PROTOCOL FOR SHARING INFORMATION

between

GLASGOW CITY COUNCIL

and

NHS GREATER GLASGOW

Version	1.6 – 23 May 2005
Previous versions	Changes in version
V1.2	As Version 1.1 (distributed to MGF2 project team members on 27 January 2004) with tracked changes from K Meechan, based on NHS comments of December 2003 and of April 2004 plus results of "Show and Tell" to Aberdeen City Council. Purely advisory content removed.
V1.3	As version 1.2 (1 July 2004) :Scottish Executive "Gold Standard" ISP accreditation included. New Section 4.2.7 added to address MGF2 issues. Assorted tidying up. Escalation provision added. Fair Processing Notice content added.
V1.4	As Version 1.3 (18 March 2005) which assorted typos removed and incorporating comments from NHS Greater Glasgow.
V1.5	As Version 1.4 (19 April 2005) with Appendix 2 added
V1.6	As Version 1.5 (18 May 2005) with tracking removed and small correction to 3.2.1.5

PROTOCOL FOR SHARING INFORMATION

TABLE OF CONTENTS

1. INTRODUCTION

1.1. Scope

1.1.1. In order to place the sharing of information between them on a more formal footing, Glasgow City Council and NHS Greater Glasgow have developed a two level approach to Information Sharing consisting of this Protocol supported by a series of Guidance Procedures. Each Information Sharing context will require a unique set of policies and procedures and these are defined and agreed in the Guidance Procedures. The Guidance Procedures exist within the context of nationally and locally agreed information sharing principles and these are contained in this Protocol. This Protocol exists to ensure that information can be shared in a way, which satisfies the legal and professional obligations of the Parties and their respective staff, and the legitimate expectations of service users. It is not intended to be used as an operational guide book or manual; reference should instead be made to the appropriate Guidance Procedures.

1.1.2 Whenever a subsequent agreement is made to share information between the local partners, Guidance Procedures will need to be developed 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, most relating to assisting them in complying with their respective statutory duties or to improving service delivery. (A full description of the purposes of information exchange is provided in paragraph 4.1).

1.2. Parties to the Protocol

This Protocol is a legal agreement between

NHS Agency:

- Greater Glasgow NHS Board (also known as NHS Greater Glasgow), a body corporate established under the National Health Service (Scotland) Act 1978 (as amended) and having its Head Office at Dalian House, 350 St Vincent Street, Glasgow G3 8UZ (hereinafter referred to as "NHSGG");

Local Authority partner:

- Glasgow City Council, a local authority incorporated under the Local Government etc (Scotland) Act 1994 and having its Head Office at City Chambers, George Square, Glasgow G2 1DU (hereinafter referred to as "the Council").

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 circumstances of each individual. Sharing information about an individual between the Parties is vital to the provision of co-ordinated and seamless care to that individual 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 may be linked to the legal requirements or ethical standards, which must be satisfied, but sometimes these impediments have focused on less relevant issues or avoidable problems. Where information sharing has occurred, its value has often been reduced by such problems as misunderstandings in the use of language or inefficiencies in communications channels. These

barriers have led to concerns and to uncertainties about when 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 and a framework 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, developing on an earlier Protocol between the Council and the former Greater Glasgow Primary Care NHS Trust. The Protocol adheres to the national model authorised by the Scottish Executive'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 set out the specific arrangements and responsibilities designated any additional requirements, and the service level agreements for that application. This Protocol is expected to cut down the development time for Guidance Procedures. A template for Guidance Procedures can be found at Appendix 1.

1.4.2. This Protocol supersedes the Protocol for Sharing Information entered into between the Council and Greater Glasgow Primary Care NHS Trust dated 19 November 2002 and executed on 11 and 18 December 2002, which Protocol shall terminate on the date on which this Protocol comes into force.

1.4.3. This Protocol conforms to the standards laid down in the Scottish Executive's "Gold Standard" for Information Sharing Protocols.

1.5 OVERARCHING PRINCIPLES.

1.5.1 It shall be a fundamental principle of this Protocol that, except in specific limited circumstances, all processing of Service User Personal Data between the Parties shall be processed on the basis of the explicit consent of the Service User.

