



**GENERAL PROTOCOL FOR
SHARING INFORMATION**

Document History

Copyright Notice

The original format of this document is copyright IBM (UK) Ltd. 1998.

Document Location

Tayside Data Sharing/Information Governance/FINAL ISP V3

Revision History

Date of this revision: 31/07/2007

Date of Next revision: 31/07/2008

Revision date	Version	Summary of Changes	Changes Section
31/07/07	3	Make changes as identified by SE to bring the protocol to gold standard status	numerous
29/05/03	2	Changed to include all council logos to act as a single protocol across all agencies within Tayside	
29/05/03	2	Changes to state only this protocol needs signed, the other protocols developed will reference this document in the appendices and will signatures will not be required	1.1.2 1.4 8.1.1 8.1.3
03/01/03	1.2	Variety of changes from the Angus version for Dundee	numerous
10/09/02	1.2	Variety of Changes from the original Perth Version for Angus	numerous
01/12/2001	1.0	Original version	

Approvals

This document requires the following approvals.

Name	Signature	Title	Date of Issue	Version
Professor Tony Wells		Chief Executive NHS Tayside	November 2007	3
Dr. Drew Walker		Director of Public Health NHS Tayside	November 2007	3
Dr. Bill Mutch		Medical Director NHS Tayside	November 2007	3
Mr. Stewart Forsyth		Medical Director Single Delivery Unit	November 2007	3
Mr. Alex Stephen		Chief Executive Dundee City Council	November 2007	3
Mr David Sawers		Chief Executive Angus Council	November 2007	3
Bernadette Malone		Chief Executive Perth and Kinross Council	November 2007	3

This is a Controlled Document. On receipt of a new version, destroy all previous versions (unless a specified earlier version is in use throughout a Project).

TABLE OF CONTENTS

DOCUMENT HISTORY	2
Copyright Notice	2
Document Location.....	2
Revision History	2
Approvals	2
SECTION 1.....	4
1. INTRODUCTION.....	4
SECTION 2.....	6
2. OBJECTIVES.....	6
SECTION 3.....	7
3. GENERAL PRINCIPLES	7
SECTION 4.....	12
4. PURPOSES FOR WHICH INFORMATION WILL BE SHARED	12
5. JOINT PROCEDURES	12
6. SUBJECT ACCESS	12
7. DISCLOSURE OF PERSONAL INFORMATION	14
8. ACCESS AND SECURITY PROCEDURES	19
9. PROTOCOL MANAGEMENT PROCEDURES	20
10. ACCESS AND SECURITY	22
SECTION 5.....	24
11. CONTRACTUAL AGREEMENT.....	24
APPENDIX A: PRINCIPLES OF THE DATA PROTECTION ACT	25
APPENDIX B: PROCESSING OF PERSONAL DATA	26
APPENDIX C: CONFIDENTIALITY STANDARDS	29
APPENDIX D: DICTIONARY OF DEFINITIONS	30
APPENDIX E - INFORMATION SHARING PROTOCOLS GUIDANCE.....	32

SECTION 1

1. INTRODUCTION

1.1. Scope

1.1.1. Joint Future has developed a two level approach to Information Sharing consisting of a General Protocol supported by Individual Protocols. Each Information Sharing context will require a unique set of policies and procedures and these are defined and agreed in the Individual Protocols. Each Individual Protocol exists within the context of nationally and locally agreed information sharing principles and these are contained in the General Protocol.

1.1.2 Whenever a subsequent agreement is made to share information between the Joint Future partners an Individual Protocol will need to be developed (*see Appendix E*) and the General Protocol will be included as an Appendix. Each organisation will *only require to sign the General Protocol, but the individual protocols should be approved through the Cross Boundary Strategic Group*. In practice this will allow additional projects to concentrate resources on the development of practical policies and procedures.

1.2. Parties to the Protocol

*NHS Tayside
Dundee City Council
Perth and Kinross Council
Angus Council*

all parties are defined in the Appendix D annexed and signed as relative hereto and are referred to in this document wherever the words “organisation”, “agency” or “party” are used.

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 requires agencies to work effectively and efficiently together to tailor services to the particular circumstances of each individual. Sharing information about an individual between partner agencies is vital to the provision of co-ordinated and seamless care to that individual.

1.3.2. There have been both real and felt barriers to information sharing 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 personal, inter-professional and inter-organisational mistrust; sometimes on worries about responsibility and accountability for personal information; sometimes on the absence of enabling mechanisms; and sometimes on technical matters. Where information sharing has occurred, its value has often been reduced by such problems as misunderstandings in the use of language or inefficiencies in communication channel. These barriers have led to concerns and to uncertainties about the circumstances of information sharing.

1.3.3. The General Protocol (and the Individual Protocols which will follow hereon) has been developed to address these responsibilities and concerns. The protocols are supported by training and procedures to ensure that boundary crossing processes work smoothly and are managed effectively.

1.3.4. The need to share information between agencies has long been recognised. The Information Management and Technology (IM&T) strategies of the partner agencies recognise the need for shared information standards and robust information security to support the implementation of Joint Future.

1.4. Development Process

The General Protocol has been developed by a Joint Future IM&T Group of NHS Tayside and its Local Authority partners. The protocol adheres to the national model recommended by the Scottish Executive. The intention has been to develop an over-arching protocol for all information-sharing applications. This is supplemented by protocols for specific applications which will adopt the common core principles as their base line. The Individual Protocols set out the specific arrangements and responsibilities designated, any additional requirements, and the service level agreements for that application, *if applicable*. The General Protocol is expected to cut down the development time for new protocols.

SECTION 2

2. OBJECTIVES

2.1 Purpose of this protocol

2.1.1. To provide a framework for the secure and confidential sharing of information between organisations to enable them to meet the needs of citizens for care, protection and support in accordance with legislative requirements.

