The

GREATER GLASGOW AND CLYDE PROTOCOL

for

SHARING INFORMATION

between

EAST DUNBARTONSHIRE COUNCIL

EAST RENFREWSHIRE COUNCIL

GLASGOW CITY COUNCIL

INVERCLYDE COUNCIL

RENFREWSHIRE COUNCIL

WEST DUNBARTONSHIRE COUNCIL

and

NHS GREATER GLASGOW AND CLYDE

Final Version May 2013

1. EXECUTIVE SUMMARY

1.1 Introduction

1.1.1 This document is a binding agreement between the Councils party to the protocol (Local Authorities established in terms of the Local Government etc (Scotland) Act 1994 and having their headquarters as noted at the end of this document Appendix 3) and NHS Greater Glasgow and Clyde (an NHS Board established in terms of National Health Service (Scotland) Act 1978 (as amended) and having its Head Office at JB Russell House, Gartnavel Royal Hospital Campus, Glasgow G12 OXH). This document will refer to them as "Local Authorities" and "the Board" throughout or, when referring to them both, to "the Parties".

1.1.2 The Parties positively encourage their staff to share information appropriately about their service users when it benefits their care and when it is necessary to protect vulnerable adults or children. This document describes how the Parties will exchange information with each other - particularly information relating to identifiable living people, known legally as "personal data". The purpose of this document is to explain why the partner organisations want to exchange information with each other and to put in place a framework which will allow this information to be exchanged in ways which respect the rights of the people the information is about, while recognising the circumstances in which staff must share personal data to protect others, without the consent of the individual. This protocol complies with the laws regulating this, particularly the Data Protection Act 1998. This Protocol explains how and when it is permissible to share personal data, either with or without the consent of the individual. This document is intended to provide a high level statement of principles on data sharing and associated issues, and to provide general guidance to staff on sharing information or disclosing it to another Party. The intention is to enable the appropriate flow of information to enable services to be delivered and to give clear guidance to staff on their responsibility to share information where they have concerns about a third party. Staff must therefore familiarise themselves with the relevant summarised guidance and any local procedures before releasing information to the other Parties. This document is also intended to be made available to service users and others whose information may be exchanged, in order to be as open and transparent with those individuals as possible regarding what may happen with their personal information. A template for local guidance, where this is required, is included as Appendix 1.

1.1.3 This document was originally built upon the Data Sharing Framework issued by the Information Commissioner (the independent official who oversees data protection issues in the UK) in October 2007. It has since been reviewed and updated to reflect the Data Sharing Code of Practice issued by the Information Commissioner in May 2011. The Information Commissioner's Office (ICO) endorsed this information sharing document as addressing the key areas set out within the ICO's information sharing framework code of practice. The ICO is pleased with the organisations' public commitment to allow the ICO to audit their compliance with the framework code as part of this endorsement and welcomes the promotion and following of good practice within the organisations. Whilst this document provides a sound basis for ensuring compliance with the data protection principles as set out in the code it is vital that information sharing is carried out in line with this code in practice. This summary describes, in general terms, the main ways in which information will be exchanged and addresses all the areas mentioned in the Commissioner's Code of Practice. Each area is described in more detail in the corresponding section of the Protocol which follows.

1.1.4 Across the Local Authorities within the boundaries of NHS Greater Glasgow and Clyde, an increasing number of health and social care services are delivered through integrated health and care teams. This includes through Community Health and Care Partnerships (CHCPs) which are legally established under NHS legislation but include staff carrying out statutory functions of both the Board and the Local Authorities. There are also integrated teams, delivering health and social care services in Local Authorities covered by Community Health Partnerships, which manage only NHS services. For purposes of this Protocol, information handled within an integrated team is generally treated as being processed by both the Parties, rather than to attempt to ascribe it to one or other body.

1.2 Deciding to Share Personal Information

1.2.1 The Board and the Local Authorities encourage their staff to share information about their service users for the purposes of better and more effective care and where information sharing is necessary to protect vulnerable adults or children who may not be service users. Information has been shared between the Parties for a number of years for the benefit of clients. Sharing relevant information leads to benefits for service users in improved and more joined-up services. However, it is important to recognise that legal safeguards are in place to ensure that only relevant information is exchanged in the appropriate way and that it can only be seen by staff that require to see it for the purposes of their job. All staff of the Parties who have access to personal information are contractually obliged to treat it as strictly confidential, and all information exchanged is kept secure by both parties. There will be occasions when information will be shared without consent and these are described later in this Protocol. More detail on this can be found in section 2 below

1.2.2 This Protocol is concerned with the exchange of information between the Parties. However, both staff and service users should be alerted to the fact that all Parties will exchange information with, or disclose information to, other organisations and agencies who are not a party to this Protocol. This will be governed by the appropriate legislation; the data protection policies and notifications of each Party should be referred to for more information on such exchanges and disclosures.

