acting jointly, the Parties shall:

4.2.5.1 Specify in any applicable Guidance Procedures the respective rights of the Parties to add, amend and delete Service User Personal Data from the system;

4.2.5.2 Clearly allocate responsibility between the Parties for both physical and logical security of the system and appropriate measures for ensuring back-up and integrity of the data.

4.2.6 If a Service User requests that their details be amended or deleted from a system, and it is reasonable or legally obligatory for such request to be given effect to, the Parties shall cooperate in ensuring that the request is given effect to on any joint systems, as well as systems controlled by the Party which received the request.

5. Joint Procedures

5.1.1 Each Party will adhere to all joint policies and procedures formally agreed and authorised by the Parties, and to any Guidance Procedures agreed between the Parties.

5.1.2 Each Party will adhere to its own internal and any agreed joint policies and procedures covering Information Sharing, disclosure of personal information, access and security. The Parties shall endeavour to streamline these procedures with a view to achieving consistency of approach, in line with the principles of this Protocol. Either Party may, as a prerequisite to allowing a member of staff of the other Party access to its own systems, require that member of staff to agree to abide by such policies and guidelines as the Party may apply from time to time in relation to matters such as permitted use, security precautions, recording procedures etc.

5.1.3 The Fourth Data Protection Principle requires personal data to be kept accurate and where necessary, up to date. The Parties recognise the importance of good records management, in ensuring that information is regularly validated and refreshed. Inaccurate and out of date data is clearly detrimental to effective information sharing. The Parties should seek advice from records management staff on how best to manage and sustain data systems.

6. Subject Access Requests

6.1.1 One of the most important rights given to individuals by the DP Act 1998 is the right of subject access. The following clauses shall apply if a Service User or someone duly authorised to act on their behalf makes a request to any Party for access to their Personal Data under Section 7 of the DP Act 1998 (hereafter a "subject access request").

6.1.2 The Parties shall ensure that they have detailed Subject Access Procedures and Guidance in place to allow staff to respond to subject access requests. The Parties shall endeavour to make these consistent insofar as possible.

6.1.3 The Party receiving the subject access request shall ascertain whether the Service User Personal Data requested consists of Health Information and/or Social Work Information and/or Other Party Information or only one of them; and in any cases of doubt shall ensure that the views of a Health Professional, a Social Work Professional, and/or other appropriate professional are sought before reaching a decision.

6.1.4 In any case where Service User Personal Data contains information from more than one Party, the Party which received the subject access request shall, as soon as possible but in any event within 14 days of receipt of the request, ensure that a discussion takes place involving relevant staff chosen to ensure that a social worker professional and a health professional, where appropriate, are involved. The purpose of this discussion is to determine the extent, if any, to which the exemptions (detailed further in 6.1.6) contained in Article 5(1) of the Data Protection (Subject Access Modification) (Health) Order 2000 (hereafter referred to as "the Health Order") or Article 5(1) of the Data Protection (Subject Access Modification) (Social Work) Order 2000 (hereafter referred to as "the Social Work Order") or Part lll of the Data Protection (Miscellaneous Subject Access Exemptions) Order 2000, apply to the request under Section 7 of the DP Act 1998. In any case where the subject access request has been made on behalf of child aged under 12 years or on behalf of any adult with a mental incapacity, the discussion shall also consider whether the exceptions contained in Article 5(3) of each of the Orders are applicable in the case under discussion.

6.1.5 Although s7 DP Act 1998 provides a Service User with a right of access to his Personal Data, the Orders provide for circumstances where it is inappropriate to grant him full access if this would be likely to cause serious harm to the physical or mental health or condition of the Service User or any other person. The Orders also provide that where someone else makes a request for information on behalf of a Service User who is a child or an adult with mental incapacity, this should be withheld if the information was provided by the Service User in the expectation that it would not be so disclosed.

6.1.6 The Health Order details when it is necessary to consult the Appropriate Health Professional prior to complying with the subject access request. In general, a data controller who is not a health professional must not disclose health data to a Service User in response to a subject access request, unless he has first consulted the Appropriate Health Professional on whether or not disclosure would be likely to cause serious harm to the physical or mental health or condition of the Service User, or any other person. Note: The Appropriate Health Professional should not be asked for consent to the subject access request being complied with in its entirety. He should merely be invited to participate in the discussion, or provide a written opinion, on whether the serious harm

referred to in Article 5(1) of the Orders applies. Where the Health Professional involved in the discussion referred to in Paragraph 6.1.4 is not the Appropriate Health Professional and the Appropriate Health Professional is not available, the Caldicott Guardian of the Party for whom the Appropriate Health Professional works or worked shall instead be consulted. For the purposes of this paragraph, "the Appropriate Health Professional" has the meaning given in the Data Protection (Subject Access Modification) (Health) Order and means;

> **(a)** the health professional who is currently or was most recently responsible for the clinical care of the data subject in connection with the matters to which the information which is the subject of the request relates; or
>
> **(b)** where there is more than one such health professional, the health professional who is the most suitable to advise on the matters to which the information which is the subject of the request relates; or;
>
> **(c)** where –
>
> > (i) there is no health professional available falling within paragraph (a) or (b), or
> >
> > (ii) the data controller is the Secretary of State and data to which this Order applies are processed in connection with the exercise of the functions conferred on him by or under the Child Support Act 1991[Schedule 2] and the Child Support Act 1995[Schedule 3] or his functions in relation to social security or war pensions, a health professional who has the necessary experience and qualifications to advise on the matters to which the information which is the subject of the request relates.

6.1.7 The Parties agree that, in relation to Service Users who lack sufficient capacity to make a subject access request in their own right, the making of and acceding to such a request constitutes an intervention in the affairs of the Service User and so falls to be justified in terms of the Adults with Incapacity (Scotland) Act 2000 (AWI(S) Act 2000), in accordance with the procedure described in paragraph 6.1.9**.**

6.1.8 If a subject access request is received by either of the Parties in relation to Service User Personal Data, but the request is made on behalf of a Service User lacking capacity, the Parties shall follow the procedures described in paragraphs 6.1.3 to 6.1.7 as though the request had been by the Service User, but subject to the additional tests and safeguards described in paragraphs 6.1.9 to 6.1.15. It shall be the duty of the Party which received the subject access request to ascertain whether the person purporting to act on the Service User's behalf is legally entitled to do so.

6.1.9 If a discussion as described in paragraph 6.1.4 is to be held in relation to a subject access request received on behalf of an adult with a mental incapacity, it shall be the additional purpose of this discussion to ascertain the factors requiring to be taken into account in terms of Section 1(4) of the AWI(S) Act 2000, and to attempt to reach consensus as to whether acceding to the request is of benefit to the Service User in accordance with Section 1(2) of that Act

6.1.10 If the Parties are unable to reach agreement on the question of the proposed disclosure being of benefit to the Service User, they shall advise the person making the request on the Service User's behalf that the request cannot be acceded to unless authorised by the Sheriff under Section 3 of the AWI(S) Act 2000. The Parties agree not to release Service User Personal Data of which they are jointly Data Controllers to the person making the request unless and until such authorisation is granted or there is a change of circumstances meaning the Parties can reach agreement on the question of Service User benefit.

6.1.11 It shall not be necessary for the Parties to consider the question of benefit where a person acting under a valid Power of Attorney relating to the Service User's personal welfare has been given the express power to request confidential personal information relating to the Service User.

6.1.12 Any release of Service User Personal Data in terms of paragraph 6.1.9 to a person other than the Service User shall be done under terms which inform the recipient of the Service User Personal Data that they owe a duty of confidentiality to the Service User in respect of that data.