2.1.2. To inform customers or patients of the organisations who are party to this protocol of the reasons why information about them may need to be shared and how this sharing will be managed.

2.1.3 This protocol does not represent a legal document but an agreed understanding of the legal issues relating to sharing information and the agreed principles and procedures to best meet these requirements.

2.2. The Document:

2.2.1. Sets out the principles which underpin the exchange of information between the parties detailed in section 1.2.

2.2.2. Specifies the organisational objectives which define the purposes for which these organisations have agreed to share information to meet their responsibilities to protect, support and care for citizens.

2.2.3. Describes the roles and structures which will support the exchange of information between parties to the protocol.

2.2.4. Describes the procedures which will ensure that information is disclosed in line with statutory responsibilities.

2.2.5. Describes the arrangements which have been agreed for exchanging information.

2.2.6. Describes the security procedures necessary to ensure that the confidentiality of information exchanged is maintained.

2.2.7. Sets out the responsibilities of organisations to implement internal arrangements to meet the requirements of the protocol.

2.2.8. Describes how this protocol will be implemented, monitored and reviewed.

SECTION 3

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 patient/client information (Personal Data) has been the **Data Protection Act 1998** ("the Act"). The Act does not apply to information relating to the deceased.

3.1.2. The Act gives seven rights to individuals in respect of their own personal data held by others, They are:

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

3.1.3. The key principles of the Act are set out in Appendix A.

3.1.4. The first 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 Schedule 1 of the Act requires those purposes (and other information) to be given to the data subject.

3.1.5. Another vital consideration on information sharing is whether the use of information for the additional purposes is permitted by the organisation's notified purposes – if not, amendments would need to be notified to the Information Commissioner.

3.1.6. The Act 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 personal data. Sensitive personal data, as defined by the Act, includes health data and information regarding a person's sexuality, ethnicity and trade union membership. The requirements of Schedules 2 and 3 are set out in Appendix B.

3.1.7. Where information sharing means that personal data is to be used for purpose(s) other than the original purpose then the fair processing code will need to be specified as part of an Individual Protocol (see 1.1).

3.1.8. If consent to a proposed disclosure is not forthcoming, compliance with another of the Schedule 2 or 3 conditions alone may not permit a disclosure, however, there are circumstances where organisations would still be able to make a disclosure. In particular, Section 29 of the Act permits this for the purposes of prevention or detection of crime, or apprehension or prosecution of offenders, and where those purposes would be likely to be prejudiced by non-disclosure. This is also permitted where information has to be made public, or where disclosure is required by law. For the purposes of the common law duty of confidentiality (see section 7), if there is no consent, this is the point where the need for confidentiality would need to be balanced against countervailing public interests – again preventing crime is accepted as one of those interests. For the purposes of the Human Rights Act 1998, the Article 8 rights would need to be considered.

3.1.9. Data subjects now have access rights to all records irrespective of when they were created, although

under Section 30 of the Act access to some health, education and social work data may be constrained or denied. Where there is a joint personal record, all parties must have arrangements in place to provide access. (It should be noted that for some categories of manual data, there are exemptions from some aspects of the Act up to 24/10/2007).

3.1.10. The Act 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 confidentiality requirements.

3.1.11. Section 115 of the **Crime and Disorder Act 1998** provides that any person has the power to lawfully disclose information to the police, local authorities or health authorities (or persons acting on their behalf) where they do not otherwise have the power, but only where it is necessary and expedient, for the purposes of the Crime and Disorder Act 1998. However, whilst all agencies have the power to disclose, section 115 does not impose a requirement on them to exchange information, and responsibility for the disclosure remains with the agency that holds the data.

3.1.12. Article 8 of the European Convention on Human Rights (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."

3.1.13. In the event of a claim arising from 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, an interference with that right can be justified but only if it can be shown that this is lawful; necessary to pursue a legitimate aim and proportionate to that aim.

3.1.14. All staff 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.

3.1.15. The duty of confidentiality requires that unless there is a statutory requirement to use information that has been provided in confidence or the 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). Whilst it is not entirely clear under law whether or not a common law duty of confidentiality extends to the deceased, the Scottish Executive Health Department (SEHD) and professional bodies responsible for setting ethical standards for health professionals accept that this is the case.

3.1.16. 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 Act apply whether or not the information was provided in confidence.

3.1.17. Where it is judged that an individual is unable to provide consent (for example due to mental incapacity or unconsciousness), other conditions in Schedules 2 and 3 of the Act must be satisfied (processing will normally need to be necessary in the *vital interests* of the individual) unless there is someone else who is lawfully entitled to consent on behalf of the individual (see section 7).

3.1.18. Whilst, under current law, no-one who has not been officially appointed to give medical consent on behalf of an adult can provide such consent on behalf of an adult, it is generally accepted that decisions about treatment, and the disclosure of information, should be made by those responsible for providing care and that they should be in the best interests of the individual concerned. Where consent is sought on behalf of children, then the Age of Legal Capacity (Scotland) Act 1991 will apply.

3.1.19. All partner agencies are subject to their own **codes or standards relating to confidentiality and information security** (see Appendix C).

3.1.20. NHS organisations which are party to this agreement are committed to the **Caldicott principles** when considering whether confidential 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

3.1.21. Scottish Access to Information legislation (including the **Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004**) provides, as at 1 January 2005, a statutory right of access to all information held by Scottish public authorities unless one of the exemptions to this right applies. Scottish public authorities are required to have procedures in place to facilitate disclosure of information under this legislation. In responding to requests for information which relate to matters covered by this and Individual Protocols, the parties undertake to co-operate fully with each other but the ultimate decision as to whether the information falls within one of the exemptions or not, rests with the organisation who receives the request for information. The "**Regulation of Investigatory Powers Act 2000**" and the "**Regulation of Investigatory Powers (Scotland) Act 2000**" also ensure that investigatory powers are used in accordance with human rights.