1.5.2 The Parties shall apply the presumption that all Service Users aged 12 years or older enjoy capacity to give, withhold or modify the consent referred to in Clause 1.5.1 and Section 6 of this Protocol.

1.5.3 The presumption of capacity referred to in Clauses 1.5.1 and 1.5.2 shall only be regarded as having been rebutted if the procedures for establishing incapacity laid down in Appendix 2 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. The Parties agree that no use shall be made of that data which is inconsistent with the aims of providing health services and social care to Service Users and with Service Users' 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 confidence 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 Data relating to the deceased to the extent that the use of or proposed use of such Data would (if being done in relation to Personal Data) constitute Processing which in terms of Part IV of the Data Protection Act 1998 would be exempt from the non-disclosure provisions as defined in Section 29(3) of that Act.

1.5.7 The provisions of this Protocol shall not apply to Personal Data 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 (detailed procedures being 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. Sets out the responsibilities of the Parties to implement internal arrangements to meet the requirements of the protocol; and

2.1.8. Describes 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 "DPA 1998" in the rest of this Protocol). The DPA 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 or from other information held or likely to come into the possession of the "data controller" (i.e. the Party responsible for determining how and why the data are processed, as described in paragraph 3.1.2).

3.1.2. The DPA 1998 gives seven rights to individuals in respect of their own personal data held by others, 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, the 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. and requires that the processing of personal data complies with the eight Data Protection Principles.

3.1.3. The 1st principle is one of the crucial principles when considering information sharing. 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 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" (this is the legal entity which determines the purpose and manner of the processing); 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 requires the information in question; the intention is in that Service Users will agree to information being shared between the Parties in which case the data controller will be each of the Parties acting jointly with all the others. In any case where information sharing means personal data will be used for a purpose other than the original purpose, it is for the original data controller to ensure that the fair processing code is complied with.

3.1.3 The DPA 1998 provides, in schedules 2 and 3, conditions that must be met before personal data can be processed fairly and lawfully – schedule 2 for all personal data; schedule 3 as an additional test for sensitive data. 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. Section 6.4 of this Protocol covers situations where personal data may be disclosed without consent.

3.1.4. The DPA 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. 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.

3.1.5. Article 8.1 of the European Convention on 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."

3.1.6. In the event of a claim arising under the Human Rights Act 1998, that an organisation has acted in a way which is incompatible with the Convention rights, a key factor will be whether the organisation can show, in relation to its decision to take a particular course of action :-

- 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 qualified rights) whether the organisation has proceeded in the way mentioned below (this will indicate whether the interference in the Convention right has a lawful basis);
- whether any interference with Convention rights was proportionate to the benefits the organisation was trying to achieve through its action or inaction.

Adherence to the terms of this Protocol should ensure that any infringement on the rights conferred by Article 8 would do so in a way, which is in accordance with the law.

3.1.7. 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.

3.1.8. 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 Executive 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. The European Court of Human Rights has also ruled that in some

circumstances, rights under Article 8 of the European Convention on Human Rights can extend beyond the death of a person.

3.1.9. 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 of the DPA 1998 apply whether or not the information was provided in confidence.

3.1.10. 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 DPA 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.

3.1.11. 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) if the Parties who will have access to Service User personal data in terms of this Protocol understood 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.

3.1.12. NHSGG is committed to the Caldicott principles when considering whether patient-identifiable information should be shared. These 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

GCC undertakes to respect the Caldicott Principles in respect of patient-identifiable information, which it receives.

3.1.13. Scottish Freedom of Information (FOI) legislation requires public authorities to put procedures in place to facilitate disclosure of information under the Freedom of Information (Scotland) Act 2002. In responding to requests for information under the Freedom of Information (Scotland) Act which relates to matters covered by this Protocol, the Parties undertake to co-operate fully with each other. However, both Parties accept that the personal and confidential nature of the information exchanged under this Protocol is such that much of it will properly be treated as exempt from the provisions of the Freedom of Information Act. The Parties are free to release details of this Protocol and any Guidance Procedures made under it either in response to an FOI request or productively.