6.1.13 It shall be the duty of the Party which receives the subject access request to ensure that it is responded to within the Statutory 40 day time limit; this duty shall take precedence over the duties of consultation contained in this Protocol. Both Parties shall therefore ensure that they have robust procedures in place to ensure timely consultation as required by this Section 6 of the Protocol.

6.1.14 If the request received under paragraph 6.1.8 is in respect of a child aged less than 12, or a child aged 12 to 15 but who lacks the requisite mental capacity, the Party receiving the request shall give it full effect and apply the provisions of paragraphs 6.1.3 to 6.1.7, but only if satisfied that in terms of the Children (Scotland) Act 1995 the request is a proper exercise of parental rights and responsibilities.

7. Disclosure of Personal Information

7.1 Obtaining consent

7.1.1 The procedures used by the Parties for obtaining consent recognise the need to handle consent-seeking in as sensitive a manner as possible.

7.1.2 Any member of staff, who may have to seek the consent of a person to share information about them, will present and explain the issues to the individual, will request their consent to share personal information with the other Parties (or some of them) and will explain the consequences if consent is not given.

7.1.3 Where consent is to be sought, it will be sought at the earliest opportunity. This should be at the first contact with the Service User concerned unless the Service User is unable, at that time, to fully comprehend the implications or make an informed judgement. If, in the professional judgement of the staff member(s) concerned, it would be detrimental to the health of the person concerned to address these issues at that time, then the reason for not doing so should be recorded and arrangements agreed to complete this task at the first available opportunity.

7.1.4 It is the responsibility of all Parties to ensure that consent is given on an informed basis. This means that consent should only be given with the full understanding of what information will be shared, with whom and for what purpose.

7.1.5 Where it has been established that a Service User is able to make an informed decision then the member of staff seeking consent will first tell the Service User that:

- Everyone has a right to prevent the disclosure of information about themselves.
- It is a requirement of the DP Act 1998 that consent to disclosure of information should be on an informed basis.
- The right to prevent disclosure is recognised by the Parties. However, the Party has a responsibility in some cases to take steps to prevent harm to an individual or to protect their vital interests. If, in a particular case, the Party concludes that they have such a responsibility and this constitutes statutory grounds for disclosing information without consent, then they may exercise their right to do so.

7.1.6 The Parties' individual procedures will specify the circumstances under which information may be disclosed without consent.

7.1.7 Where an adult Service User does not have the capacity to make an informed decision but another person has authority to act as their guardian and take decisions on their behalf, then this situation must be explained to that person. The procedures described in Section 7.8.4 should be followed in these circumstances. Where the Service User is a child under 16, the procedures described in Section 7.9 should be followed.

7.1.8 The Service User or their guardian should be made aware that information about their case may be shared with other agencies in order to inform planning and development of relevant policies and procedures. They should be assured that if this happens, under no circumstances will personal information be released. The data will be anonymised or shared in aggregated form.

7.1.9 The Service User or their guardian must also be made aware of any specific records or systems which are maintained to support the purpose for which they are in contact with the Party at that point in time and which require them to pass information about the case to staff based in another. They must be told the purpose and content of these records, details of how they are stored and who has access to them.

7.1.10 The Service User or their guardian will be made aware that, other than for the purpose of protecting the vital interests of the Service User or the public, or where disclosure is required by law, personal information acquired by one Party, in the course of that Party's direct involvement with the person, will only be disclosed to the other Parties with their consent.

7.1.11 Each Party will have available material which explains:

- The rights of individuals under the DP Act 1998, particularly in relation to sensitive information
- Details of the procedures in place to enable Service Users to access their records
- Details of the procedures which may have to be initiated when a member of staff suspects that an adult or child has been or is at risk of abuse. These procedures must include details of who information will be shared with at each stage, the minimum amount of information which will be shared (each case being decided on an individual basis) and how the information will be used.
- Details of the circumstances under which information may be shared without consent and the procedures which will be followed
- Details of the complaints procedures to follow in the event that the Service User concerned believes information about them has been inappropriately disclosed.
- So far as practicable, a summary of how the information they provide will be recorded, stored and the length of time it will be retained by the point of contact Party, together with contact details for any agencies (including the other Party) to whom they envisage disclosing that information.
- Details of the length of time for which consent to particular disclosures is valid (including reference to any practice adopted whereby consent is taken to be valid indefinitely until revoked or withdrawn).

7.1.12 The Parties shall produce their own guidance material describing the purpose for which consent to disclose is being requested, together with such other details relating to the identity of the Parties and other information required in the interests of Parties, as required by the Information Commissioner's Office, Code of Practice for Sharing Personal Information. So far as practicable, the Parties will jointly agree the terms of the fair processing notice to be provided to Service Users whose personal data will be (or is intended to be) shared between the Parties in terms of this Protocol, and shall include the terms of any agreed notices in the relevant Guidance Procedures. As a minimum, such fair processing notices shall contain the information contained in Appendix 5.

7.1.13 As a minimum, the material should, so far as practicable, be available in a variety of formats and languages to the extent required by disability discrimination and race relations legislation. The Parties must also have access to appropriate means of communicating that information and ensure that these are made available if required. The Service User concerned must be given sufficient time to consider the material provided. There should be no doubt that the Service User concerned or, in the event that the Service User is unable

to make informed decisions, their legitimate representative, have been given every help to access and understand the facts before being asked to give consent.

7.1.14 Given the stressful conditions which may exist at the time a Service User is in direct contact with the Parties, it is unlikely that conditions will exist for the Service User to fully digest and understand their rights at that point in time.

7.2 Recording consent

7.2.1 Where consent is required, each of the Parties must have a means by which a Service User, or their guardian, can record whether they give consent to the disclosure of personal information. Individuals should be informed that withholding consent to information sharing may result in difficulties or delays in the provision of services, but no pressure should be put on the individual to agree to the disclosure of their data. If a Service User or potential Service User refuses to consent to their personal data being transferred to the other Party, this refusal of consent must be clearly marked on the Service User's case file. So far as possible, the Party to whom this refusal of consent was given shall record the reasons for this, if the Service User has given such reasons. A refusal of consent should be over-ridden only in exceptional circumstances (such as those described in Section 7.4). Such exceptional circumstances would include situations where information is required by statute or court order, where there is serious risk to public health, risk of harm to the Service User or other individuals, or for the prevention, detection or prosecution of serious crime.

7.2.2 Service Users should be able to prescribe, in respect of all information held by the contact organisation, which organisations information can and cannot be shared with. The Parties shall ensure that their response systems can properly reflect such choices.

7.2.3 It is recognised that, in an urgent or emergency situation and in many routine referrals, it is impractical for existing Service User records to be studied in detail and amended at that point in time. Parties should therefore have procedures in place to enable opportunities on a regular basis for Service Users to amend the contents if they are factually incorrect.

7.2.4 If a Service User withholds consent to the disclosure of information in any way, then this must be flagged both on the consent form and on their records in such a manner that any member of staff subsequently involved with that person is alerted to this. Information, which is held subject to a refusal of consent, should be stored in such a manner that access can be controlled. This refusal of consent should be recorded whether or not a decision is taken to disclose without consent.

7.2.5 The period of validity of consent should be specified within the Parties' individual procedures, unless the Service User concerned withdraws consent in the interim period. A record must be kept of the date on which consent was given, the date on which it is due to expire and the date on which it was withdrawn, if applicable. If at any time following the withdrawal or expiry of consent, a Party wishes to disclose that information for the same or another purpose, then consent will need to be sought again. Consent forms should therefore be designed to incorporate a period of validity. This may explicitly be an indefinite period i.e. until consent is subsequently withdrawn.

7.2.6 Where it is necessary to obtain the consent of a child before the disclosure of personal information to their parent, the child should complete a consent form which will be subject to regular review, until the date of the child's 16th birthday, after which date consent is no longer required and the consent form will cease to have any validity. All such consent forms should be retained on the former child's file so long as the file continues to exist.