3.2. Principles governing the sharing of information in Joint Future

3.2.1. In seeking to share information to improve services and to support the citizens of Tayside, agencies in Joint Future will adhere to the following principles:

3.2.1.1. Organisations and agencies in Joint Future recognise that initiatives requiring a multi-agency approach cannot be achieved without the exchange of information about individual service users, levels of activity, the level and nature of resources and about their approach to addressing the issues. Their adoption of a multi-agency approach to address issues, therefore, includes a commitment to enable such information to be shared, albeit in a manner which is compliant with their statutory responsibilities.

3.2.1.2. Non-NHS organisations recognise the requirements that Caldicott imposes on NHS organisations and will ensure that requests for information from NHS organisations are dealt with in a manner compatible with these requirements.

3.2.1.3. Information is provided in confidence when it appears reasonable to assume that the provider of the information believed that this would be the case. It is generally accepted that most (if not all) information provided by patients/clients is confidential in nature. All organisations which are party 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 members of partner organisations staff in all organisations will respect this responsibility and not seek to override the procedures which each organisation has in place to ensure that information is not disclosed illegally or inappropriately.

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

3.2.1.5. Organisations/agencies 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 Act are adhered to and underpin the sharing of information between their agencies. They recognise the sensitivity of information about a person's racial or ethnic origin, political opinions, religious or other similar beliefs, trade union membership, physical and mental health, sexuality, the commission or alleged commission of any offence and any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings. Organisations which have obtained information in these categories about an individual, in the course of their direct contact with that person, will seek to obtain the explicit consent of that person to disclose that information to another 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 legal grounds for doing so and one of the remaining conditions in each of Schedules 2 and 3 of the Act can be demonstrated.

3.2.1.6. Individuals in contact with organisations/agencies will be fully informed about information which is recorded about them. If an organisation has statutory grounds for restricting an individual'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 organisation 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 individual 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.

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

3.2.1.8. In seeking consent to disclose information, an individual will be made fully aware of the information that will be shared and the purposes for which it will be used.

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

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

3.2.1.11. Careful consideration will be given to the disclosure of information concerning a deceased person and if necessary, legal advice will be sought on each individual case.

3.2.1.12. Organisations/agencies are committed to putting in place efficient and effective procedures to address complaints relating to the disclosure of information, and individuals will be provided with information about these procedures.

3.2.1.13. Organisations will ensure that all relevant staff are aware of, and comply with, their responsibilities in regard both to the confidentiality of information about people who are in contact with their organisation/agency and to the commitment of the organisations to share information.

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

3.2.1.15. Staff will be made aware that disclosure of personal information which cannot be justified on statutory grounds and under Schedules 2 or, in the case of sensitive information, Schedules 2 and 3 of the Act, whether inadvertent or intentional may be subject to disciplinary action.

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

SECTION 4

4. PURPOSES FOR WHICH INFORMATION WILL BE SHARED

The organisational objectives which define the purposes for Information Sharing are as follows :

- To improve the quality of services for citizens in Tayside.
- 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 integrated management teams and those of partner organisations with planning and management information.
- 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.

5. JOINT PROCEDURES

5.1.1. Each organisation will adhere to all joint policies and procedures formally agreed and authorised by both organisations.

5.1.2 Each organisation will adhere to each others internal policies and procedures covering Information Sharing, disclosure of personal information, access and security where appropriate.

5.1.3 Each organisation will ensure the availability of these policies and procedures to staff in the partner organisations as required (see Appendix C).

6. SUBJECT ACCESS

6.1.1. One of the most important rights given to individuals by the Act is the right of subject access. The following clauses shall apply if an individual/client or someone duly authorised to act on their behalf makes a request to any organisation for access to their personal data under Section 7 of the Act (hereafter a “subject access request”).

6.1.2 Organisations shall ensure that they have detailed subject access procedures and guidance in place to allow staff to respond to subject access requests. Organisations shall endeavour to synchronise these insofar as possible.

6.1.3. The organisation which receives the subject access request shall ascertain whether the individual/client’s personal data requested 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 (where appropriate).

6.1.4. In any case where an individual/client’s personal data contains both health information and social work information the organisation which received the subject access request shall, as soon as possible but in any event within 14 days of receipt of the request, ensure that a discussion takes place (where appropriate) involving relevant staff chosen, ensuring 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 (detailed further in 6.1.5) contained in Article 5(1) of the Data Protection (Subject Access Modification) (Health) Order 2000 (hereafter referred to as “the Health Order”) or Article 5(1) of the Data Protection (Subject Access Modification) (Social Work) Order 2000 (hereafter referred to as “the Social Work Order”) (both together known as “the Orders”) apply to the request under Section 7 of the Act. In any case where the subject access request has been made on behalf of

child aged under 12 years or on behalf of any adult with a mental incapacity, the discussion shall also consider whether the exceptions contained in Article 5(3) of each of the Orders are applicable in the case under discussion.

6.1.5. Although section 7 of the Act provides an individual/client with a right of access to his personal data, the Orders provide for circumstances where it is inappropriate to grant him full access if this would be likely to cause serious harm to the physical or mental health or condition of the individual/client or any other person. The Orders also provide that where someone else makes a request for information on behalf of the individual/client who is a child or an adult with mental incapacity, this should be withheld if provided by the individual/client in the expectation that the information would not be so disclosed.