1.3 Fairness and Transparency

1.3.1 The Parties to this agreement explain the general nature of their data sharing arrangements in a number of ways – leaflets, posters, forms, and through their respective websites – and will continue to do so (and indeed, will continually develop and improve their approach to publicising these arrangements). The minimum content of such explanations is described later in this Protocol. The websites of the respective Parties also include more detailed information for those who wish to find out more. The Parties also have systems in place for dealing with inquiries, including inquiries about these arrangements, and are committed to being as open and transparent as possible about what information is exchanged and why. More detail on this can be found in section 3 below.

1.4 Security of Shared Information

1.4.1 The Board and the Local Authorities agree that following an evaluation of information sensitivity and business impact levels, the highest available levels of both organisational and technical security measures will be applied All Parties have strict information security policies which must be applied to information exchanged under this Protocol. All staff having access to shared information are professionals who have professional and contractual confidentiality obligations which the Parties agree to enforce if necessary. This is reinforced through staff induction procedures and training. More detail on this can be found in section 4 below.

1.5 Information Governance

1.5.1 Information sharing can best achieve improvements in service delivery if the information conforms to certain standards to ensure that it is accurate, up-to-date, and correctly applied to the right person. The Parties have their own systems to monitor and check the quality of the information they hold, including information exchanged with the other Parties. Sharing only takes place where there is no doubt that the information relates to the right person. The Parties have mechanisms for informing the others in the event that information is found to be incorrect, out of date etc.

1.5.2 By law, neither the Board nor the Local Authorities are entitled to hold personal information for longer than is necessary. It is, however, not always easy to define how long it will be necessary to hold particular information, as circumstances may change and events may only come to light many years after they originally happened. The Parties will have their own policies on how long to keep different types of records (policies such as this are known as "retention schedules" as they describe how long to retain the different types of document or record). Shared information is covered by the retention schedule of the Party holding it subject to arrangements to ensure consistency of approach between the Parties on this.

Before introducing new methods of processing or sharing personal data it is good practice to consider the benefits as well as the risks and potential negative effects for the individuals to whom the data relates. A Privacy Impact Assessment (PIA) is one method of doing this. This protocol commits each party to conducting such assessments in certain circumstances. More detail on this, as well as information standards and retention referred to above, can be found in section 5 below.

1.6 Individual's rights

1.6.1 Everyone has the right to ask to see what information an organisation holds on them, to object to information about them being processed and to complain about the use of their information or denial of access to it. This Protocol spells out how these rights will be given effect to in a joint working environment. In essence, a request by someone to see the information held which relates to them (known as a "subject access request") addressed to either organisation will be taken to include any information relating to them which has been provided by the other Party, including information on any jointly held databases or held in a joint working environment such as a Community Health and Care Partnership.

1.6.2 All Parties have a policy of being as open with people as possible, but there are circumstances (described in general terms later in this Protocol) where someone will not be given full access to their file. The procedures for subject access operated by all Parties also ensure that the rights of third parties who may be mentioned in someone else's files are adequately respected and, where appropriate, protected. More detail on this can be found in section 6 below, which also covers the process for responding to requests to stop processing information.

1.7 Freedom of Information

All the Parties are Scottish public authorities for purposes of the Freedom of Information (Scotland) Act 2002 and must respond to any request for recorded information made to them in a permanent form (such as letter or email). This would include an obligation to respond to requests about information sharing practices and procedures such as the arrangements under this Protocol. It should be noted that the actual personal information exchanged between the Parties will, in almost every case, itself be exempt from disclosure under the freedom of information legislation. All Parties will include this Protocol and its supporting documentation into their respective Publication Schemes. More detail on this can be found in section 7 below.

1.8 Review

1.8.1 Information sharing initiatives will be reviewed regularly to ensure that they continue to meet their objectives in a way which is consistent with the rights of the individuals concerned. This Protocol builds on work previously undertaken between the Parties under previous Protocols and in preparing it, the opportunity was taken to review the effectiveness of those existing arrangements and amend them where necessary. This Protocol will itself be subject to annual review. More detail on this can be found in section 8 below.

2. DECIDING TO SHARE PERSONAL INFORMATION

2.1 The Board has the statutory responsibility to provide or arrange for the provision of a comprehensive range of healthcare, health improvement and health protection services. The Local Authorities have the statutory responsibility to provide or arrange for the provision of social care services, education services and a number of other local authority functions which impact on the health and welfare of service users or those they are responsible for. In each case, many of the services the organisations provide can be provided better or more efficiently if there is a joined-up approach to these services – and this can only be done if the organisations are able to exchange relevant information with each other. Specifically, information is shared for the following purposes:

- to improve the quality of services for service users
- to protect vulnerable adults and children, who may or may not be service users themselves
- to provide staff with the information they need to deliver joined-up and integrated services
- to enable each Party to discharge its statutory duties within the joint working environment
- to produce consistent services and information
- to support joint care planning and commissioning.