3.2. Principles governing the sharing of information in Glasgow:

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

3.2.1.1. 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.

3.2.1.2. 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 in the requesting Party 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.

3.2.1.3. 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 the general use of the Party.

3.2.1.4. 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 DPA 1998 are adhered to and underpin the sharing of information between them and in particular will adhere to the requirements of Schedule 3 of the DPA 1998 in circumstances where information to be shared includes sensitive personal data. 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 will seek to avoid asking for consent from a Service User to disclose information to another person or Party where it is clearly envisaged that the information will be disclosed irrespective of consent. This shall not absolve that Party from its obligation to satisfy the Fair Processing Code, to the extent that this is applicable to the circumstances (e.g. for certain criminal investigations which could be prejudiced if a suspect knew that they were under suspicion, it may be legitimate not to inform them of disclosure to the police or other investigating agency).

3.2.1.5. Service Users in contact with either or both 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 to correct the factual error and record their disagreement with the recorded opinion. If information has been disclosed by one Part to another which is later the subject of a correction or recorded disagreement, the Parties will ensure, so far as practical, that the other Party is made aware of the correction or recorded disagreement.

3.2.1.6. 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.

3.2.1.7. 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.

3.2.1.8. 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.

3.2.1.9. 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. 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.

3.2.1.10. 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 (see paragraphs 1.5.5 to 1.5.7).

3.2.1.11. 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.

3.2.1.12. 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.

3.2.1.13. Procedures will be put in place to ensure that decisions to disclose personal information without consent have been fully considered relevant to applicable legislation and Schedule 2 and, in the case of sensitive information, Schedule 3 of the DPA 1998, and that these decisions can be audited and defended. All relevant staff will be provided with training in these procedures.

3.2.1.14. 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 DPA1998, whether inadvertent or intentional will be subject to disciplinary action. This statement should not discourage staff from disclosing suspicions relating to suspected child abuse or other criminal activity to the appropriate agencies, and in all cases local Child Protection Procedures or other means of alerting the authorities to criminal activity MUST be adhered to.

3.2.1.15. 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 Glasgow.
- 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 cannot be 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.

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 Social Work (Scotland) Act 1968 and other legislation which imposes powers or duties on Social Work Authorities, in terms of the Education (Scotland) Act 1980 and other legislation which imposes powers or duties on Education Authorities, and in terms of the National Health Service (Scotland) Act 1978 respectively, all Acts as amended or re-enacted from time to time.

4.2.2 The parties may additionally use Service User Personal Data for 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 Confidentiality and Security Advisory Group for Scotland) and has notified the other Party 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 an 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 co-operate 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.

4.2.7 Where the Parties agree to set up a multi-agency database which is populated by Service User Personal Data, the following provisions shall apply:

4.2.7.1 The designated Lead Party shall be responsible, in consultation with the other Party, for establishing data matching procedures which provide both Parties with reasonable assurance that the merged datasets accurately match Service User Personal Data from each Party which relates to the same Service User, and that so far as practicable false matches are avoided.

4.2.7.2 The designated Lead Party shall ensure that appropriate logical and (when relevant) physical security measures are put in place in respect of the multi-agency database such that access to Service User Personal Data is restricted to match the consent to data sharing which has been given by that Service User or their legal representative in accordance with the provisions of Paragraph 6.2.6 or if, in the case of a Service User lacking the requisite mental capacity, where Service User Personal Data may be exchanged between the Parties in accordance with Paragraph 6.7.6 .

4.2.7.3 The designated Lead Party shall ensure that there are provisions within the operation in the multi-agency database to permit information to be disclosed to a Party without the Service User's consent when permitted in terms of Paragraphs 6.4.5 to 6.4.10.

4.2.7.4 The Lead Party shall ensure that Service Users are able to make a subject access request in respect of their Personal Data held within the multi-agency database whether or not they have consented to all the Parties having access to this data.

5. JOINT PROCEDURES AND SUBJECT ACCESS

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 following clauses shall apply if a Service User or someone duly authorised to act on their behalf makes a request to either Party in terms of Section 7 of the Data Protection Act 1998 (hereafter a "subject access request").