6.1.6. The Health Order details when it is necessary to consult the Appropriate Health Professional (as defined below) prior to complying with the subject access request. Note: The Appropriate Health Professional should not be asked for consent to the subject access request being complied with in its entirety. He should merely be invited to participate in the discussion or provide a written opinion on whether the serious harm referred to in Article 5(1) of the Orders applies. Where the health professional involved in the discussion referred to in Paragraph 6.1.4 is not the Appropriate Health Professional and the Appropriate Health Professional is not available, the Caldicott Guardian of the organisation for whom the Appropriate Health Professional works or worked shall instead be consulted. For the purposes of this paragraph, “the Appropriate Health Professional” has the meaning given in the Data Protection (Subject Access Modification) (Health) Order and means;

- (a) the health professional who is currently or was most recently responsible for the clinical care of the data subject 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 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.

6.1.7. The organisations agree that, in relation to individuals/clients 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 individual/client and so falls to be justified in terms of the Adults with Incapacity (Scotland) Act 2000, in accordance with the procedure described in paragraph 6.1.8.

6.1.8. If a subject access request is received by either of the organisations in relation to individual/client personal data, but the request is made on behalf of an individual/client lacking capacity, the organisations shall follow the procedures described in paragraphs 6.1.3 to 6.1.7 as though the request had been by the individual/client but subject to the additional tests and safeguards described in paragraphs 6.1.9 to 6.1.14. It shall be the duty of the organisation which received the subject access request to ascertain whether the person purporting to act on the individual/client’s behalf is legally entitled to do so.

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

6.1.10. If the organisations are unable to reach agreement on the question of the proposed disclosure being of benefit to the individual/client, they shall advise the person making the request on the individual/client’s behalf that the request cannot be acceded to unless authorised by the Sheriff under Section 3 of the Adults with Incapacity (Scotland) Act 2000. The organisations agree not to release individual/client 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 organisations can reach agreement on the question of individual/client benefit.

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

6.1.12. Any release of individual/client personal data in terms of paragraph 6.1.8 to a person other than the individual/client shall be done under terms which inform the recipient of the individual/client personal data that they owe a duty of confidentiality to the individual/client in respect of that data.

6.1.13. It shall be the duty of the organisation which receives the subject access request to ensure that it is responded to within the Statutory 40 day time limit. All organisations shall therefore ensure that they have robust procedures in place to ensure timely consultation as required by this Section 6 of the Protocol.

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

7. DISCLOSURE OF PERSONAL INFORMATION

7.1. Obtaining consent

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

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

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

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

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

- Everyone has a right to prevent the disclosure of information about themselves.
- It is a requirement of the Act that consent to disclosure of information should be on an informed basis.
- The right to prevent disclosure is recognised by the organisation(s) involved. However, the organisation 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 organisation concludes that they have such a responsibility and this constitutes statutory grounds for disclosing information without consent, then they may exercise their right to do so.

7.1.6. Individual organisations procedures will specify the circumstances under which the agency may exercise their right to disclose information without consent.

7.1.7. Where a person does not have the capacity to make an informed decision but another person has authority to act as their representative and take decisions on their behalf, then this situation must be explained to that person. Individual agency procedures will identify who is able to take decisions on behalf of the client group concerned. Obtaining the signature of an individual who has not understood the implications of giving consent, or their choice to refuse consent, is not appropriate or lawful.

7.1.8 Where an individual does not have capacity to give consent to sharing information, the only person who can consent on their behalf is the person who has been given the power to do so either by a Court or through a Power of Attorney.

7.1.9 If it is believed that an individual is incapable of giving consent to sharing information about them, efforts should be made to discover if such a representative exists. This can be done by contacting the Office of the Public Guardian.

7.1.10 Where an individual does not have the capacity to make an informed decision, but another person has authority to act as their welfare guardian or attorney and take decisions on their behalf, that person should have the implications of sharing information explained to them in accordance with this guidance.

7.1.11 Where an individual is unable to give consent, and in the absence of a welfare guardian/attorney, information sharing may still be permissible in law if any of the circumstances set out in Section 6 apply. Only the minimum amount of disclosure necessary to achieve the desired aim should be disclosed.

7.1.12 If any of these circumstances apply, and before deciding to share information, account should be taken of any known wishes of the individual and appropriate carers. Discussion should also take place with other members of the care team in order to reach a decision as to whether or not information should be shared.

7.1.13 The decision to share information in these circumstances, and the reason(s) for that decision, should be recorded in accordance with the organisation's own procedures.

7.1.14 The record of the decision should include an explanation of why the individual cannot give consent, and how the sharing of information will meet one of the requirements set out in Section 6.

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

7.1.16 The client or their representative 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 organisation at that point in time and which require them to pass information about the case to staff based in another agency. They must be told the purpose and content of these records, details of how they are stored and who has access to them.

7.1.17 The client or their representative will be made aware that, other than for the purpose of protecting the vital interests of the client or the public or as otherwise required by law, personal information acquired by an agency, in the course of their direct involvement with that person, will only be disclosed to another agency with their consent.

7.1.18 In order to ensure that consent to the sharing of personal information is informed, all agencies will have available, material which explains:

- The rights of individuals under the Act , particularly in relation to sensitive information
- Details of the procedures in place to enable clients/patients to access their records

- Details of the procedures which may have to be initiated when a member of staff suspects that an individual has been or is at risk of abuse. These procedures must include details of who information will be shared with at each stage, what information will be shared 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 individual concerned believes information about them has been inappropriately disclosed.
- Details of how the information they provide will be recorded, stored and the length of time it will be retained both by the point of contact agency and the agencies to whom they may disclose that information.
- Details of the length of time for which consent to particular disclosures is valid

7.1.19 They will also make available a copy of the protocol covering the purpose for which consent to disclose is being requested at that point in time.