- to support a single point of access and out of hours services for the community
- to support national initiatives on multi-agency working and information exchange
- to support statutory reporting functions and effective use of resources
- to assist the management teams of the Parties with planning and management information; and
- to enhance the robustness and effectiveness of systems to protect service users and others from harm
- other purposes which may emerge from time to time. Provided the Parties agree that such further uses are necessary and proportionate and that the information exchange underpinning such purposes is consistent with the over-arching principles of this Protocol, then this Protocol shall also apply to such other purposes. Any such additional functions which are identified will be added to this list on the next review of this Protocol and reflected as quickly as possible in the fair processing information made available to clients which is described in Section 3 below. The Parties will exercise a high degree of scrutiny to ensure that any additional purposes identified meet all the necessary requirements of this Protocol.

2.2 Information has been shared between the Parties for a number of years for the benefit of clients, under previous versions of this Protocol. In the course of drawing up this version, work has been undertaken to identify areas of good practice (where sharing information has led to improved services being provided) and to identify areas where lack of information sharing has been a barrier to improvement. This version of the Protocol seeks to build on the previous good work and to eliminate unnecessary barriers where these have been identified.

2.3 Where service planning or other objectives can be achieved equally well using statistical or anonymised data, then this is done in preference to exchanging details about identifiable people. The Parties only exchange information which can identify someone/can be related to a specific person where using statistical or anonymised data will not achieve the objective. This approach is line with the Caldicott Principles which regulate the use and dissemination of health service information. The procedures (and this Protocol) are designed to ensure that data sharing between the Parties complies with all applicable law and professional guidance, including the requirements of the Data Protection Act 1998. As the Parties are also public authorities for purposes of the Human Rights Act 1998, this Protocol is also intended to ensure that the right to respect for private and family life laid out in Article 8 of the European Convention on Human Rights is observed and complied with at all times, and that any infringement of that right is a necessary, lawful and proportionate response to a particular situation.

2.4 In order to achieve the improvements in service delivery and the other purposes mentioned in paragraph 2.1, the following sorts of information are exchanged:

- non-personal statistical and financial information derived from personal data
- research data and findings derived from personal data
- standard demographic information about service users and those involved in their care (names, addresses, dates of birth, contact details etc)
- unique personal identifiers (including Community Health Index (CHI) numbers and internal reference numbers)
- the following information in respect of service users or those involved in their care only where relevant to the provision of joint services to those individuals or the protection of the service user and/or others from harm:

- information concerning physical and mental health and condition
- medication, aids, adaptations, social supports, therapeutic interventions
- family history/circumstances and other significant relationships (e.g. marital status, dependants)
- social circumstances and environmental factors
- history of past involvement with any of the Parties
- financial information
- detail of enquiries or complaints received from and about service users and those involved in their care
- history of violent or abusive behaviour
- criminal record
- assessment of risk or threat posed to or by an individual

2.5 The law in Scotland makes very few explicit references to sharing information in the way envisaged by this Protocol. Most of the information exchanged is carried out to better achieve the general duties and obligations which the Parties have. Where specific statutory "gateways" exist which authorise particular data exchanges between the Parties, these are utilised where appropriate and with appropriate publicity for those concerned.

2.6 Information regarding individuals will always be sensitive. All sharing of personal information requires to be carried out in light of the legitimate rights and expectations of service users and others, and an awareness of the risk to those individuals. For example will any individual be damaged by data sharing? Are they likely to object to data sharing? Will it damage their trust in either party?

2.7 In all cases, staff will be expected to maintain awareness of such risks and to only exchange information which is relevant to and required for the purposes of data sharing. Information will be accessed only by the staff with a need to see it, and will be kept secure at all times no matter which of the Parties holds it at any given time, in accordance with the information security policies of the Local Authorities and/or the Board, as appropriate. All staff of both the Board and the Local Authorities who have access to personal information are contractually obliged to treat it as strictly confidential.

2.8 There are also however risks of harm associated with not sharing information in some circumstances. There will be occasions when information about an individual will be shared without their consent, particularly to protect vulnerable adults and children, who may not themselves be service users. If any member of the Parties' staff believe there are risks to a vulnerable person which may be mitigated by sharing personal information, they are obliged to share that information, if necessary without consent. Staff will be expected to exercise good professional judgement in balancing these risks and to always operate within the context of sharing information in a secure, proportionate manner only when necessary to achieve the objectives set out above.

2.9 Otherwise this Protocol proceeds on the basis that information will be shared with the consent of the individual service user (or, if a person cannot consent by reason of age, mental condition etc, with the consent of the person able to take decisions on their behalf). Such consent must be informed and freely given, and the fact that consent has been given (or withheld, or withdrawn) must be clearly recorded in the appropriate service user file(s). Service users should also be advised as to the consequences which withholding consent may have in terms of affecting the services they can be offered. The status of this consent must be checked before information is released to the other Party. Everyone has the right to decline to give this consent, withdraw it once it has been given, or give consent only to a limited type of information sharing.