7.3 Checking for consent

7.3.1 Where consent is required a Service User's personal case file should always be checked to ascertain consent before personal information is disclosed to another Party. Members of staff without access to a Service User's case file must check with case holders before releasing information.

7.3.2 It is essential that the person receiving a request for personal information about a Service User first checks that consent does not contradict any previous consent agreements held in their case file. Any contradictions must be resolved before information is released and should be notified to the persons responsible for controlling access to information. Legal advice should be taken if necessary.

7.3.3 Particular care should be taken before sensitive personal data as defined by the DP Act 1998 is released. As described in 3.1.5, sensitive personal data should only be released if its disclosure is critical to the case, explicit consent has been given to its release for that purpose, or the disclosure meets at least one of the other requirements of both Schedules 2 and 3 to the DP Act 1998, listed in Appendix 2.

7.3.4 When disclosing information about individual Service Users, the Parties must indicate to what extent this information is current, is factual or an expression of opinion and whether factual information has been confirmed as correct by the Service User.

7.3.5 It is recognised that in particular investigations (e.g. adult protection enquiries) the significance of information is often not apparent at the early stages and the Parties may put in place procedures that enable them to share all information they hold about the person(s) under investigation. In this case specific procedural guidance will clearly state that such an agreement has been made and will set out the specific arrangements they have put in place to limit the access to such information to those with a need to know.

7.3.6 The Parties will keep each other fully informed about the disclosure of information originating from the other's files, whether it is with or without the consent of the Service User to whom the information pertains. Accurate records must be kept of what information has been disclosed to whom, the source of the data disclosed, and the date on which it was disclosed, and written documentation relating to information disclosure must specify who will be responsible for ensuring that this is done (see 7.4.6). This information shall be provided to the originating Party on request.

7.4 Disclosing information without consent

7.4.1 It is possible, and on occasions essential, for information to be disclosed without the consent of the data subject. However, this must be handled carefully as failure to observe the proper procedures could result in some or all of the Parties being exposed to court

action or to enforcement action under DP Act 1998, the Human Rights Act 1998, or at common law (e.g. for breach of confidence). In some circumstances, there is the possibility of personal criminal liability by a member of staff. Usually, however, a member of staff would need to be clearly acting in bad faith before his actions would attract personal criminal liability. An inadvertent breach is unlikely to constitute a criminal offence albeit the data controller could be liable for an award of compensation by a court or subject to enforcement action by the Information Commissioner. The risk of falling foul of the law on information sharing must be weighed against the fact that numerous inquiries into service failures in the health and social services fields have criticised agencies for failing to share relevant information. None have criticised agencies for sharing too much.

7.4.2 Each Party shall put in place a mechanism whereby any member of staff concerned about disclosing personal data, and exposing the Data Controller to legal liability, can obtain the approval of the Data Controller to the disclosure. Such a mechanism means that the legality of the disclosure in question is a civil matter aimed at the Data Controller, and not a criminal matter aimed at the individual

7.4.3 Each Party will have procedures in place to allow decisions on such disclosures to be taken speedily. Individual Party procedures will indicate who will be the point of contact for advice for the client group covered by the procedure. The person(s) designated to make such decisions will be provided with clear guidance to enable them to decide whether there are statutory grounds for disclosure without consent and whether any of the conditions in Schedule 2 or 3 of the DP Act 1998 can be met. If they are in any doubt, they should refer the case to the designated point of contact for advice. It is the responsibility of each Party to ensure that the responsible staff know who to contact for advice, including legal advice where this is necessary; and how to contact them.

7.4.4 Disclosure without the consent of the Data Subject can take place for a number of statutory purposes. The DP Act 1998 acknowledges that in some circumstances, certain information must be disclosed. Such information is expressly exempt from the non-disclosure provisions of the DP Act 1998. Data protection therefore places no barrier to disclosure of such information. Typically, for the purposes of this Protocol, this will involve information relating to the investigation of crime or the detection and prosecution of offenders and the exercise of statutory functions.

7.4.5 Disclosure without consent may also take place if the processing complies with another condition specified in Schedule 2 of DP Act 1998 (plus a further condition specified in schedule 3, in the case of sensitive personal data). Two points need to be noted before relying on those provisions, however. Firstly, although consent is not the only justification for the processing of personal data listed in the Schedules to the DP Act 1998, this Protocol takes Service User consent as a basic principle except in certain circumstances. Outwith those circumstances, routine exchanges are not envisaged under the Protocol except on the basis of consent. Secondly, there remains the requirement to comply with the Fair Processing Code (see App 5), so disclosure under other Schedule 2/3 conditions (i.e. without consent) will only be permissible if this has been notified to the individual. Again, there are certain statutory exceptions to this requirement but these mostly have to be decided and applied on a case by case basis. Advice should always be sought by staff if they are in any doubt. Most justifications for exchanging information without consent relate to situations where this is necessary for the protection of the Service User or another individual. Neither the DP Act 1998 nor the Human Rights Act

1998 conflict with the protection of individuals. Both the DP Act 1998 and Art 8.1 of the European Convention on Human Rights are designed to protect the privacy rights of individuals. However, in cases of risk, it is important that both pieces of legislation are properly interpreted, as in some circumstances, the protection of the Service User or others may outweigh privacy considerations. The DP Act 1998 for example protects the integrity of a Service User's personal information. However, it also recognises that information must be shared, even when this is against a Service User's wishes, if this is necessary to protect vital interests. The Human Rights Act 1998 imports the proportionality principle into UK law which requires an appropriate balance to be struck between competing considerations. In some circumstances, a decision to share information without consent will be necessary and proportionate and will therefore comply with the Human Rights Act 1998. As any decision to share information should not be disproportionate to the overall aim e.g. protection of an individual, staff should always consider whether sharing information without consent is necessary and whether there is any viable alternative. Staff are required to exercise a professional judgment in such cases. The often inevitable tension between the privacy of the Service User and avoidance of risk to that Service User or others, should be overcome by careful risk assessment.

7.4.6 If information is disclosed without consent, then full details will be recorded about the information disclosed, the reasons why the decision to disclose was taken, the person who authorised the disclosure and the person(s) to whom it was disclosed. Such documentation will provide an audit trail, by showing that staff have exercised their professional discretion in a proportionate manner. Individual procedures within each Party will specify the person(s) responsible for ensuring that this happens.

7.4.7 Wherever possible, organisations will nominate contacts for the receipt of personal and sensitive personal information. These contacts will be responsible for instigating the agreed security procedures to ensure that this information is restricted to those who need to know it for the purposes agreed. Specific Guidance Procedures will set out the contacts agreed for the purpose integral to each particular exchange of information.

7.4.8 Recipients of the information will be made aware that it has been disclosed without consent and will put agreed security procedures in place.

7.4.9 A record of the disclosure will be made in the Service User's case file and, if they have the capacity to understand, the Service User must be informed; unless informing the client would prejudice the purpose for which the disclosure was made, or otherwise constitutes processing which is exempt from the subject information provisions.

7.4.10 For the avoidance of doubt, nothing in this Protocol should be taken as in any way impeding disclosure of information in accordance with each of the Parties' established Adult/Child Protection Procedures, which MUST continue to be adhered to.

7.5 Where consent is refused or withheld

7.5.1 If a Service User or potential Service User refuses to consent to their personal data being transferred to the other Party, this refusal of consent must be clearly marked on the Service User's case file.

7.5.2 So far as possible, the Party to whom this refusal of consent was given shall record the reasons for this, if the Service User has given such reasons.

7.5.3 The Party to whom the refusal of consent was given shall explain the consequences of their refusal of consent to the Service User, namely that fully integrated services will not be able to be provided or offered to the Service User.