7.1.20 The material should be available in a variety of formats and languages. Agencies must also have access to appropriate means of communicating that information and ensure that these are made available if required. The person concerned must be given sufficient time to consider the material provided. There should be no doubt that the person concerned or, in the event that a person is unable to make informed decisions, their legitimate representative, have been given every help to access and understand the facts before being asked to give consent.

7.1.21 Given the stressful conditions which may exist at the time a person is in direct contact with an organisation, it is unlikely that conditions will exist for the person to fully digest and understand their rights at that point in time. Each agency will have in place a strategy, therefore, to inform the public of their rights and the requirement for them to give consent.

7.2. Recording consent

7.2.1. Agencies must have a means by which an individual 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-riden only if there are statutory grounds for doing so and one of the conditions of Schedule 2 of the Act can be demonstrated. For sensitive personal information, one of the conditions of Schedule 3 of the Act must also exist (Appendix B).

7.2.2. Individuals should be able to prescribe, in respect of all information held by the contact organisation:

- Which organisations information can and cannot be shared with.
- Whether the defined shared dataset can be shared or remain confidential.

7.2.3. In addition, in respect of sensitive personal information (as defined by the Act) which is held by the contact organisation, individuals must be able to prescribe the explicit purposes for which they agree to this information being disclosed to another organisation.

7.2.4. This means that an individual must have access to their files in order to comprehend what information an organisation holds about them and must be given an opportunity to amend and correct any information which is incorrect.

7.2.5. It is recognised that, in an urgent or emergency situation and in many routine referrals, it is impractical for existing client records to be studied in detail and amended at that point in time. All organisations should therefore have procedures in place to ensure that clients are fully informed at all times of the content of their records (both manual and computerised) and have opportunities to amend the contents if they are wrong.

7.2.6. Under no circumstances will consent be sought, or taken to have been given, unless the individual or their representative has been fully informed of the consequences of giving consent. As such, consent forms will contain a facility for the individual to confirm that such information has been made available to them. The consent form should be stored in the individual'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 individual.

7.2.7. If a person 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 with 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.

7.2.8. Consent to disclosure of personal information for a particular purpose, will continue indefinitely until the individual concerned withdraws consent. A record must be kept of the date consent was given and the date on which it was withdrawn. If at any time following the withdrawal, an organisation wishes to disclose that information for the same or another purpose, then consent will need to be sought again.

7.3. Checking for consent

7.3.1. An individual's personal case file should always be checked to ascertain consent before personal information is disclosed to another agency. Members of staff without access to an individual's case file must check with case holders before releasing information.

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

7.3.3. Particular care should be taken before sensitive information as defined by the Act is released. Sensitive personal information should only be released if its disclosure is critical to the case, explicit consent has been given to its release for that purpose or the disclosure meets one of each of the other Schedule 2 and 3 requirements or as otherwise required by law.

7.3.4. When disclosing information about individual clients, organisations 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 individual.

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

7.3.6. Organisations will be kept fully informed about the disclosure of information originating from their files, whether it is with or without the consent of the person 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 protocols must specify who will be responsible for ensuring that this is done.

7.4 Disclosing information without consent

7.4.1. Passing information without consent could place both individual staff members and organisations at risk of prosecution. If there is no lawful basis for disclosing information without consent, there is also the risk of an enforcement order or action under the Data Protection Act, or damages for breach of confidence/breach of the Human Rights Act 1998.

7.4.2. The disclosure of personal information without consent must be justifiable on statutory grounds and meet one of the conditions of Schedule 2 of the Act.

7.4.3. In addition, the disclosure of "sensitive" personal information without consent must meet one of the conditions of Schedule 3 of the Act.

7.4.4. Each agency will therefore appoint a person or persons who has the authority and knowledge to take responsibility for such a decision. Person(s) with this authority will be available at all times, to enable emergency situations to be dealt with.

7.4.5. 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 Act can be met. If they are in any doubt, they should refer the case to the designated legal expert for advice. It is the responsibility of each organisation to ensure that the responsible staff know how and who to contact for legal advice. Individual agency procedures will indicate who will provide the legal expertise for the client group covered by the procedure.

7.4.6. If information is disclosed without consent, then full details will be recorded about the information disclosed, the reasons why the decision to disclose was taken, the person who authorised the disclosure and the person(s) to whom it was disclosed. Individual agency procedures will specify the person(s) responsible for ensuring this happens.

7.4.7. Wherever possible organisations will nominate contacts for the receipt of personal information. These contacts will be responsible for instigating the agreed security procedures to ensure that this information is restricted to those who need to know it for the purposes agreed. Individual Protocols will set out the contacts agreed for the purpose integral to that protocol.

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

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

7.4.10 In circumstances where the individual refuses to give consent, this should be recorded on the consent form and signed by the assessing officer/professional. The implications of the refusal in limiting the responses of all agencies should be explained to the individual and the fact that this has been done should be recorded.

7.5. Staff Guidance on Consent-seeking

7.5.1. To support staff, each organisation will put in place procedures that give clear guidance on:

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

7.6. Maintaining contact details

7.6.1. All organisations will maintain a list of the staff who have been trained to seek consent.

7.6.2. Organisations 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 Protocols
- who will provide legal advice in respect of the disclosure of information concerning a particular client group
- who is authorised to receive confidential information in respect of a particular purpose

8. ACCESS AND SECURITY PROCEDURES

8.1. Transfer of personal information

8.1.1. It is essential that requests for information about particular individuals 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 data subject should accompany requests for information wherever possible.

8.1.2. Agencies will take every precaution to ensure that information which identifies individual clients and/or patients is transferred and shared in a secure manner.

8.1.3. Fax transfer will be avoided wherever possible. Where it is necessary, then individual agency procedures for secure transfer by fax will be followed.