2.10 Information may be exchanged without the consent of the individual on the basis of lack of capacity of the individual to consent, or because of concerns or perceived risks regarding the welfare of the individual or others. More specifically, it may be shared without consent in the following circumstances:

2.10.1 if the individual cannot consent due to their age (noting that children aged 12 or above are presumed to have the required capacity to consent or not; if aged less than 12, it is necessary to assess the child's capacity to do so): in these cases, the person having parental rights should be asked to consent on their behalf, in accordance with local guidance procedures;

2.10.2 if the individual has lost the required mental capacity due to a long-term condition, then a person lawfully appointed and able to take welfare decisions on behalf of that person should be asked to consent on their behalf;

2.10.3 if the individual has lost the required mental capacity due to a long-term condition, and there is no person lawfully appointed and able to take welfare decisions on behalf of that person, then the relevant professionals will decide on behalf of that person in accordance with the tests laid down in incapacity legislation, on the basis of the person's known/ascertainable wishes, those of nearest relatives and primary carers etc. In all cases, the paramount consideration will be the welfare of the individual consistent with their expressed wishes;

2.10.4 if a person has lost capacity due to a short-term event (such as unconsciousness), information will only be exchanged where necessary to protect their immediate interests, and then only to the minimum extent necessary;

2.10.5 if one of the Parties' staff has concerns that there are risks to a vulnerable adult or child, information on a service user may be shared without consent

2.10.6 information will be exchanged in terms of the MAPPA arrangements (Multi-Agency Public Protection Arrangements) which the Local Authorities, the Board and a range of other public bodies are party to under the laws governing management and supervision of offenders; and

2.10.7 information may be exchanged in relation to suspected serious criminal acts or other seriously improper conduct where no reasonable local authority or health board could fail to act on the information in its possession.

2.11 In any case where mental capacity is in issue, staff will follow procedures laid down in relevant local guidance documentation on how capacity is to be assessed, and will not make unsubstantiated assumptions regarding capacity or otherwise without a proper assessment being carried out.

2.12 In line with legislation and the Information Commissioner's advice, the Parties agree that it is not appropriate to ask for someone's consent in circumstances where the relevant professional staff acting in good faith have taken the view that the information in question will be released whether that consent has been given or not.

2.13 It is anticipated that most data sharing between the parties will be on the basis of routine joint working and pre-planned activities. However there may be instances, particularly urgent or emergency situations, where staff of either party may be asked to share information with staff from the other on an unplanned ad-hoc basis. This could be for a number of reasons, for example, to protect either staff or service users or to ensure emergency provision of services. In these circumstances the person requesting information may not be the person that the other party's member of staff normally deals with. In such situations, the following process should be observed:

2.13.1 The person receiving the request should satisfy themselves as to the identity of the person making the request and their reasons for making the request.

2.13.2 The person receiving the request should ascertain whether the person making the request has obtained the consent of the data subject to data sharing and, if not, should make a decision as to whether the circumstances require that consent should be sought before the data is shared or whether it is reasonable in all circumstances to share the data without seeking consent.

2.13.3 In determining what is reasonable, the staff member should have regard to the balance of risk as outlined at 2.6 – 2.8 above.

2.13.4 If deciding to share information then the data shared should be the minimum necessary to meet the requirements of the situation and data should be shared by the most secure means available.

2.13.5 Both the person making the request and the person providing the information should make a reasonable detailed record of the fact of data sharing and the reasons for it.

3. FAIRNESS AND TRANSPARENCY

3.1 It is a basic requirement of data protection law that individuals should be told (or easily be able to find out) who is holding information relating to them, what that organisation will do with that information, and who they will pass it on to. In terms of this Protocol, both Parties are "data controllers" of the personal information which they hold, including information which they have received from each other. For joint/integrated team settings, such as those within the Community Health and Care Partnerships, both Parties are jointly data controllers of information held in the joint team or integrated CHCP. This position should be made clear to any service user who approaches either Party and whose information may be shared under this Protocol.

3.2 The position regarding the identity of the data controller and the arrangements for sharing information between the Parties will be publicised by both Parties in a range of ways: through leaflets, poster, wording added to forms, and on the websites of the Parties. The minimum content of such a privacy notice is described in Appendix 2. The Parties will, through ongoing contact with service users and engagement with them, continue to raise awareness of the content of the privacy notice.

3.3 The content described in Appendix 2 is regarded as the minimum required to comply with the general legal obligation to provide a privacy notice. It is recognised that some service users and others will be interested in receiving much more information than this basic minimum. The Parties agree to respect such wishes by developing more detailed supplemental fair processing information to be provided to interested persons on request and published on their respective websites.

3.4 The Parties further recognise that even such a layered approach to the privacy notice requirements may not satisfy everyone and that there will still be some people with unanswered questions. Both Parties have in place existing (separate) mechanisms for such inquiries from members of the public and any such request will be dealt with through these existing procedures (and see also section 8 below)

3.5 As described in section 2 above, most information will be exchanged on the basis of the express consent of the individual concerned. Such consent requires to be informed consent, and so will only be valid if the individual has been given an appropriate privacy notice prior to consenting to what is described. However, as described in paragraphs 2.7, 2.9 and 2.10 there are circumstances where consent is not required. The Parties will, so far as possible, continue to provide appropriate fair processing information to the affected individuals even when their consent is not required (and not asked for) prior to the information being released. However, in some cases this is not appropriate, for example where telling someone about the proposed release of information might actually endanger a child or vulnerable adult. This will only happen in the circumstances described in paragraphs 2.9.5, 2.9.6 or 2.9.7 and even then only where the relevant professionals involved have formed a view that notifying the individual would have undesirable consequences for themselves or someone else.