7.5.4 If a Service User withholds consent, Service User Personal Data relating to them may only be disclosed to the other Parties (or any of them) in the circumstances described in Section 7.4 and not otherwise.

7.5.5 The Parties shall, at regular intervals, advise each other of the number of Service Users (and the Service User group which they fall into) who have refused to consent to their personal data being exchanged.

7.6 Staff guidance on consent-seeking

7.6.1 To support staff, each Party will put in place procedures that give clear guidance on:

- The need to seek consent and the consequences of not doing so;
- Who is trained to seek consent and how their involvement should be initiated.
- Who is able to take a decision on behalf of another person;
- The circumstances under which information may be disclosed without consent;
- Who can authorise the disclosure of information without consent and how this authority should be requested;
- The records which must be kept of this process;
- The procedures for recording and storing consent to share information;
- The procedures for recording limitations of consent to share;
- When consent expires and in which circumstance consent is invalidated.
- The procedures to be followed when consent is limited.

7.7 Maintaining contact detail

7.7.1 Both Parties will maintain a list of the staff that have been trained to seek consent.

7.7.2 The Parties will provide to their own staff the names and contact details of members of staff:

- To whom requests for information for particular purposes should be directed
- Who can authorise disclosure in respect of individual joint activities or other arrangements.
- Who will provide legal advice in respect of the disclosure of information concerning a particular Service User group?
- Who are authorised to receive confidential information in respect of a particular purpose

7.8 Cases of uncertain capacity

7.8.1 In a case where the professional principally responsible for the care of a Service User (hereafter referred to as the "relevant professional"), in exercise of his or her best professional judgement, entertains genuine doubts as to the capacity of a Service User (which in this Section 7.8 includes a potential Service User) to give consent to the

processing of Service User Personal Data, the assessment procedure described in Appendix 4 shall be followed.

7.8.2 The following clauses shall apply in cases where an adult Service User is incapable of giving consent.

7.8.3 The relevant professional shall ascertain whether a Welfare Attorney has been appointed by the Service User (and the document conferring the Power of Attorney duly registered with the Public Guardian in accordance with Section 19 of the AWI(S) Act 2000) or whether a guardianship order relating to the personal welfare of the Service User (other than one appointing the chief social work officer as guardian) has been made under Sections 57 and 58 of the AWI(S) Act 2000, or whether some other person has a legally valid power to consent on the Service User's behalf to matters relating to the Service User's personal welfare.

7.8.4 If any person as described in paragraph 7.8.3 has been appointed and has a duly subsisting authorisation, the relevant professional shall seek their consent and act on the basis of that consent (or refusal thereof) as though it were that of the Service User.

7.8.5 If no person as described in paragraph 7.8.3 has been appointed or can be found, the relevant professional shall discuss the situation with the Primary Carer and Nearest Relative of the Service User (if these can be found). Said discussions shall specifically include the possibility of making an application under Sections 53 or 57 of the AWI(S) Act 2000 to make an Intervention Order or appoint a guardian in relation to the Service User's personal welfare, in which case paragraph 7.8.4 shall thereafter apply.

7.8.6 If no application is to be made, the relevant professional shall consider the following factors.

- The present and past wishes and feelings of the Service User so far as they can be ascertained by any means of communication, whether human or by mechanical aid (whether of an interpretative nature or otherwise) appropriate to the Service User;
- The views of the Nearest Relative and the Primary Carer of the Service User, in so far as it is reasonable and practicable to do so;
- The views of
  - (i) Any guardian, continuing attorney or Welfare Attorney of the Service User who has powers relating to the proposed intervention; and
  - (ii) Any person whom the sheriff has directed to be consulted, insofar as it is reasonable and practicable to do so; and
- The views of any other person appearing to the relevant professional to have an interest in the welfare of the Service User or in the proposed intervention, where these views have been made known to the relevant professional, insofar as it is reasonable and practicable to do so.

If, having considered these factors, the relevant professional is of the opinion that the provision of services to the Service User by the Parties (or any of them) is justifiable in terms of Section 1 of the AWI(S) Act 2000 notwithstanding their lack of consent, he or she shall record that fact (and the reasons for it) in writing where a professional is considering the provision of services.

7.8.7 If the relevant professional has decided that provision of services is justifiable in terms of paragraph 7.8.6, then Service User Personal Data may be processed by the Parties to the extent necessary to provide those services, notwithstanding the lack of consent by the Service User.

7.9 Consent relating to children

7.9.1 The Parties recognise that for the purposes of the rights affected by this Protocol, individuals are presumed to enjoy full mental capacity to take decisions in their own right from the age of 12.

7.9.2 The assessment procedure in Appendix 4 is an adult assessment framework. In determining the capacity of a child aged 12-15 years, careful consideration should be given as to whether the child is capable of understanding the implications of his/her decision. A child in this group shall be presumed to enjoy full legal capacity until the presumption referred to in Paragraph 7.9.1 has been rebutted on the basis that he/she is not capable of understanding this.

7.9.3 The Parties are mindful that parental rights and responsibilities continue, until age 16 and beyond, and therefore agree that they will seek to keep parents/guardians involved in issues affecting their children, but only to the extent that this is compatible with the rights and autonomous choices of the young person. Accordingly, any disclosure of information relating to a young person with the requisite mental capacity made to their parent or guardian without the consent of the young person will need to be justified in the same way as any other disclosure of information without consent. Reference should be made to the tests and procedures in Section.7.4. The right of the young person to confidentiality will always prevail unless any of the circumstances detailed in Section 7.4 apply to a particular case.

8. Access and Security Procedures

8.1 Transfer of personal information

8.1.1 Access to identifiable information supplied by the Parties must be restricted to staff on a need to know basis in connection with one or more of the purposes listed in this Protocol. Personal details should only be accessed by those involved in the provision of services to the individual or other authorised staff.

8.1.2 It is essential that requests for information about particular Service Users be accompanied by sufficient personal information to ensure that the person can be clearly identified. In the absence of a common identifier, the name, address and date of birth of the Service User should accompany requests for information wherever possible.

8.1.3 The Parties will take every precaution to ensure that information which identifies individual Service Users is transferred and shared in a secure manner.

8.1.4 Fax transfer will be avoided wherever possible. Where it is necessary, then each individual Party's procedures for secure transfer by fax will be followed.

8.1.5 Electronic transfer of personal information will only be permitted on a system to system basis across secure networks.

8.1.6 All information systems containing identifiable information must be effectively password protected. Users must not divulge their passwords, nor leave systems active while absent.

8.1.7 It is recognised that in urgent cases, information about individual Service Users may have to be requested or provided via the telephone. Each Party's internal code of conduct for transferring and sharing information verbally will be followed. Face-to-face transfers are also covered by this Protocol. The Parties should ensure that their internal procedures reflect this Protocol.

8.1.8 Written communications containing personal information should be transferred in a sealed envelope and addressed by name to the designated person within each Party organisation. They should be marked Private and Confidential and the sender should consider placing the marked envelope inside an addressed sealed envelope which does not carry any confidentiality markings, or consider using a tamper proof envelope. Where a Party has a policy that all mail is to be opened at a central point, prior to delivery to the named recipient, then this policy must be made clear to the other Parties so that an alternative means of transfer can be adopted where it is essential that the information is restricted to those who have a need to know.

8.1.9 Where information is compiled for a particular purpose, then the procedural guidance specific to that purpose must state in detail the arrangements made for the secure storage and management of the information. These arrangements must be such that the information is available only to those who have a defined role relative to that purpose. The access privileges of each role must be specified in the procedural guidance.

8.1.10 Where information is disclosed it is important that the purpose for information sharing is clear, valid and recorded.