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

8.1.5. It is recognised that in urgent cases, information about individual clients and/or patients may have to be requested or provided via the telephone. The internal agency code of conduct for transferring and sharing information verbally will be followed. Face-to-face transfers are also covered by this code. All organisations should ensure that their internal procedures reflect this code of conduct.

8.1.6. Written communications containing personal information should be transferred in a sealed envelope and addressed by name to the designated person within each organisation. They should be marked "Personal and Confidential – to be opened by the recipient only". 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 an organisation 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 all partners so that an alternative means of transfer can be adopted where it is essential that the information is restricted to those who have a need to know.

8.1.7. Where information is compiled for a particular purpose, then the protocols 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 Individual Protocol.

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

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

8.2.1. It is recognised that members of organisations fulfil a number of roles within that organisation. In fulfilling one particular role, they may be given privileged access to information about a client or patient which they believe would assist them in one of their other roles, or be of wider interest to their organisation.

8.2.2. However, confidential information is disclosed only for the purpose specified at the time of disclosure and it is a condition of access that it should not generally be shared or used for any other purpose without the consent of the original data controller or the data subject (unless one of the remaining Schedule 2/3 conditions can be met). The purpose will be set out in the Individual Protocol and information should not be shared or used for any other purpose.

8.2.3. Members 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 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 patient or client to the further use of that information or to decide whether the reason the information is required justifies disclosure without consent.

8.2.4. Individual Protocols 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 one of the other parties to a protocol.

8.3. Restrictions on the use of statistical and anonymous data

8.3.1. Organisations in receipt of statistical data derived from the client records of partner organisations must request permission from the originating organisations (the data controller) if they wish to use that information for any purpose other than that for which the information was originally provided.

8.3.2. Organisations submitting or circulating reports or articles beyond the community covered by this protocol which incorporate statistics or other data supplied by a partner, will ensure that the other organisation has the opportunity to view and comment on the report prior to its release.

8.3.3. Individual Protocols 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 the protocol

8.4. GP Clinical Systems

The sharing of patient's medical history and medication from GP clinical systems will only take place with the explicit consent of the GP and the patient/client (or as otherwise required by law) and under the strict controls as documented in this General Protocol and any relevant Individual Protocols.

9. PROTOCOL MANAGEMENT PROCEDURES

9.1. Formal approval and adoption

9.1.1. The General Protocol is a product of the Joint Future Agenda and will be formally signed off by all Health and Council parties. *Individual Protocols will be signed off by the Cross Boundary Strategic Group.*

9.1.2. The Protocols will continue to be developed as part of Joint Future and will be formally reviewed on an annual basis.

9.1.3. Formal adoption will follow the signing of the document *as described in 9.1.1 above*. They will then be formally adopted by each signatory agency involved in Information Sharing *and individual protocols will be developed to provide guidance to staff involved in the sharing of information.*

9.2. Dissemination/Circulation of protocol

9.2.1. Protocols will be introduced to managers and fieldworkers following internal agency training plans and procedures.

9.2.2. Copies of protocols will be circulated to all relevant staff, in line with the each agency's internal arrangement for distribution of procedures and guidelines. Wherever possible, the protocol will be available to staff on-line.

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

9.2.4. Protocols will be published, wherever possible, on the web sites of organisations involved and made available at information points such as Public Libraries. Each partner agency will keep sufficient copies to enable the protocol to be readily available to members of the public who require it.

9.3. Monitoring and review procedures

9.3.1. All protocols will be subject to regular formal review.

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

9.3.3. Each protocol will set out the particular arrangements for the review of that protocol. These will include details of:

- The body responsible for reviewing and agreeing changes to the protocol
- The date of the initial review and the review frequency
- The body or individual who will co-ordinate the review

9.3.4. Following the introduction of a protocol, its use and application 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 in all protocols. During this period changes will only be considered if the issues and problems identified are felt to be a significant barrier to information exchange.

9.3.5. The use and effectiveness of the protocol will be evaluated in a number of ways.

9.3.6. Staff in all organisations will be required to log and report responses and behaviour, which they believe, are in breach of the 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 protocol are addressed before they become a major issue.

9.3.7. Complaints received by organisations will be analysed to determine whether they relate to a breakdown or inadequacy of an information-sharing protocol. All organisations will establish a procedure by which they deal with reports regarding the inappropriate use or disclosure of information to the body responsible for the security of that information.

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

9.4. Reporting breaches of the protocol

9.4.1. The period following the introduction of the protocol until the completion of the first formal review of the protocol will be regarded as the pilot phase. During the pilot phase, all breaches of the 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. It will be necessary to designate a responsible officer for monitoring any such breaches who will deal with the matter in accordance with their organisation's procedures.

9.4.2. The following types of incidents will be logged :

- Refusal to disclose information
- Conditions being placed on disclosure
- Delays in responding to requests
- Disclosure of information to members of staff who do not have a legitimate reason for access;
- Non-delivery of agreed reports
- Inappropriate or inadequate use of procedures e.g. insufficient information provided
- Disregard for procedures

- The use of data/information for purposes other than those agreed in the protocol
- Inadequate security arrangements
- Actual or attempted access security breaches

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

9.4.4. *Breaches noted by members of staff:*

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

9.4.4.2. Individual Protocols should detail the mechanism by which breaches will be reviewed, addressed and resolved. A log should be maintained of breaches to the protocol to enable review of the protocol.

9.4.5. *Breaches alleged by a member of the public:*

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

- Make them aware of their rights in relation to information that the organisation 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.

9.4.5.2. 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 organisation who received the complaint: Any disciplinary action will be an internal matter for the organisation concerned.

9.4.5.3. However, in order to monitor and police adherence to and use of this protocol, procedures should be established within each organisation by which complaints relating to the inappropriate disclosure of information are passed to the officer designated to deal with breaches of the protocol. The designated officer should report any complaints of this nature to the appropriate officer in each agency (Caldicott Guardians within NHS Tayside, and the Data Protection Officer the Councils). Individual Protocols should detail the specific arrangements for that protocol.