3.6 The more detailed supplemental fair processing information described in paragraph 3.3 will, in particular, advise people as to when information will be shared without their express consent, and will also advise as to the sorts of activity where the Parties would release information without revealing the fact that they have done so to the individuals concerned.

4. SECURITY OF SHARED INFORMATION

4.1 The information passed between the Board and the Local Authorities under this Protocol can include extremely sensitive data. The Parties have evaluated the appropriate level of security and have concluded that the highest available levels of both organisational and technical security measures will be applied to this information.

4.2 Both the Board and the Local Authorities have information security policies which are designed to protect the information (particularly, but not exclusively, personal information) which they hold. These policies are binding on all staff of the employing Party and disciplinary action could be taken against staff who violate them. The policies apply to information held by that Party, whether it has originated with that Party or been passed to it by the other. Where there is a joint or integrated team, each member of staff continues to be bound by their own organisation's security policy. The governance arrangements for such joint working will address any particular security issues which require to be addressed beyond the scope of the general information security policies. Where the Board and a Local Authority establish any joint databases, the agreements regulating the creation and use of such databases will explicitly assign responsibility for information security to one or the other Party to ensure that this is not overlooked.

4.3 The Parties will review their respective information security policies and associated procedures in the light of this Protocol to ensure that they are compatible with each other. Any identified areas where they are not will be the subject of local guidance designed as a minimum to bring the less secure Party or Parties up to the level of the most secure one, and ultimately to bring all Parties up to the highest available levels of both organisational and technical security measures as indicated in Section 6.1. In addition, the professional staff of both organisations have shared professional values and obligations of confidentiality to service users and may be subject to professional disciplinary action (as well as, or instead of, disciplinary action by their employer) if they breach those obligations. This is emphasised in staff training.

In extreme cases of knowingly and recklessly disclosing personal information without the consent of the data controller, a criminal offence may have been committed and in appropriate circumstances any Party may refer a member of staff (or other individual) to the Police in connection with such an event. Staff disclosing personal data in line with this Protocol and any relevant local procedural guidance will be deemed to be acting with the permission of the data controller and so not be liable to criminal prosecution.

4.4 The Parties will each ensure that the other Parties are promptly notified of any security breaches or security risks (considered significant in line with current Information Commissioner's Office Guidance) affecting shared information. In addition, should the breach be considered significant, the ICO will also be notified. The Parties will, where appropriate, work together to rectify any such breach or mitigate any such risk to information security. If personal data is lost as a result of a security breach, the Parties will consider on a case by case basis whether to notify the affected individuals of the breach.

5. INFORMATION GOVERNANCE

5.1 Information Standards

5.1.1 Shared information only has value if it is accurate and up-to-date. The Local Authorities and the Board each have a range of initiatives underway to check the quality and accuracy of the data which they hold, and particular emphasis is placed on checking the accuracy and quality of information to be shared externally. These include case recording audit and revision exercises, supervision of case management procedures and similar data quality exercises undertaken from time to time.

5.1.2 Similarly, information exchange can only work properly in practice if it is provided in a format which the Party receiving it can utilise.

5.1.3 In all cases of data exchange, local guidance documentation will examine the precise data sets and fields which require to be exchanged in order to achieve a particular objective. These will be subject to periodic review at a local level to ensure the continued relevance of all the information exchanged.

5.1.4 The quality of data is important whether in shared records or in records held by one Party only. The Parties will make arrangements for periodic sampling of records held to evaluate the accuracy and general quality of data held.

5.1.5 The Parties undertake to notify the other as soon as practicable if an error is discovered in information which has been provided to the other Parties, to ensure that the Parties are then able to correct their respective records. This will happen whether the error is discovered through existing data quality initiatives or is flagged up through some other route (such as the existence of errors being directly notified to one or other Parties by the data subjects themselves).

5.1.6 The parties undertake to have in place risk management and disaster recovery processes which protects the integrity of personal data held for the purposes of data sharing or held in any joint databases or held in a joint working environment.

5.1.7 Relevant managers within each organisation will have the responsibility to notify through their own organisation's reporting procedures any significant failing in the systems that hold these data. The parties undertake to notify each other as soon as practicable if any such failing is identified and is likely to remain unresolved for significant period of time.

5.2 Retention

5.2.1 The Parties have their own policies on how long to keep different types of records (policies such as this are generally known as "retention schedules" as they describe how long to retain the different types of document or record). For some records, the retention period is laid down by law; for others, the Parties determine themselves how long they need to keep the records for. Shared information will be covered by the relevant provision of the holding Party's retention schedule, although it should be noted that it is still also covered by the retention schedule of the originating Party. In terms of operational requirements, the other Parties may not need to keep the information for as long a period as the originating Party, particularly for files with an extremely long statutory retention period. This is covered within the Parties' existing retention schedules

5.2.2 The Parties will ensure that their retention schedules (particularly relating to shared information) will be subject to periodic review to ensure that information is being kept for as long as required, but not any longer.