8.1.11 Formal policies and procedures must be in place addressing the physical security of buildings, security awareness, training of staff and security management of systems, both manual and electronic, where identifiable information may be held. The Parties shall endeavour to make such policies and procedures consistent where possible and reserve the right for external audit of such policies and procedures as may be deemed appropriate. ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management (formerly BS7799) has been adopted to facilitate this.

8.2 Use of personal information for purposes other than that agreed

8.2.1 It is recognised that staff and agents of the Parties fulfil a number of roles within their own organisation. In fulfilling one particular role, they may be given privileged access to information about a Service User, which they believe would assist them in one of their other roles, or be of wider interest to their organisation.

8.2.2 However, confidential information is disclosed only for the purpose specified at the time of disclosure. Making further use of this information simply because this is of wider interest to the recipient organisation is likely to breach the first and second data protection principles. It is a condition of access that it should not be used for any other purpose without the consent of the original data controller. In routine circumstances, the consent of the Service User will also be required unless one of the other justifications in Schedule 2 (and Schedule 3 if this is sensitive personal data) to the DP Act 1998 is applicable. The purpose should be set out in the guidance documentation relating to a particular project or service and information should not be shared or used for any other purpose.

8.2.3 Persons wishing to use that information for any other purpose, or who wish to disclose that information to any person other than those authorised to receive the information, must submit a formal application to the Party which is the data controller. It is the responsibility of the person making the application to provide sufficient information to justify why that information should be disclosed for that purpose. It is the responsibility of the data controller to obtain the consent of the Service User to the further use of that information or to decide whether the reason the information is required justifies disclosure without consent.

8.2.4 Individual information sharing arrangements must also include agreements which indemnify any of the Parties' data controllers for any action taken against them or their organisation as a result of the unauthorised use of confidential information by other Parties. This indemnity is for the benefit of any of the Parties to the protocol, in the event of their being found liable because of some act or omission of one or more of the other Parties employees, agents, etc.

8.3 Restrictions on the use of statistical and anonymous data

8.3.1 A Party in receipt of statistical data derived from the Service User records of the other Party must request permission from the originating Party (the data owner) if they wish to use that information for any purpose other than that for which the information was originally provided.

8.3.2 A Party submitting or circulating reports or articles beyond the community covered by this Protocol which incorporate statistics or other data supplied by the other Party, will ensure that the other Parties have the opportunity to view and comment on the report prior to its release.

8.3.3 Guidance material relating to specific projects should also specify arrangements for the approval of the wider use or publication of case studies based on material collated for the specific purposes covered by that project.

8.4 Recording of Service User Data

8.4.1 Any of the Parties who are involved in integrated care teams (being teams comprising the staff of more than one Party) shall agree between them systems for storing Service User Personal Data relating to that team, being either storage on the case/file management system of one or the other of the Parties, or else a shared data store. Responsibility for data archiving, back-up, and securing the integrity of the system used to store such records shall be agreed between the Parties (which agreement may also involve agreement as to sharing any costs associated therewith) and advice on managing and sustaining such systems should be sought from records managers.

8.4.2 If the records of a joint care team are to be stored on one Party's own computer system, the other Party or Parties whose staff will require access to that system shall ensure that those staff are advised and agree:

8.4.2.1 That the information stored on the system is confidential;

8.4.2.2 That the member of staff is given access to the system purely to enable them to carry out their functions within the joint care team, and is not to be used for any other purpose;

8.4.2.3 That the member of staff is only authorised to access records on the system relating to Service Users who have been allocated to that member of staff, and will not access or attempt to access the records of anyone else.

8.4.3 The Party whose system it is may make it a requirement of granting access that the staff of another Party first sign confidentiality and conditions of use undertakings .

8.4.4 In the event of an actual or apprehended breach of the confidentiality undertaking referred to in Clause 8.4.2 and 8.4.3, whichever of the Parties employs or employed the individual responsible for the breach, or apprehended breach, shall use its best endeavours to enforce the undertaking.

8.4.5 All employees of the Parties shall ensure that Service User Personal Data stored other than on the system agreed in terms of paragraph 8.4.1 is kept safe and secure in a manner which satisfies the 7th Data Protection Principle of the DP Act 1998 which provides that appropriate technical and organisational measures must be taken to guard against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data.

8.4.6 Service User Personal Data must not be disclosed or made available to anyone not subject to an enforceable duty of confidentiality in respect thereof, unless this is necessary by law.

9. Protocol Management Procedures

9.1 Formal approval and adoption

9.1.1 This Protocol is a development of eCare Projects in Dumfries and Galloway, in respect of services for adults and services for children, and to take cognizance of Modernising Government Fund backed initiatives to increase the integration of Services.

9.1.2 Formal adoption will follow the signing and, where appropriate, sealing of the document by an officer of each Party who is able to execute legally-binding documents on behalf of that Party. This Protocol shall take effect immediately on being formally executed by all the Parties.

9.2 Dissemination/Circulation of protocol

9.2.1 Parties will have their own internal training plans and procedures which will introduce procedural guidance to managers and fieldworkers.

9.2.2 Copies of each Party's own procedural guidance will be circulated to all relevant staff (to be determined by each Party), in line with the each Party's internal arrangement for distribution of procedures and guidelines. Wherever possible, the procedural guidance will be available to staff on-line.

9.2.3 A strategy for disseminating information 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.

9.2.4 Relevant information concerning data sharing between the Parties will be published, wherever possible, on the web sites of the Parties involved and made available at information points such as Public Libraries. Each Party will keep sufficient copies of these information leaflets etc., to enable the information to be readily available to members of the public who require it.

9.3 Monitoring and reviewing procedures

9.3.1 All projects and joint services carried out under the auspices of this Protocol will be subject to regular formal review.

9.3.2 Legal advice will always be sought before any major changes to joint arrangements are considered.

9.3.3 Each project or joint service will set out the particular arrangements for the review of that project or service. These will include details of:

- The Party responsible for reviewing and agreeing changes to the project/service
- The date of the initial review and the review frequency
- The Party or individual who will co-ordinate the review

9.3.4 Following the introduction of any new area of joint working, the use and application of personal data shared in consequence of that joint working will be closely monitored until the date of the first formal review. The length of this period and the individual responsible

for monitoring its use will be specified for all joint working. During this period changes will only be considered if the issues and problems identified are felt to be a significant barrier to information exchange.

9.3.5 The use and effectiveness of joint working arrangements will be evaluated in a number of ways.

9.3.6 Staff in each Party organisation will be required to log and report responses and behaviour, which they believe, are not in accordance with agreed procedures or this Protocol. A report on these breaches will be a major part of the formal review process. Breaches will be analysed frequently to ensure that problems with the implementation of the joint working arrangements are addressed before they become a major issue.

9.3.7 Complaints received by organisations will be analysed to determine whether they relate to a breakdown of, or inadequacy in, information-sharing arrangements. Parties will establish a procedure by which their complaints officers report complaints regarding the inappropriate use or disclosure of information to the Party responsible for the security of that information.

9.3.8 Prior to each formal review, a survey will target all stakeholder groups. The survey will seek to establish the ease of application of the procedures, the effectiveness of these procedures in encouraging the Parties to share information, difficulties encountered in working jointly, proposals for improving procedures, and the contribution of the joint working arrangements to achieving the objectives of relevant strategies.

9.4 Reporting breaches of the joint working arrangements/this Protocol

9.4.1 The period following the introduction of new joint working arrangements until the completion of the first formal review of these arrangements will be regarded as the pilot phase. During the pilot phase, all breaches of the agreed procedures or this Protocol are to be logged, investigated and the outcome of negotiations noted. The continued need to do so after the pilot phase will be examined as part of the review process.