5.1.4 The Party receiving the subject access request shall ascertain whether the Service User Personal Data consists of both Health Information and Social Work Information or only one of them and in any cases of doubt shall ensure that the views of both a Health Professional and a qualified social worker are sought before reaching a decision.

5.1.5 In any case where Service User Personal Data contains both Health Information and Social Work Information the Party which received the subject access request shall, as soon as possible but in any event within 21 days of receipt of the request, ensure that a discussion takes place involving relevant staff chosen to ensure that both a qualified social worker and a Health Professional are involved. The purpose of this discussion is to determine the extent (if any) to which the exemptions contained in Article 5(1) of the Data Protection (Subject Access Modification)(Health) Order 2000 or Article 5(1) of the Data Protection (Subject

Access Modification)(Social Work) Order 2000 apply to the request under Section 7. 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. (Articles in the Orders relating to withholding information from parents etc. in some cases).

5.1.6 Where the Health Professional involved in the discussion referred to in Paragraph 5.1.5 is not the Appropriate Health Professional and the circumstances are such that it is necessary to consult the Appropriate Health Professional prior to complying with the subject access request, the Appropriate Health Professional shall be invited to participate in the discussion or to provide a written opinion on whether Article 5(1) of the Data Protection (Subject Access Modification)(Health) Order ("the Health Order") applies, which opinion shall be considered as part of the discussion. If 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 Health Order, and means;

(a) the health professional who is currently or was most recently responsible for the clinical care of the data subject to 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 there is no health professional available falling within paragraph (a) or (b), 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.

5.1.7 In responding to a subject access request, the parties shall pay due accord to Social Work Services' Procedures and Guidance on Subject Access and the Health Service Guidance and procedures on Subject Access.

5.1.8 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 Incapacity Act, in accordance with the procedure described in paragraph 5.1.9.

5.1.9 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 5.1.3 to 5.1.7 as though the request had been by the Service User, but subject to the additional tests and safeguards described in paragraphs 5.1.10 to 5.1.15. 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.

5.1.10 If a discussion as described in paragraph 5.1.5 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 Incapacity Act, 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.

5.1.11 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 Incapacity Act. 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.

5.1.12 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.

5.1.13 Any release of Service User Personal Data in terms of paragraph 5.1.9 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.

5.1.14 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 5 of the Protocol.

5.1.15 If the request received under paragraph 5.1.9 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 5.1.3 to 5.1.7, but only if satisfied that in terms of the Children (Scotland) Act 1995 the request is a proper exercise of parental rights and responsibilities.

6. DISCLOSURE OF PERSONAL INFORMATION

6.1. Obtaining consent

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

6.1.2. 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.

6.1.3. Consent 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, following the decision to involve other Parties 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.

6.1.4. 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.

6.1.5. 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 DPA 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.

6.1.6. The Parties' individual procedures will specify the circumstances under which the Party may exercise their right to disclose information without consent.

6.1.7. 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 6.7 should be followed in these circumstances. Where the Service User is a child under 16, the procedures described in Section 6.9 should be followed.

6.1.8. 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.

6.1.9. 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.

6.1.10. 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 their direct involvement with that person, will only be disclosed to the other Parties with their consent.

6.1.11. Parties will have available material which explains:

- The rights of individuals under the DPA 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).

6.1.12. The Parties shall produce 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 Fair Processing Code. 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 maximum, such fair processing notices shall contain the information contained in Appendix 3..

6.1.13. The material should so far as practicable, and as a minimum to the extent required by disability discrimination legislation be available in a variety of formats and languages. 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.

6.1.14. 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. Each Party will have in place a strategy, therefore, to inform the public of their rights and the requirement for them to give consent.

6.2. Recording consent

6.2.1. 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 and what limits, if any, they wish placed on that disclosure.

These limitations should be over-ridden only if there are statutory grounds for doing so and one of the conditions of Schedule 2 of the DPA1998 can be demonstrated. For sensitive information, one of the conditions of Schedule 3 of the DPA 1998 must also exist.

6.2.2. 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.