5.2.3 The respective retention schedules of the Parties describe, where applicable, the relevant statutory or professional regulatory or other guidance which has informed or set the retention period for the information in question.

5.2.4 The Parties have established mechanisms for archiving information which they require to retain for a period but which is not required for normal operational use. Such archiving helps comply with respect for the privacy of those involved by significantly reducing the number of people with potential or actual access to that information.

5.2.5 In general, information exchanged under this Protocol will be shared with the other Parties, and the originating Party will have retained a copy of the information for its own continuing use. Against this position, the Parties therefore agree that when information has reached the point where it is no longer required by one Party, that that Party will securely delete or destroy the information (in accordance with good information security practice) rather than returning it to the other Party. In some limited situations the

Local Authorities and the Board may be acting as "data processors" for each other. In these instances the originating Party remains the data controller of the information and the other Party is merely acting as their agent, processing the data under instruction. In these circumstances the Party acting as data processor will either delete/destroy the information or return it to the originating Party, as determined by the instructions of the originating Party under the relevant data processing agreement.

5.2.6 Data quality initiatives undertaken by the Parties will include within their scope a review of adherence to the agreed retention periods to ensure these are being applied correctly.

5.3 Privacy Impact assessments (PIA)

5.3.1 A Privacy Impact Assessment is a tool for assessing, prior to implementation, the benefits, risks and potential negative effects of any new or substantive change in the manner of processing or sharing personal data.

5.3.2 Each party agrees to carry out a PIA before implementing any new process involving the use of personal data where either party considers likely to have a substantive or significant impact upon the sharing of data under this protocol or on the use or sharing with third parties of any data that is held on any jointly held databases or held in a joint working environment

5.3.3 Such a PIA will include formal consultation with the other party as to the risks, benefits, privacy implications and potential reputational damage to the parties in introducing the new process and will be in line with guidance produced by the Information Commissioner's Office.

6. INDIVIDUAL'S RIGHTS

6.1 <u>Access to Personal Information</u>

6.1.1 Everyone has the right to ask to see what information an organisation holds which relates to them. The Parties have existing informal routes to give individuals access to the information held, which are encouraged and should continue to operate even in a joint working environment. However, the informal routes will not always provide access to complete files, which the formal right covers. This Protocol accordingly spells out how this right will be given effect to in a joint working environment.

6.1.2 The basic principle applied is that a subject access request addressed to either organisation will be taken to include any information relating to them which has been provided by the other Party, including information on any jointly held databases or held in a joint working environment such as a Community Health and Care Partnership (see paragraph 3.1). However, if there is any such shared information then a joint team meeting will be held to consider whether specific rules relating to health, social work or education files apply to any of the information concerned (and which might mean the individual is not given access to that information). This joint team meeting will also consider whether it would be appropriate to charge for the access request. The Parties have a policy of being as open with people as possible, but there are circumstances (described in paragraph

6.2.1 and 6.2.2 below) where someone will not be given full access to their file.

6.1.3 The Parties have existing procedures for processing subject access requests. It is recognised that not everyone will wish to see all the information held on them but may instead be interested in one particular issue. To facilitate this, and in addition to assisting those who might have difficulty in reading or understanding a copy of their file, the Parties permit individuals to attend their offices and inspect/be talked through their file, with appropriate explanations (and where appropriate, the offer of counselling) from professional staff. The Parties have existing accessibility strategies and access to translating and interpreting services should these be required to facilitate access by those with disabilities or for whom English is not their first language.

6.1.4 Any request to either the Board or the Local Authorities will be taken to include shared information which that Party has access to. The subject access procedures followed by both Parties therefore include searching any joint databases where appropriate, to ensure that all relevant information is located and, unless exempt (on which see paragraph 6.2) provided to the applicant. A request made to a joint team (such as a Community Health and Care Partnership) will be processed by whichever of the Parties appears most directly involved with the subject matter of the request.

6.1.5 A service user who wishes to request a copy of all the information on them held by each of the Board and Local Authorities must be advised that this can only be done by making separate requests, one addressed to each Party, from whom they want information.

6.1.6 A subject access request also includes the obligation on the data controller to advise the data subject as to the purpose the information is held and any potential recipients of that information. In terms of this Protocol, the Parties agree that they may refer to the fair processing material described in paragraph 3.3 above, and to this Protocol, Where information has been received by one Party from another, this will be clearly explained to the data subject (and the Parties will ensure that their records management procedures relating to joint working are able to capture this information).

6.2 Withholding data from subject access

6.2.1 The Parties agree that, consistent with their respective obligations under the Data Protection Act 1998 (and regulations made under the Act), not all information exchanged in terms of this Protocol should be released in response to a subject access request. In particular, care needs to be taken in respect of requests relating to Schedule 1 offenders, adults with mental incapacity, children, and deceased persons. The Parties agree to issue local guidance to their staff on how to respond to requests relating to these groups.