9.4.2 The following types of incidents will be logged :

- 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
- Inadequate security arrangements
- Any actual or attempted security breach by an external party (e.g. hacking)

9.4.3 The following procedures should be followed:

9.4.4 Breaches noted by members of staff:

9.4.4.1 A member of staff, working for any Party, who becomes aware that the procedures and agreements, set out in or in accordance with this Protocol, are not being adhered to, whether within their own or the other Party; should first raise the issue with the line manager responsible for the day-to-day management of the project or joint service in question.

9.4.4.2 The manager should record the issue and check whether the concern is justified. If the manager concludes that procedures are being breached, he 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 who should file the details in the "breaches" log.

9.4.4.3 The member of staff who raised the issue should be informed of the outcome by the line manager 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.

9.4.4.4 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.

9.4.4.5 Joint working arrangements should detail the mechanism by which breaches will be reviewed, addressed and resolved. A log should be maintained of such breaches to enable review of these arrangements.

9.4.5 Breaches alleged by a Service User or a member of the public:

9.4.5.1 At the initial contact with any person making an allegation about whom personal information will be recorded, the senior professional present will:

- Make them aware of their rights in relation to information about them already held by that Party; or that they may disclose about themselves during the course of the interview or any subsequent investigation.
- Provide them with details of how to make a complaint in the event that they are unhappy about the conduct of any professional involved; and explain that this includes their right to complain if at any time they believe information has been inappropriately disclosed to another organisation or another person (whether or not the other organisation is a Party to this Protocol).

9.4.5.2 Any complaint containing allegations of inappropriate disclosure of information, received from or on behalf of, a Service User, will be dealt with in the normal way, by the internal complaints procedures of the Party which received the complaint: Any disciplinary action will be an internal matter for the Party concerned.

9.4.5.3 However, in order to monitor and police adherence to and use of this Protocol, procedures should be established within each Party by which complaints relating to the inappropriate disclosure of information are passed by the complaints officer to the officer designated to deal with breaches of this Protocol. The designated officer should report any complaints of this nature to the equivalent officer in each Party. Individual joint working arrangements should detail the specific arrangements for that project/joint service in question.

9.4.5.4 All alleged breaches of this Protocol and/or joint working arrangements under it, whether proven or not, should be analysed as part of the formal review process.

9.4.5.5 Individual joint working arrangements will indicate the arrangements made to report and review breaches of agreed procedures.

10. Contractual agreement

10.1 Undertaking

10.1.1 The Parties to the Protocol accept that the procedures laid down in this document will provide a secure framework for the sharing of information between them in a manner compliant with their statutory and professional responsibilities.

10.1.2 As such, they undertake to :

10.1.3 Implement and adhere to the procedures and structures set out in this Protocol.

10.1.4 Ensure that where these procedures are adopted then no restriction will be placed on the sharing of information other than those specified in this Protocol.

10.2 Data Protection notification and control

10.2.1 The Parties are each jointly Data Controllers of shared Service User Personal Data.

10.2.2 The Parties confirm that each has a valid notification under the DP Act 1998 and that this notification includes reference to the fact that Social Work Information and Health Information and other Party Information is held and may be disclosed to the other Parties.

10.2.3 The Parties undertake not to allow the said notification to lapse or be amended in a way which would render it inconsistent with paragraph 10.2.2 for the duration of this Protocol.

10.3 Duration and variation

10.3.1 This Protocol shall come into force immediately on being executed by all Parties.

10.3.2 This Protocol shall last until it is terminated as provided by 10.3.4 hereof, varied as provided by 10.3.5 hereof of suspended as provided by 10.3.5 hereof.

10.3.3 Notwithstanding the termination of this Protocol, any duties of confidentiality imposed on the Parties or in respect of staff or agents hereunder shall subsist indefinitely.

10.3.4 Any Party may terminate this Protocol on giving six months' written notice to the others of their intention to do so.

10.3.5 This Protocol may be varied by the written agreement of the Parties.

10.3.6 This Protocol shall terminate on the execution by the Parties (or their successors) and coming into force of another Protocol on sharing personal data which is expressly stated to supersede this Protocol.

10.3.7 Any Party may terminate this Protocol by notice in writing immediately if:-

(i) another Party is in breach of any of the terms of this Protocol which, in the case of a breach capable of remedy, shall not have been remedied by that other Party within 21 days of receipt of a written notice specifying the breach and requiring its

remedy; or (ii) another Party is incompetent, guilty of gross misconduct and/or any other serious or persistent negligence in the carrying out of its duties hereunder.

10.4 Mutual indemnities.

10.4.1 This Section 10.4 shall apply in the event that:

10.4.1.1 A Service User brings any claim, action or proceeding seeking damages (a "Relevant Claim") from a Party (the "Indemnified Party") on the basis that the Indemnified Party has

10.4.1.1.1 processed that Service User's Personal Data other than in accordance with the requirements of the DP Act 1998; and/or

10.4.1.1.2 otherwise used or disclosed that Service User's personal information (including, where appropriate Personal Data) in breach of any other duty (whether statutory or at common law) that may have been owed to such Service User; and

10.4.1.2 The Indemnified Party can demonstrate that:

10.4.1.2.1 such Personal Data or other information has been shared or made available pursuant to the terms of this Protocol; and

10.4.1.2.2 it has complied with its obligations under this Protocol in relation to the processing, use or disclosure of such Personal Data or other information; and

10.4.1.2.3 another Party (the "Indemnifying Party") has breached its obligations under this Protocol in relation to such Personal Data or other information and that this breach has resulted in the Relevant Claim.

10.4.2 Subject to the following sub-paragraphs of this Paragraph 10.4, in the event that a Relevant Claim is made in circumstances in which the conditions set out in sub-paragraph 10.4.1 are satisfied, the Indemnifying Party shall indemnify and keep indemnified, the Indemnified Party against all reasonable costs and expenses incurred by the Indemnified Party in defending the Relevant Claim and against any damages that may be paid by the Indemnified Party or awarded against it by a Court of competent jurisdiction in respect of the Relevant Claim.

10.4.3 The obligation on the part of the Indemnifying Party to indemnify the Indemnified Party is conditional upon the Indemnified Party complying with the following provisions:

10.4.3.1 The Indemnified Party will take all steps that it would reasonably be expected to take to mitigate or reduce the damages which are the subject of the Relevant Claim;

10.4.3.2 The Indemnified Party shall notify the Indemnifying Party as soon as reasonably practicable (and in any event within 14 days) after being notified of the Relevant Claim;

10.4.3.3 The Indemnified Party will allow the Indemnifying Party to elect at any time to have conduct of the Relevant Claim and (subject to indemnification in terms of sub-paragraph 10.4.2 in respect of the costs thereof) in the event of such election will provide

the Indemnifying Party with all assistance that the Indemnifying Party reasonably requires for such purposes;

10.4.3.4 In the event that the Indemnifying Party does not elect to have conduct of the Relevant Claim, the Indemnified Party will conduct the Relevant Claim responsibly and in consultation with the Indemnifying Party;

10.4.3.5 The Indemnified Party will make no admission, compromise or settlement in connection with the Relevant Claim without the prior written consent of the Indemnifying Party; and

10.4.3.6 The duty to indemnify shall extend to extra judicial settlement of the claim for damages only where the Indemnifying Party has consented to the settlement.

10.5 Third party rights

10.5.1 The duties imposed by this Protocol on the Parties hereto are expressly declared to be enforceable at the instance of any Service User claiming its terms have been breached and who claims to have suffered prejudice as a result of such breach.

10.5.2 Notwithstanding paragraph 10.5.1, the powers contained in Section 10.3 hereof to vary, supersede or terminate this Protocol may be exercised by the Parties (or, where applicable, by any of them) without the consent of any Service User or any other person and without any requirement to advise any Service User or any other person of the proposed or actual variation, suppression or termination hereof.