6.2.3. In addition, in respect of sensitive information (as defined by the DPA 1998) which is held by either Party, Service Users must be able to prescribe the purposes for which they agree to this information being disclosed to another organisation. [Note that this right cannot be used to thwart criminal investigations etc.] Again, the Parties shall ensure that their systems can properly reflect such choices.

6.2.4. 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. Both Parties should therefore have procedures in place to enable Service Users to make themselves fully informed at all times of the consent of their records (both manual and computerised) and provide opportunities for Service Users to amend the contents if they are factually incorrect.

6.2.5. Under no circumstances will consent be sought, or taken to have been given, unless the Service User or their representative has been fully informed of the consequences of giving consent. As such, consent forms will contain a facility for the Service User to confirm that such information has been made available to them. The consent form should be stored in the Service User's personal record file and the file marked to indicate that consent forms are present. A copy of the consent form should be made available to the Service User.

6.2.6. If a Service User limits 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 limitation of consent. Information which is held subject to this limitation should be stored in such a manner that access can be controlled. This limitation of consent should be recorded whether or not a decision is taken to disclose without consent.

6.2.7. Consent to disclosure of personal information for a particular purpose, will be limited to a period to 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 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.

6.2.8 The Parties shall ensure that consent forms under which children consent to the disclosure of information to their parent/guardian are subject to regular review and will expire on the child reaching the age of 16.

6.3. Checking for consent

6.3.1. A Service User's personal case file should always be checked to ascertain consent before personal information is disclosed to the other Party. Members of staff without access to a Service User's case file must check with case holders before releasing information.

6.3.2. 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.

6.3.3. Particular care should be taken before sensitive personal data as defined by the DPA 1998 is released. Sensitive personal data should only be released if its disclosure is critical to the case and explicit consent has been given to its release for that purpose.

6.3.4. 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 it has been confirmed as correct by the Service User.

6.3.5. 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.

6.3.6. The Parties will keep full details concerning the disclosure of information originating from the other Party'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. This information shall be provided to the originating Party on request.

6.4. Disclosing information without consent

6.4.1. 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 activity under DPA 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. This 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.

6.4.2. Each Party shall put in place a mechanism whereby any member of staff concerned about being accused of disclosing personal data without the consent of the Data Controller may seek instructions on this point so as to ensure that their conduct is deemed to have the consent of the Data Controller. (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)

6.4.3. Disclosure without the consent of the Data Subject can take place for a number of statutory purposes. Disclosure of some information is, under DPA 1998, expressly exempt from the non-disclosure provisions. DPA 1998 therefore places no barrier to disclosure of such information. Typically, for purposes of this Protocol, this will involve information relating to the investigation of crime or the detection and prosecution of offenders.

6.4.4. Disclosure without consent may also take place if the processing complies with another condition specified in Schedule 2 of DPA 98 (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, this Protocol takes Service User consent as a basic principle, and so 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, 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.

6.4.5. Each Party will have procedures in place to allow decisions on such disclosures to be taken speedily. The person(s) designated 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 DPA 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 how and who to contact for advice, including legal advice where this is necessary. Individual Party procedures will indicate who will be the advice point of contact for the client group covered by the procedure.

6.4.6. 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. Individual procedures within each Party will specify the person(s) responsible for ensuring this happens.

6.4.7. Wherever possible organisations will nominate contacts for the receipt of personal and sensitive 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.

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

6.4.9 A record of the disclosure will be made in the Service User's case file and the Service User must be informed if they have the capacity to understand 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.

6.4.10 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 Child Protection Procedures, which MUST continue to be adhered to.

6.5 Staff Guidance on Consent-seeking

6.5.1 . 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.

6.6 Maintaining contact details

6.6.8 Both Parties will maintain a list of the staff who have been trained to seek consent.
:

6.6.9 The Parties will provide 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

6.7 CASES OF UNCERTAIN CAPACITY.

6.7.1 In a case where the health or social work 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 6.7 includes a potential Service User) to give consent to the processing of Service User Personal Data the assessment procedure described in Appendix 2 shall be followed.

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

6.7.3 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 Incapacity Act) 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 Incapacity Act, 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.

6.7.4 If any person as described in Clause 6.7.3 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.

6.7.5 If no person as described in Clause 6.7.3 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 Incapacity Act to make an Intervention Order or appoint a guardian in relation to the Service User's personal welfare, in which case Clause 6.7.3 shall thereafter apply.

6.7.6 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 Incapacity Act notwithstanding their lack of consent, he or she shall record that fact (and the reasons for it) in writing.

6.7.7 If the relevant professional has decided that provision of services is justifiable in terms of Clause 6.7.6, 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.

6.8 Where consent is refused or withheld:

6.8.1 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.

6.8.2 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.

6.8.3 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.

6.8.4 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 6.4 and not otherwise.

6.8.5 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.

6.9 Consent Relating to Children

6.9.1 The Parties recognise that 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.

6.9.2 Any issues concerning the debated capacity of a child aged 12-15 years shall be determined in accordance with the assessment procedure in Schedule. [NOTE: this is an adult assessment framework; require SW/NHS input into whether it is appropriate for this age group]. A child in this group shall be presumed to

enjoy full mental capacity until the presumption referred in Paragraph 6.9.1 has been rebutted in accordance with the Schedule 2 procedure.

6.9.3 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.6.4.

7. ACCESS AND SECURITY PROCEDURES

7.1. Transfer of personal information

7.1.1. 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.

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

7.1.3. 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.

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

7.1.5. It is recognised that in urgent cases, information about individual Service Users may have to be requested or provided via the telephone. The 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. Both Parties should ensure that their internal procedures reflect this Protocol.

7.1.6. Written communications containing personal information should be transferred in a sealed envelope and addressed by name to the designated person within each Party. They should be marked "Personal Private and Confidential – to be opened by the recipient only" and this placed inside an addressed sealed envelope, which does not carry any confidentiality markings. The designated person should be alerted to the despatch of such information and should make arrangements with their own organisation to ensure both that the envelope is delivered to them unopened and that it is received within the expected time scale. 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 such 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.

7.1.7. 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.

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

7.2. Use of personal information for purposes other than that agreed

7.2.1. 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.

7.2.2. However, confidential information is disclosed only for the purpose specified at the time of disclosure and it is a condition of access that it should not be used for any other purpose without the consent both of the data controller and the data subject. The purpose is 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.

7.2.3. 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.

7.2.4. Individual data sharing arrangements must also include agreements, which indemnify data controllers for any action taken against them or their organisation as a result of the unauthorised use of confidential information by the other Party.

7.3. Restrictions on the use of statistical and anonymous data

7.3.1. 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.

7.3.2. 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.

7.3.3. 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.

7.4 Recording of Service User Data

7.4.1 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, securing and systems 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).

7.4.2 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:

7.4.2.1 that the information stored on the system is confidential;

7.4.2.2 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;

7.4.2.3 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.

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

7.4.4. In the event of an actual or apprehended breach of the confidentiality undertaking referred to in Clause 7.4.2 and 7.4.3, 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.

7.4.5 All employees of the Parties shall ensure that Service User Personal Data stored other than on the system agreed in terms of paragraph 7.4.1 (such storage being purely on a temporary basis) is kept safe and secure in a manner which satisfies the 7th Data Protection Principle contained in the DPA 1998 (Personal Data must be protected by appropriate technical and organisational security measures).

7.4.6 Service User Personal Data must not be disclosed or made available to anyone not subject to an enforceable duty of confidentiality in respect thereof

8. PROTOCOL MANAGEMENT PROCEDURES

8.1 Formal approval and adoption

8.1.1 This Protocol is a development of the Protocol produced as a result of the Glasgow Joint Futures project as amended to increase its scope across NHS Greater Glasgow and to take cognisance of Modernising Government Fund backed initiatives to increase the integration of Children's Services.

8.1.2 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.

8.2. Dissemination/Circulation of protocol

8.2.1. Procedural guidance will be introduced to managers and fieldworkers following Party internal training plans and procedures

8.2.2. Copies of procedural guidance will be circulated to all relevant staff, 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.

8.2.3. 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.

8.2.4. 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 this information leaflets etc., to enable the information to be readily available to members of the public who require it.

8.3. Monitoring and reviewing procedures

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

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

8.3.3. 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

8.3.4. 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.

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

8.3.6. Staff in both Parties 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. During the pilot phase, 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.

8.3.7. Complaints received by organisations will be analysed to determine whether they relate to a breakdown or inadequacy of information-sharing arrangements. Both 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.

8.3.8. Prior to the 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.

8.4. Reporting breaches of the joint working arrangements/this Protocol.

8.4.1. 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.

8.4.2. 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)

8.4.3. The following procedures should be followed for the pilot phase:

8.4.4. Breaches noted by members of staff

8.4.4.1. A member of staff, working for either of the Parties 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.

8.4.4.2. The manager should record the issue and check whether the concern is justified. If the manager concludes that procedures are being breached, (s) 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.

8.4.4.3. The line manager should inform the member of staff who raised the issue, of the outcome, prior to submitting the issue to the designated person. If the member of staff is not satisfied with the response then they should be able to record their comments on the form prior to submission.

8.4.4.4. 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.

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

8.4.5. Breaches alleged by a member of the public:

8.4.5.1. At the initial contact with any member of the public about whom personal information will be recorded, the senior professional present will:

- Make them aware of their rights in relation to information that the Party they have approached already holds about them, or that they 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).

8.4.5.2. Any complaint received by, or on behalf of, a member of the public containing allegations of inappropriate disclosure of information 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.

8.4.5.3. 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.

8.4.5.4. 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.

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

9. CONTRACTUAL AGREEMENT

9.1. Undertaking

9.1.1. 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.

9.1.2. As such, they undertake to:

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

9.1.2.2 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.

9.2 Data Protection Notification and Control

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

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

9.2.3 The Parties undertake not to allow the said notification to lapse or be amended in a way, which would render it inconsistent with Clause 9.2.2 for the duration of this Protocol.

9.3 Duration and Variation

9.3.1 This Protocol shall come into force immediately on being executed by both Parties.

9.3.2 This Protocol shall last indefinitely unless terminated or superseded in terms hereof.

9.3.3 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.

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

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

9.3.6 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.

9.3.7 Either Party may terminate this Protocol by notice in writing immediately if;

(i) The other Party shall be 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) The other Party shall be incompetent, guilty of gross misconduct and/or any other serious or persistent negligence in the carrying out of its duties hereunder.

9.4 Mutual Indemnities.

9.4.1 This Section 9.4 shall apply in the event of a breach by either Party of its obligations hereunder (whether or not such breach results in the Party terminating or purporting to terminate this Protocol) where such breach results in harm or distress to any third party.

9.4.2 In the event that the third party who has suffered harm as a result of such breach seeks damages (whether at common law, under Section 13 of the DPA 1998 or otherwise) from the Party which was not in breach of its obligations, that Party shall be entitled to be indemnified by the Party in breach of its duties hereunder.

9.4.3 The indemnity referred to in Clause 9.4.2 shall include the costs, which the Party being indemnified has incurred in resisting or defending the claim for damages.

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

9.4.5 The duty to indemnify shall include the costs of any appeal against an initial adverse decision of the Court (whether by reclaiming motion or otherwise) only where the Party in breach has consented to the taking of the appeal.

9.5 Third Party Rights

9.5.1 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.

9.5.2 Notwithstanding paragraph 9.5.1, the powers contained in Section 9.3 hereof to vary, supersede or terminate this Protocol may be exercised by the Parties (or, where applicable, by either 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, supersession or termination hereof.

9.6 Disputes

9.6.1 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. If a dispute cannot be resolved at any given management level, each Party shall escalate the discussion to the next management tier and ultimately to their respective Chief Executives.

9.6.2 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 Glasgow.

9.6.3 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 Glasgow. The decision of the arbiter shall be final.

9.6.4 For the avoidance of doubt, this Section 9.6 shall apply to the duties contained in Section 9.4 hereof (mutual indemnities) as it applies to the rest of this Protocol.

9.6.5 Paragraphs 9.6.2 and 9.6.3 shall not apply to any disagreement between the Parties as to the question of benefit to a Service User described in paragraph 5.1.10.

9.7 Definitions

9.7.1 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.