6.2.2 Information may be withheld in responding to a subject access for a number of reasons listed in the Data Protection Act 1998. In terms of the information shared in terms of this Protocol, information may be withheld on various grounds. The following (6.2.3 to 6.2.10) are the most obvious examples but this list is not exhaustive and where appropriate (and if necessary following the joint team meeting referred to in paragraph 6.1.2)

information may be withheld on other grounds permitted by the Act or regulations.

6.2.3 Schedule 1 offenders: information may be withheld which would prejudice any ongoing investigations or prosecutions, or would permit confidential witnesses or complainers to be identified, or would increase the risk posed by the offender to third parties; in the case of investigations, the fact that information is being withheld may itself be withheld to avoid tipping someone off about the fact that the investigation is taking place;

6.2.4 Children and adults with incapacity: since by definition the request must be being made by someone acting on the data subject's behalf, information may be withheld if the data subject has made it clear that they did not expect or wish the person acting on their behalf to see the information;

6.2.5 In the case of children, a request may be declined if the Parties feel that the person making the request is exercising their parental rights by making the request other than in the best interests of the child;

6.2.6 Deceased persons: while information relating to deceased persons is not covered by the provisions of the Data Protection Act, the Parties agree that this information remains sensitive and confidential in nature and should be protected by appropriate measures. In general, requests for information relating to the deceased will only be complied with where the law confers such a right (under the Access to Medical Records Act 1987 as amended) or where it can be seen to be compatible with ongoing professional obligations of confidentiality to the deceased person and their right to privacy;

6.2.7 In all cases, information relating to someone other than the immediate data subject may be withheld, other than information about health, social work or education staff (and even this may be withheld if there are concerns over e.g. staff safety);

6.2.8 Where clearly medically indicated, health information may be withheld from a person because providing it to them may cause serious mental or physical harm to the applicant or others;

6.2.9 Information may also be withheld where it would be likely to prejudice the carrying out of social work by causing harm to the physical or mental health of any person;

6.2.10 Information exchanged under the MAPPA arrangements (see paragraph 2.9.7), will almost always be exempt from data protection requests.

6.3 Objections to data processing

6.3.1 Individuals can object where the use of their personal data is causing them substantial, unwarranted damage or distress. This can be an objection to a specific use of information about them or to the fact that either or both parties hold any information at all on that individual.

6.3.2 If this objection is put in writing by the individual (often referred to as a 'section 10 notice') then the party receiving it is obliged to reply in writing within 21 days. This reply should either confirm that the party intends to comply with the request to stop processing data in the manner specified

and the timescale within which this will be done, or should confirm that they find the request unreasonable and do not intend to comply, in which case they must state reasons.

6.3.3 The parties each agree to have in place procedures to deal with such requests. Where the request covers information on any jointly held databases or held in a joint working environment then the party who receives the request agrees to notify the other party and to jointly discuss the matter before responding.

6.3.4 A person who wishes each of the parties to cease processing information held on them must be advised that this can only be done by submitting separate written notifications, one addressed to each Party.

6.4 Complaints

6.4.1 Individuals may have complaints about how their information is being shared, the accuracy of data held by either party, the fairness of comment and opinion relating to them or the manner in which a request to access data or notice to cease processing has been dealt with.

6.4.2 Each party agrees to deal with such complaints under the complaints procedure in place within their respective organisations.

6.4.3 Each party agrees to analyse and report on complaints received and to communicate to the other party where it appears to them that a significant number of complaints, or one or more complaints of a serious or significant nature, have been received relating to data sharing activities between the two parties. There should then be a joint discussion at management level in order to identify and resolve any problems within the data sharing activity.

7. FREEDOM OF INFORMATION

7.1 As noted above at paragraph 1.7, both the Board and the Local Authorities are Scottish public authorities for purposes of the Freedom of Information (Scotland) Act 2002. In consequence, the Parties are obliged to respond, within twenty working days, to any request for information submitted to them in a permanent form (such as letter or email). They are both additionally required to produce and maintain a Publication Scheme (describing the classes of information which they publish), requiring the approval of the Scottish Information Commissioner. The Publication Schemes of the Parties are available on their respective websites. The Parties will refer to this Protocol and its supporting documentation in their respective Publication Schemes and will include this Protocol and the supporting documentation to their websites for public perusal.

7.2 The Parties' obligations under freedom of information legislation include an obligation to respond to requests about information sharing practices and procedures such as the arrangements under this Protocol. Any request for information submitted to either Party will be processed under that Party's existing FOI handling procedures, and if necessary pass up through that Party's internal review procedure if the applicant is dissatisfied. The actual personal information exchanged between the Parties will, in almost every case, itself be exempt from disclosure under the freedom of information legislation, because exemptions built into the legislation mean that an individual cannot use FOI to obtain personal information about him/herself (the appropriate route for this is a subject access

request under the Data Protection Act 1998); nor can it be used to obtain information about someone else (as disclosures about other people may breach the Data Protection Act 1998) except in unusual circumstances. Requests for information submitted to a joint team such as a CHCP will be routed through the most appropriate procedure, based on the nature of the request and the information sought, unless the applicant has expressed a preference for the request to be handled by one Party rather than the other. Governance arrangements for CHCPs will address this issue in more detail. It should be noted that some information, such as that exchanged under the MAPPA arrangements (see paragraph 2.9.6), will almost always be exempt from both data protection and FOI requests.

7.3 A request for information may include a mixture of both personal information and non-personal information. Such requests require to be handled carefully and may require a joint team meeting to be convened to discuss the most appropriate way of dealing with this. The website of the Scottish Information Commissioner (www.itspublicknowledge.info) includes detailed guidance on this issue and should be referred to in appropriate cases.

8. REVIEW

8.1 Prior versions of the Information Sharing Protocol cease to have effect on the day this revised Protocol is signed by the Chief Executives of the Parties. This Protocol itself will continue in force until it is superseded by another Protocol in due course, or if all Parties agree to terminate it. Any Party may withdraw on giving six months' notice in writing of its intention to do so.

8.2 In drawing up this Protocol, extensive work was done to review what worked, and what did not work, in terms of the previous Protocols. That work has informed the terms of this Protocol and, critically, the terms of the various local procedural guidance documents to be issued under the Protocol. This work is ongoing and will continue to shape and inform future developments of the Protocol and the data sharing arrangements it is intended to facilitate. This Protocol will therefore be reviewed annually and, as a consequence of submission to ICO for endorsement, will be subject to audit at the discretion of the Information Commissioner. All Parties agree to such auditing and undertake to provide all necessary cooperation with the ICO in the event of an audit being held or considered.

8.3 In addition to these scheduled reviews, the Parties will also review this Protocol and the operational arrangements which give effect to it, if any of the following events takes place:

8.3.1 One (or more) of the Parties is found to have breached the terms of this Protocol in any significant way, including any data security breach or data loss in respect of personal data which is subject to this Protocol;

8.3.2 Any Party indicates that it intends to withdraw from this Protocol; or

8.3.3 The Information Commissioner or any of his or her authorised staff recommends that the Protocol be reviewed.

Any such unscheduled review may be either in respect of the entire Protocol, or only in respect of the elements of the Protocol directly relating to the event which triggered the review, as the majority of the Parties agree is appropriate.

8.4 The local guidance procedures and other documentation to be issued under this Protocol will be subject to document control and approval procedures agreed jointly by the Parties affected by the procedures in question.

8.5 If there is a dispute between the Parties concerning this Protocol, the Parties shall attempt to settle matters amicably on the basis of their respective professional perspectives. If a dispute cannot be resolved by the officers immediately concerned, they shall both escalate matters to a higher management tier, and ultimately to their respective Chief Executives IN WITNESS WHEREOF this information sharing protocol consisting of this and the seventeen preceding pages, together with the three appendices attached, are signed for and on behalf of the Parties as follows:

Executed for and on behalf of:	**NHS Greater Glasgow & Clyde**
Signature	
Name (Print)	
Job Title (Print)	
Date of Signature (Print)	
Location	

Executed for and on behalf of:	East Dunbartonshire Council
Signature	
Name (Print)	
Job Title (Print)	
Date of Signature (Print)	
Location	

Executed for and on behalf of:	East Renfrewshire Council
Signature	
Name (Print)	
Job Title (Print)	
Date of Signature (Print)	
Location	

Executed for and on behalf of:	Glasgow City Council
Signature	
Name (Print)	
Job Title (Print)	
Date of Signature (Print)	
Location	

Executed for and on behalf of:	Inverclyde Council
Signature	
Name (Print)	
Job Title (Print)	
Date of Signature (Print)	
Location	

Executed for and on behalf of:	Renfrewshire Council
Signature	
Name (Print)	
Job Title (Print)	
Date of Signature (Print)	
Location	

Executed for and on behalf of:	West Dunbartonshire Council
Signature	
Name (Print)	
Job Title (Print)	
Date of Signature (Print)	
Location	

Appendix 1: Template for local 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

The Local Authorities and NHS Greater Glasgow and Clyde 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

The Local Authorities and NHS Greater Glasgow and Clyde 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 2: Privacy Notice - Minimum Content

The Privacy Notice 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.

Appendix 3: List of Local Authority Headquarters

East Dunbartonshire Council
12 Strathkelvin Place, Kirkintilloch, G66 1TJ

East Renfrewshire Council
Eastwood Park, Giffnock, East Renfrewshire, G46 6UG

Glasgow City Council
City Chambers, George Square, Glasgow, G2 1DU

Inverclyde Council
Municipal Buildings, Greenock, PA15 1LY

Renfrewshire Council
Cotton Street, Paisley, PA1 1EN

West Dunbartonshire Council
Garshake Road, Dumbarton, G82 1HG