10.6 Disputes

10.6.1 The Parties agree to act in good faith at all times and attempt to resolve any disputes arising as a result of their respective rights and duties hereunder on an amicable basis.

10.6.2 In the event that the Parties are unable to resolve the dispute amicably, the matter shall be referred to a mutually agreed mediator. If the identity of the mediator cannot be agreed, a mediator shall be chosen by the Dean of the Royal Faculty of Procurators in Dumfries and Galloway.

10.6.3 If mediation fails to resolve the dispute or if the chosen mediator indicates that the dispute is unsuitable for mediation, the matter shall be referred to arbitration. The arbiter shall be mutually agreed or, failing agreement, chosen by the Dean of the Royal Faculty of Procurators in Dumfries and Galloway. The decision of the arbiter shall be final.

10.6.4 For the avoidance of doubt, this Section 10.6 shall apply to the duties contained in Section 10.4 hereof (mutual indemnities) as it applies to the rest of this Protocol.

10.6.5 Paragraphs 10.6.2 and 10.6.3 shall not apply to any disagreement between the Parties as to the question of benefit to a Service User described in paragraph 6.1.10.

Dumfries & Galloway Data Sharing Partnership - Information Sharing Protocol

10.7 Governing law

10.7.1 This Protocol shall be governed by Scots law and the Parties hereto submit to the exclusive jurisdiction of the Scottish Courts.

10.7.2 We, the undersigned, agree to adopt and adhere to this information sharing protocol: IN WITNESS WHEREOF

Signatures

Chief Executive
NHS Dumfries & Galloway

(print name) JOHN BURNS

(signature) J G Burns

(date) 21/12/09

Chief Executive
Dumfries & Galloway Council

(print name) GAVIN STEVENSON

(signature) G Stevenson

(date) 21/12/09

Chief Constable
Dumfries & Galloway Constabulary

(print name) PATRICK J. SHORTER

(signature) Patrick J. Shorter

(date) 21/12/09.

3 September 2009 Page 41 of 51

Appendix 1

Data Protection Principles

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

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

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

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

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

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

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

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

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

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

Appendix 2

Conditions relevant to the Processing of Personal Data

1. The data subject has given his consent to the processing.

2. The processing is necessary:-

(a) for the performance of or any matters pertaining to a contract to which the data subject is a party, or

(b) for the taking of steps at the request of the data subject with a view to entering into a contract.

3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract, imposed on the data controller or any of the Parties hereto.

4. The processing is necessary in order to protect the vital interests of the data subject.

5. The processing is necessary:-

(a) for the administration of justice,

(b) for the exercise of any functions conferred on any person by or under any enactment,

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or

(d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

6.

(1) The processing is necessary for the purposes 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.

(2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied

Conditions Relevant To The Processing Of Sensitive Personal Data

1. The data subject has given his explicit consent to the processing of the personal data.

2.

(1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

(2) The Secretary of State may by order:-

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in (1) Is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3. The processing is necessary:-

(a) in order to protect the vital interests of the data subject or another person, in a case where:-

(i) consent cannot be given by or on behalf of the data subject, or

(ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or

(b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the subject has been unreasonably withheld.

4. The processing:-

(a) is carried out in the course of its legitimate activities by any body or association which:-

(i) is not established or conducted for profit, and

(ii) exists for political, philosophical, religious or trade-union purposes,

(b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,

(c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and

(d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6. The processing:-

(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

(b) is necessary for the purpose of obtaining legal advice, or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7.

(1) The processing is necessary:-

(a) for the administration of justice,

(b) for the exercise of any functions conferred on any person by or under an enactment, or

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

(2) The Secretary of State may by order:-

a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in subparagraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

8.

(1) The processing is necessary for medical purposes and is undertaken by:-

(a) a health professional, or

(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provisions of care and treatment and the management of healthcare services.

9.

(1) The processing is of sensitive personal data consisting of information as to racial or ethnic origin which,

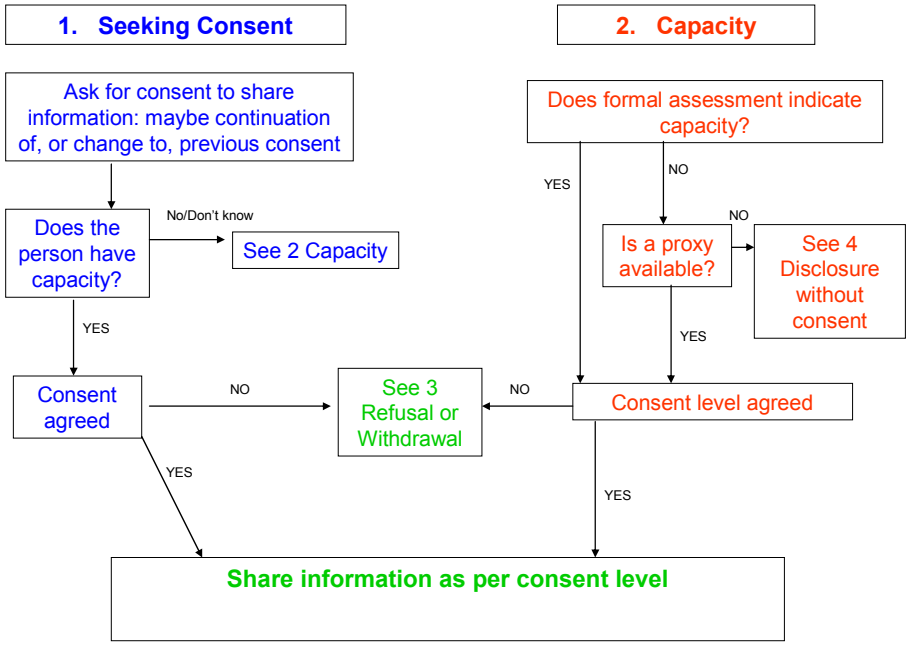
(a) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and

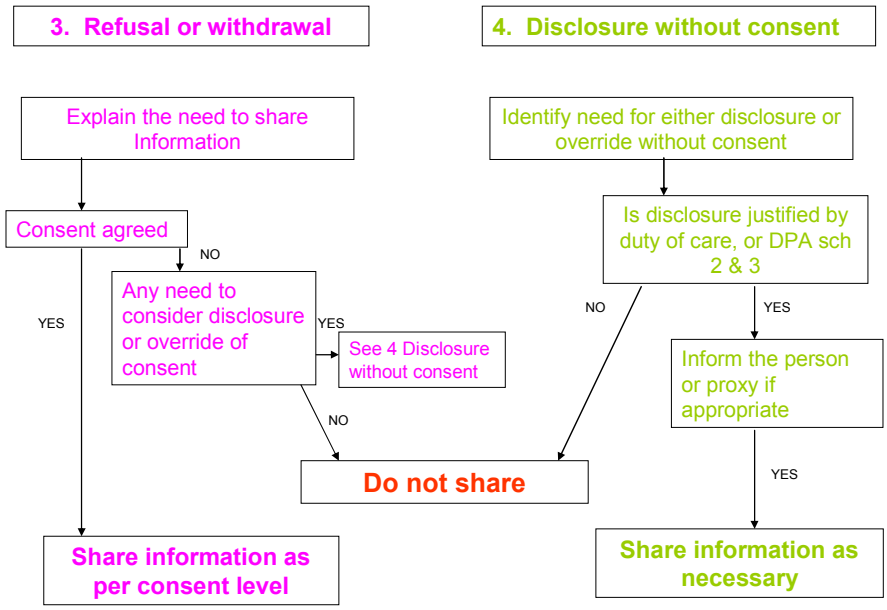
(b) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

10. The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.

Appendix 3


1. Seeking Consent
2. Capacity
Ask for consent to share information: maybe continuation of, or change to, previous consent
Does formal assessment indicate capacity?
YES
NO
Does the person have capacity?
No/Don't know
See 2 Capacity
NO
Is a proxy available?
See 4 Disclosure without consent
YES
YES
Consent agreed
NO
See 3 Refusal or Withdrawal
NO
Consent level agreed
YES
YES
Share information as per consent level


3. Refusal or withdrawal
4. Disclosure without consent
Explain the need to share Information
Identify need for either disclosure or override without consent
Consent agreed
NO
Is disclosure justified by duty of care, or DPA sch 2 & 3
YES
Any need to consider disclosure or override of consent
YES
See 4 Disclosure without consent
NO
YES
NO
Inform the person or proxy if appropriate
NO
Do not share
YES
Share information as per consent level
Share information as necessary

Appendix 4

Procedures for Assessing Capacity and Gaining Consent.