"Appropriate Health Professional" shall have the meaning ascribed to it by the Data Protection (Subject to Access Modification)(Health) Order 2000

"Data", "Data Subject", "Personal Data", "Processing" and "Sensitive Personal Data" shall have the meanings assigned to them by the DPA 1998, and "Data Protection Principles" shall mean the Principles found in Part I of Schedule 1 to the DPA 1998.

"Education Information" means information held by the Council in its capacity as Education Authority for the City of Glasgow.

"Former Personal Data" means data which would constitute Personal Data but for the death of the former Data Subject.

"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", "Nearest Relative", "Primary Carer" and "Welfare Attorney" shall have the meanings ascribed to them respectively by the Incapacity Act, and "Capable" and "Capacity" shall be construed accordingly.

"The Parties" means the Council and "Party" shall mean either of them as the context requires.

"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 either Party in their respective capacities as Social Work Authority, (Education Authority) and NHS Board.

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

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

9.7.2 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).

9.8 Governing Law

9.8.3 This Protocol shall be governed by Scots law and the Parties hereto submit to the exclusive jurisdiction of this Scottish Courts:

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

APPENDIX 1 : Procedures for Assessing Capacity and Gaining Consent.

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

In the case of Learning disability, procedures need to be developed to give opportunity to gain such consent.

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

For the purposes of the Act, 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 Act. 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.

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.

Once this assessment is complete, the findings should be discussed to identify the most appropriate method of communication for that individual.

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

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)

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.

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.
The Service User's responses and those of others present should also be recorded in full.
Once completed, the minutes should be read and signed by all present, as this could also form part of the recorded consent form.

APPENDIX 2 : TEMPLATE FOR GUIDANCE PROCEDURES

Introduction
This template exists to assist in identifying the key procedures that will be used to allow the legal sharing of information between partner agencies in providing effective joint services to their users. Type in your response to each area and attach this document to the information sharing protocol. Together this then forms both a legal and procedural framework document for information sharing.
1. Aims and Responsibilities:
State the aims of your service here.
2. Information storage
How many formats will information be stored in. (i.e. Paper systems, electronic systems including spreadsheets etc.) Give brief descriptions of each one.
3. Information Sharing / Security
State when and how in the course of your work that information may get shared and any procedures that are followed in facilitating for this. Is data shared by written format, joint access to systems etc. Who has access to this data? How is this access monitored?
4. **Consent Issues:**
How are Clients / Patients made aware of consent issues? How is consent obtained – by whom? How is this recorded? How are staff made aware of the client/patients consent? State any current procedures adhered to.
5. Care management
State briefly how a persons care is managed from assessment through to service provision and what methods are used for recording by various parties involved (i.e. paper file, electronic, CareFirst etc)
6. Retention of information
Give details of any relevant procedures for retention and archiving of data and include relevant link or contact to obtain access to this document.

7. Subject access
Glasgow City Council and NAMED ORGANISATION/AGENCY have separate procedures to comply with the requirements of the Data Protection Act, and access to personal records. (include relevant link or contact to obtain access to this document.)
8. Complaints
Glasgow City Council and NAMED ORGANISATION/AGENCY have separate procedures to enable people to complain about any aspect of their services, including breaches of the data-sharing protocol. (include relevant link or contact to obtain access to this document.)

APPENDIX 3 -

Fair Processing Notice - Minimum content.

The Fair Processing Notices to be given or made readily available to Service Users whose personal data is or is likely to be shared in terms of the Protocol for sharing information shall as a minimum include the following:

- The identity of the Party whose notice it is;
- The fact that the Parties work jointly to provide improved services;
- The fact that such joint working requires information to be shared in order to work properly;
- The fact that such information will only be shared between the Parties in accordance with agreed policies and procedures with the result that
  - information will (except in exceptional circumstances) only be shared with the Service User's consent
  - information is only shared on a need to know basis where it is necessary for the better provision of Services
  - information shall be kept secure and confidential by all Parties and only accessed by the staff who need to access it for purposes of improved service delivery
- All parties may require to disclose information to other public bodies where this is necessary for the provision or detection of crime or the protection of children and vulnerable adults.