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

10. ACCESS AND SECURITY

10.1. Access to individual identifiable information must be restricted to staff who need access to it to enable them to perform their duties..

10.2. The partner organisations must take all reasonable care and ensure safeguards are in place to protect both systems for the storage of data and the data contained within them.

10.3. All computer systems containing identifiable information must be effectively password protected and staff members must not divulge their password, or leave systems active when they are absent.

- 10.4. All computer systems must be kept in secure locations and any associated items, such as CDs, disks or tapes, must be stored in a secure area when not in use.
- 10.5. Identifiable personal information will not be left on voicemail or answerphone systems unless these can only be accessed by the designated recipient via a secure password.
- 10.6. When using answerphones for receiving information about individuals, every effort should be made to avoid messages being overheard by unauthorised personnel.
- 10.7. All manual files containing identifiable information should be stored in secure, locked areas when not in use.
- 10.8. Records held on individuals, other than those held by the individual themselves, will not be taken from the office or building where they are normally kept, except when absolutely necessary.
- 10.9. Destruction of files should comply with the partner organisations' own regulations governing the retention, safekeeping and disposal of confidential information.

SECTION 5

11. CONTRACTUAL AGREEMENT

11.1. Undertaking

11.1.1. 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 their agencies in a manner compliant with their statutory and professional responsibilities.

11.1.2. As such, they undertake to :

11.1.3. Implement and adhere to the procedures and structures set out in this protocol.

11.1.4. Ensure that all **INDIVIDUAL PROTOCOLS** established between their agencies for the sharing of information relating to the delivery of integrated health and social care services to the citizens of Tayside are consistent with the relevant legislation and this **GENERAL PROTOCOL**.

11.1.5. Ensure that where these procedures are adopted then no restriction will be placed on the sharing of information other than those specified within **INDIVIDUAL PROTOCOLS**.

11.2. Indemnity agreement

11.2.1 The indemnity procedures fall under the jurisdiction of the Caldicott Guardians, or their equivalent, in each of the partner organisations and will be specified within **INDIVIDUAL PROTOCOLS** (see section 8.2.4).

11.3. Signatures.

11.3.1 We, the undersigned , agree to adopt and adhere to this information sharing protocol:

Name	Signature	Title	Date of Issue	Version
Professor Tony Wells		Chief Executive NHS Tayside	November 2007	3
Dr. Drew Walker		Director of Public Health NHS Tayside	November 2007	3
Dr. Bill Mutch		Medical Director NHS Tayside	November 2007	3
Mr. Stewart Forsyth		Medical Director Single Delivery Unit	November 2007	3
Mr. Alex Stephen		Chief Executive Dundee City Council	November 2007	3
Mr David Sawers		Chief Executive Angus Council	November 2007	3
Bernadette Malone		Chief Executive Perth and Kinross Council	November 2007	3

APPENDIX A: Principles of the Data Protection Act

1. Personal Data must be processed (e.g. collected, held, disclosed) fairly and lawfully (looking to the common law and other legislation) and processing must satisfy one of the conditions in Schedule 2 of the Act. Sensitive personal data, e.g. health information, is further protected in that processing must satisfy at least one of the conditions listed in Schedule 3 of the Act i.e. for the processing of sensitive personal data a Schedule 2 *and* a Schedule 3 condition need to be met.
2. Personal Data shall be obtained and processed only for one or more specified and lawful purposes.
3. Personal Data shall be adequate, relevant and not excessive in relation to the specified purpose(s).
4. Personal Data shall be accurate and kept up to date.
5. Personal Data shall not be held longer than is necessary.
6. Processing must be in accordance with the rights of the individual (in particular the right of access to information held).
7. Appropriate technical and organisational measures should protect Personal Data.
8. Personal Data should not be transferred outside of the EU unless adequate protection etc is provided by the recipient.

This is the Appendix A referred to in the foregoing Agreement between NHS Tayside and the Councils

APPENDIX B: Processing of Personal Data

1. SCHEDULE TWO: CONDITIONS RELEVANT FOR THE PROCESSING OF ANY PERSONAL DATA

The data subject has given his consent to the processing.

The processing is necessary for the performance of a contract to which the data subject is a party, or for the taking of steps at the request of the data subject with a view to entering into a contract.

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

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

The processing is necessary for the administration of justice; for the exercise of any functions of either House of Parliament; for the exercise of any functions conferred on any person by or under any enactment; for the exercise of any functions of the Crown, a Minister of the Crown or a government department; or for the exercise of any other functions of a public nature exercised in the public interest by any person.

The processing is necessary for the purpose of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject. The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

2. SCHEDULE THREE: CONDITIONS RELEVANT FOR THE PROCESSING OF SENSITIVE PERSONAL DATA

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

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

(2) The Secretary of State may by order exclude the application of sub-paragraph (1) in such cases as may be specified, or provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

The processing is necessary-

a) in order to protect the vital interests of the data subject or another person, in a case where consent cannot be given by or on behalf of the data subject, or, the data controller cannot reasonably be expected to obtain the consent of the data subject, or

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

The processing -

a) is carried out in the course of its legitimate activities by any body or association which is not established or conducted for profit, and exists for political, philosophical, religious or trade-union purposes,

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

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

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

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

The processing-

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

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

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

(1) The processing is necessary –

(a) for the administration of justice,

(aa) for the exercise of any functions of either House of Parliament

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

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

(2) The Secretary of State may by order -

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

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

(1) The processing is necessary for medical purposes and is undertaken by a health professional, or a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

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

(1) The processing is of sensitive personal data consisting of information as to racial or ethnic origin, is necessary for the purpose of identifying or keeping under review the existence or absence of equality of

opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and is carried out with appropriate safeguards for the rights and freedoms of data subjects.

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

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

This is the Appendix B referred to in the foregoing Agreement between NHS Tayside and the Councils

APPENDIX C: Confidentiality Standards

This section contains each organisation's codes or standards relating to confidentiality :

Dundee City Council

Corporate Information Strategy
Information Security Policy Statement
Communications Policy
General Computer Security Policy
Data Protection Policy
Data Protection Subject Access Guide
Access to your Information leaflet
Email Security Policy
Internet Security Policy

Angus Council

Access to Information Policy
Guide for Customers – Data Protection
Overview for Customers – Data Protection
Subject Access Procedures
Guide for Employees – Data Protection
Overview for Employees – Data Protection
Employee Guidance – You, the Council and Data Protection
Email and Internet Policy
Information Security Policy
Information Security Policy User Guidelines
Information Security Management System

Perth and Kinross Council

Information Security Policy
Information Security Standards
Communications Security Policy
Data Protection Policy

NHS Tayside

Information, Management and Technology Strategy
Information Security – Information Technology Security Policy
Intranet, E-mail and Internet Services – Access Terms and Conditions
E-Mail Services – Policy
NHS Tayside Data Protection Policy
Information Management Handbook

This is the Appendix C referred to in the foregoing Agreement between NHS Tayside and the Councils

APPENDIX D: Dictionary of Definitions

Council	A local authority constituted by the Local Government etc. (Scotland) Act 1994.
Applications	Situations in which Individual Protocols may be required.
Caldicott	Review led by Dame Fiona Caldicott into the use of patient-identifiable information for non-clinical purposes with recommendations on appropriate safeguards to govern access to and storage of such information.
Joint Future	A partnership between Angus, Dundee and Perth and Kinross Councils and NHS Tayside to provide fully integrated health and social care services for the citizens of Tayside.
Citizen	Any individual resident, or temporarily living in Tayside.
Client	A customer of Joint Future.
Confidentiality of information	As defined in the Data Protection Act, by the Caldicott principles and by common law.
Consent	In this context the authority given by a patient or client to an organisation to share information.
Contracts	A legal agreement between agencies.
Data Protection Act 1998 /DP Act 1998	The main Act which governs all personal data held on computer and manual files and all relevant statutory instruments made under the Act, including but not exclusive to the Data Protection (Subject Access Modification) (Health) Order 2000 and the Data Protection (Subject Access Modification) (Social Work) Order 2000. All references to the Data Protection Act includes references to any amendments to the Act.
Data subject	Patient / client / customer about whom identifiable information is being shared.
Disclosure	The act of passing patient or client information to a third party.
General Protocol	An agreement between two or more organisations which defines the framework and principles for sharing information.
Health Board	Health body that funds, plans and develops services.
Indemnity Agreement	An agreement whereby the parties involved in the protocol agree to keep each other free from any legal damage or legal loss or other legal penalties.
Individual Protocol	An agreement between two or more organisations which defines the specific requirements and procedures for sharing information (in respect of any one particular purpose).

Information Community	Signatories who have agreed to share information in accordance with the protocol.
NHS Tayside	"NHS Tayside" is the name of the local health system. Tayside NHS Board is responsible for the delivery of health services for the population of Tayside throughout that system.
Non Signatories	Organisations not covered by the protocol but who may be involved with the client group through contractual agreements.
Person	In this document used in preference to 'patient', 'client' 'user' to describe someone in contact with health and/or local authority services.
Principles	Statutory and non-statutory framework and guidance relevant to the information community.
Procedure	A document describing roles, responsibilities and actions required to achieve a business purpose e.g. dealing with a complaint.
Protocols	Describe how a service will be provided by one or two or more agencies.
Seamless Service	Describes a philosophy of care to ensure that a person's health and social needs are provided in a co-ordinated way.
Secure	As defined in the Data Protection Act and by the Caldicott principles.
Signatories/Parties	Organisations who have agreed to share information in accordance with the protocol.
Staff	Employees of the party organisations.

This is the Appendix D referred to in the foregoing Agreement between NHS Tayside and the Councils

Appendix E - Information Sharing Protocols Guidance

Introduction

The General Information Sharing Protocol has been signed by NHS Tayside and the three local authorities. There is a requirement from this protocol to produce Individual Protocols for staff who are involved in the sharing of information to advise them on their responsibilities. There is no need for these individual protocols to be signed, however they must gain the approval of the Cross Boundary Working Group and ultimately the Cross Boundary Strategic Group before they are formally adopted. A register of approved protocols will be created and maintained by the Working Group.

Development of the Individual protocols

Where possible the protocols should be developed in conjunction with health and local authority parties to ensure reduction in duplication and to avoid confusion for staff.

The protocols should have a clear purpose for being developed and staff should check with the Cross Boundary Working group to ensure similar protocols have not already been or are in the process of being developed.

The protocols should contain a document history. This should contain Document Owner and Person responsible for updating. It should also state the target audience and to whom it has been formally issued to and the review date. Within the body of the protocol it should state that it will be reviewed annually.

The protocols should also reference the General Information Sharing Protocol as an appendix which can be made available to those who require it.

Service Level Agreements

If the sharing of information involves the use of an IT system between Health and Local Authority Partners, then a Service Level Agreement may be required to be drawn up. If this is the case then this should be recorded beside the protocols.

If any of the systems require access to the Community Health Index, then the relevant paperwork should be completed for each system and on behalf of the users who will be using this system. This paperwork is required as part of the NHS Tayside Information Management & Technology Strategy and is the only additional document which requires signatures.

This is the Appendix E referred to in the foregoing Agreement between NHS Tayside and the Councils