1 Wherever possible, consent should be sought in relation to sharing of personal data.

2 In the case of for example learning disability, procedures need to be developed to give opportunity to gain such consent.

3 The individual's capacity to give consent needs to be assessed in accordance with the Adults with Incapacity (Scotland) Act 2000 (AWI(S) Act 2000).

4 For the purposes of the AWI(S) Act 2000, incapacity must be judged in relation to particular matters, and not as an "all or nothing" generalisation. Medical practitioners must be alert to this whenever asked to assess capacity for purposes of the AWI(S) Act 2000. Guidance on assessment of capacity is available on the Chief Medical Officer's website. Normally an assessment under Part 5 should seek to determine whether the adult

- Is capable of making and communicating their choice
- Understands the nature of what is being asked and why
- Has memory abilities that allow the retention of information
- Is aware of any alternatives
- Has knowledge of the risks and benefits involved
- Is aware that such information is of personal relevance to them
- Is aware of their right to, and how to, refuse, as well as the consequences of refusal
- Has ever expressed their wishes relevant to the issue when greater capacity existed
- Is expressing views consistent with their previously preferred moral, cultural, family and experiential background.

5 It will also be important to investigate whether any barriers to consent are present, such as sensory and/or physical difficulties, undue suggestibility, the possible cognitive or physical effects of alcohol, drugs or medication, possible effects of fatigue, possible effects of pain and mental heath status considerations.

6 Once this assessment is complete, the findings should be discussed (with those involved in the meeting described in para 7) to identify the most appropriate method of communication for that individual.

7 The consent should be sought at a meeting / review with the person's relative/s present and their link worker or key worker and possibly (if appropriate) a speech & language therapist.

8 The Service User's preferred method of communication should be used and any other appropriate verbal or non verbal communication tools, to assist the Service User in understanding. (This could be pictorial dialogue, sign language etc)

9 Every effort should be made to ensure that the Service User is able to understand what is being asked. If the Service User is then able verbally or non verbally (thumbs up sign, nod of the head) to agree or disagree to consent, then an appropriate consent form should

be signed by the Service User and/or their relative and verified by the chairperson of the review.

10 The information relating to the discussion should be recorded fully in the review minutes, stating the method of communication, any tools used to assist and any non verbal forms of communication used.

11 The Service User's responses and those of others present should also be recorded in full.

12 Once completed, the minutes should be read and signed by all present, as this could also form part of the recorded consent form.

Appendix 5

Fair Processing

1. The term "processing" includes but is not exclusive to the concepts of obtaining, holding, recording, disclosing or carrying out any operation or sets of operations on specific personal data. Schedule 1, Part II, paragraphs 1-4 of the DP Act 1998 sets out the fair processing requirements. If any individual from whom data is collected is deceived or misled as to the purpose for which their personal information will be used, then this will have a bearing upon the validity of any consent given by that individual, for an organisation to use the information collected in the way described. In accordance with the fair processing requirements, the identity of the data controller; his nominated representative; the purposes for which data will be processed; and the likely consequences of such processing should be intimated to an individual Service User at the point of collection of their personal data.

2. In order to meet the fair processing requirements, partnership organisations should therefore ensure that an individual is not misled as to the purpose for which his/her information will be used. An individual Service User should be told at the point of first contact with a partnership organisation the identity of the data controller, his nominated representative, the purposes for which information will be processed and the likely consequences of collecting such data. Partnership organisations should ensure that provision is made within the Procedures and Guidance Documents to ensure that such detail is made available to the individual Service User at the point of first contact with the Service User.

3. Where information sharing means that personal data is to be used for a purpose other than the original purpose for which the data was first collected from the individual Service User, then the fair processing code will require to be re-visited. The individual Service User will require to be informed of any new purposes for which his/her information is being used. A Schedule 2 and (where sensitive personal data is being processed) a Schedule 3 condition will require to be met.

4. It has been agreed between the partnership organisations that all partnership organisations will seek the explicit consent of all individual Service Users in connection with the processing of their personal data. Obtaining explicit consent will satisfy both a Schedule 2 and if required, a Schedule 3 condition as set out within the DP Act 1998. Schedule 2, paragraph 1, relates to implicit consent and Schedule 3, paragraph 1, relates to explicit consent. The term "explicit consent" is not defined within the DP Act 1998, but is taken to mean active consent i.e. consent in writing or, where this is not possible, verbal consent. When consent is obtained from an individual to process their information in the way described, such consent should be recorded on that individual's records.

Appendix 6

Definitions

1 In construing this Protocol the following expressions shall have the meanings hereby assigned to them except where the context otherwise requires:-

"Acceptably anonymised" has the meaning given in "Protecting Patient Confidentiality", the Final Report of the Confidentiality and Security Advisory Group for Scotland, April 2002.

"Consent" shall mean informed consent in which the Service User has been given all the necessary information, unless declared medically inappropriate, and has the necessary capacity to make a judgement.

"Data", "Data Subject", "Personal Data", "Processing" and "Sensitive Personal Data" shall have the meanings assigned to them by the DP Act 1998.

"Data Protection Principles" shall mean the Principles found in Part I of Schedule 1 to the DP Act 1998.

"**Health Information"** means Personal Data to which the Data Protection (Subject Access Modification)(Health) Order 2000 applies.

"Incapacity Act" means the Adults with Incapacity (Scotland) Act 2000.

"Incapable", "Capable" , "Capacity", "Nearest Relative", "Primary Carer" and **"Welfare Attorney"** shall have the meanings ascribed to them respectively by the Adults with Incapacity (Scotland) Act 2000.

"Service User" means any individual receiving services, or who has applied for or been referred to any of the Parties with a view to being assessed for eligibility or need for services, from any Party in their respective capacities as Social Work Authority, Education Authority, Police and NHS Board.

"Service User Personal Data" means personal data (potentially including Health Information, Social Work Information and other Party Information) relating to a Service User.

"Social Work Information" means information to which the Data Protection (Subject Access Modification)(Social Work) Order 2000 applies.

2 Except where the context requires, words imparting the singular shall include the plural and words imparting male gender shall include the female (and vice versa).

Appendix 7

Caldicott Principles

The Caldicott Report set out a number of general principles that health and social care organisations should use when reviewing its use of client information and these are set out below:

Principle 1: Justify the purpose(s)

Every proposed use or transfer of personally identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by the appropriate guardian.

Principle 2: Do not use personally identifiable information unless it is absolutely necessary.

Personally identifiable information items should not be used unless there is no alternative.

Principle 3: Use the minimum personally identifiable information.

Where the use of personally identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiably.

Principle 4: Access to personally identifiable information should be on a strict need to know basis.

Only those individuals who need access to personally identifiable information should have access to it.

Principle 5: Everyone should be aware of their responsibilities.

Action should be taken to ensure that those handling personally identifiable information are aware of their responsibilities and obligations to respect patient/client confidentiality.

Principle 6: Understand and comply with the law.

Every use of personally identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements.