Information Sharing Toolkit

The Information Sharing Protocol

Effective From: 1st January 2010

INDEX

Acknowledgements

The documents comprising the Information Sharing Toolkit have been produced as a result of the combined efforts and contributions of a wide variety of individuals and groups from a range of organisations at local, regional and national level.

Particular thanks go to the following bodies:

- ***Greater Merseyside Connexions Partnership***
- ***Knowsley ISAP Information Sharing Sub-Group***
- ***Cheshire & Merseyside Strategic Health Authority Information Governance Group***
- ***North Mersey LIS Team***
- ***Local e-Government Standards Board IS Protocol Group***
- ***North West ISAP Cluster Group***
- ***Various Other Local Authority ISAP Trailblazer & Non-Trailblazer Groups***
- ***Merseyside Police (Joint Agency Group)***
- **St Helens Multi-Agency Information Sharing Review Group**
- ***Various Other Local Authorities and Partner Organisations***
- ***DCFS - -ISA Information Sharing Reference Group***
- ***Department for Constitutional Affairs – Information Rights Division***
- ***Information Commissioner's Office***

Apologies if anyone has been omitted.

Version Control

Version	Amended Date	Amended By	Main Changes
1.0	01.06.2009	J McKeown	First Working Draft for comment & approval
1.1	24.06.2009	J McKeown	Added Version Control/Non legally binding statement
1.2	21.12.2009	J McKeown	Minor updates to font type, layout and weblinks

Commonly used Data Protection Terms within this document and can be found in Appendix 1 - Definitions & Glossary

1. Introduction

1.1 General

The Information Sharing Toolkit has been developed to establish a comprehensive and consistent standard within and across organisations/authorities in respect of the treatment of personal identifiable information. It places the '**Service User(s)**' (i.e. children, young people, adults and their families) at the centre of how their information is used and which all signatory organisations will adopt and work towards implementing.

This Information Sharing Protocol (ISP) is the first element of the Toolkit. It sets out the rules, values and principles for information processing and sharing between organisations irrespective of the purpose. It is aimed at an organisation's 'strategic' level. It is not a legally binding document, but one that promotes effective practice when sharing data.

The other elements of the Toolkit are as follows:

- **Information Sharing Arrangement (ISA)** – This is a means of defining a specific community of two or more organisations who have come together for a common purpose with a shared objective in respect of information sharing. It state the "Who, What, When, Where, Why and How personal information is to be shared between the organisations. It is aimed an organisation's 'middle management' level.

- **Operational Arrangement (OA)** – This is a means of capturing the relevant business processes (Work Instructions) that will support effective information processing/sharing for a particular purpose and then communicating those to the appropriate operational staff within and across organisations. It is aimed at an organisation's 'operational manager/practitioner' level.

- **Privacy, Confidentiality & Consent** – This covers the range of processes and documentation that will directly impact on service users and includes things such as 'Privacy/Confidentiality Statement', 'Fair Processing Notice or Privacy Notice', 'Consent', 'Subject Access', etc. It is aimed at an organisations 'service user' level.

- **The Appendices** – are the principal reference guides and support the application of of the Toolkit.

1.2 Background

Partner Organisations/Agencies (Partner Organisation) supplying services to their users customers or clients who are resident, or accessing services, within ***the area covered by any partner organisation*** and are continually processing information about them. At times a single organisation working with a service user(s) may identify a range of issues that need to be addressed, some of which are outside of its scope or expertise. Conversely, more than one partner organisation could become involved with a service user(s) but they are unaware of each others involvement.

These organisations may be gathering the same basic information, undertaking similar assessments and producing/implementing plans of action that are appropriate to the organisations perceived need of response rather than the whole need of a service user(s). Consequently, there is often unnecessary duplication of effort, poor coordination and a lack of a coherent approach to the particular issues facing a service user(s) which could be potentially detrimental.

In these circumstances it has been recognised that a co-ordinated multi-agency response is the best way of ensuring that service users receive the type and level of support most appropriate to their needs.

Therefore, the sharing of relevant and appropriate information between organisations and their practitioners, when it is needed, with a degree of confidence and trust is vital in ensuring that service users receive the 'seamless', high quality, support they expect.

Thus, information (data) sharing should not be seen as an activity in its own right but as a necessary/reasonably ancillary requirement to the effective delivery of a policy or service that respects people's legitimate expectations about the privacy and confidentiality of their personal information but also considers the consequences of a **failure** to act.

1.3. Information (Data) Sharing Categories

There are three broad categories of information relating to service users that organisations may wish to collect, store and share and these are as follows:

- **Aggregated (Statistical) Information**
  Aggregate and management information used to plan and monitor progress of the organisation in its delivery of services and to manage its local focus so as to provide the most effective support to its service users. This is generally outside of the remit of the Data Protection Act 1998.

- **Depersonalised/Anonymous Information**
  Information that has had all person identifiable information removed (e.g. name, address, unique identifiers, etc) so as to render it anonymous and therefore outside the remit of the Data Protection Act 1998.

- **Personal Identifiable Information (including non-sensitive, confidential and sensitive data)**
  Information (name, address, unique identifiers, etc) relating to a ***living individual***, including their image or voice, that enables them to be uniquely identified from that information on its own or from that and other information available to the organisation.

The Data Protection Act 1998 defines seven types of personal identifiable information to be **'sensitive data'** and these are:

- Ethnicity
- Religious Beliefs
- Criminal Proceedings
- Physical or Mental Health
- Sexual Life
- Political Opinion
- Trade Union Membership

To process any ***'Personal Identifiable Information'*** at least one of the conditions from Schedule 2 of the Data Protection Act 1998 must be met *(See Section 4.7 & Appendix 3)* and if it is '***sensitive information***' ***(see above)*** then at least one of the conditions from **both** Schedule 2 **and** Schedule 3 of the Data Protection Act 1998 must be met *(See Section 4.7 & Appendix 3)*.

There may also be 'Personal Identifiable Information' outside of that defined as 'sensitive' by the Data Protection Act 1998 *(See Section 1.3)* but has been identified by the signatory organisations as being of a personal and sensitive nature, known as "Professionally Sensitive Information" but more often called "Confidential Data".

Examples of this include client characteristics (substance misuse, homeless, refugee, truant, etc), opinions or assessment data.

In respect of Confidential Data it is recommended that signatory organisations treat this in the same manner as Sensitive Information and that any Information Sharing Arrangement and any associated Operational Arrangement(s) reflects this understanding.

2. Scope of the Information Sharing Protocol (ISP)

2.1. General

This Protocol lays the foundation for the secure and confidential sharing of agreed appropriate **aggregated, depersonalised and personal identifiable information** *(see page 5)* within and across organisational/authority boundaries.

It is a statement of the principles and assurances which govern that activity and provides that the rights of all the parties (organisations, managers, practitioners and service users) are upheld in a fair and proportionate manner by ensuring clarity and consistency of practice in accordance with:

- The duties and powers (express or implied) arising from relevant legislation incumbent upon statutory bodies or their sub-contractors
- The Data Protection Act 1998
- The Human Rights Act 1998
- The Freedom of Information Act 2000
- The Caldicott Principles *(See Appendix 4)*
- Common Law duties (e.g. Confidentiality) *(See Appendix 5)*
- Any other relevant statutory and non-statutory regulations and/or guidance

It is designed to support and supplement the requirements arising from existing legislation and guidance as outlined at *Section 2.1* and referenced throughout this document and the other elements of the Toolkit; it does not replace or supplant them.

However, in order to achieve a 'common standard' across signatory organisations via the implementation of this Toolkit it is recommended that they migrate and convert any other existing Information Sharing Protocols/Arrangements etc at the point they are due for renewal.

The Toolkit will also complement and support a number of key national projects and initiatives relating to information sharing, most notably:

- **Public Sector Data Sharing: Guidance on the Law**;
  see www.justice.gov.uk

- **Information Governance for the Department of Health**;
  in particular the Health and Social Care environments, see www.dh.gov.uk

- **FAME Readiness Assessment Tool and FAME Generic Framework Guidance**; these push partnerships to look at their intentions, their policy drivers, legal powers, information sharing and governance and provide a process within which practitioners, ICT and governance/managers can communicate with each other and learn about the issues underlying the partnership and form an action plan. Beyond that, there is a need to recognise that no issue is on its own. The notion of joined up services has few real boundaries, those that exist, exist because of perceptions, see www.fame-uk.org

2.2. Statutory Sector Bodies

This document is intended to operate across all organisations operating in the statutory sector including, but not restricted to: Criminal Justice, Health, Local Authorities, (Other) Education/Learning/Training Providers, etc ***and*** those organisations operating in the private & voluntary sector where they are undertaking a statutory function.

All organisations operating within a statutory framework must show that they have the necessary legal basis (express or implied powers) to process and disclose personal (service user) information. These can be derived from the specific legislative requirements to provide services that by their very nature necessitate the sharing of information if they are to be delivered effectively. *(See Section 1.2)*

In this context statutory sector bodies, and those carrying out statutory functions on their behalf, should first consider what statutory powers or duties they may be subject to, in relation to sharing personal information, and also should consider the issue of service user consent. However, sharing of information must still be in accordance with their (service user) statutory rights and legitimate expectations *(See Sections 4.9 & 4.10)*

Where a statutory body is bound by particular legislation, regulation or guidance in respect of service user consent then this must be adhered to. *(See Section 6)*

2.3. Private and Voluntary Sector Bodies

Organisations within the private and voluntary sectors who ***are not*** undertaking statutory functions may still wish to adopt the Toolkit and become signatories to the Information Sharing Protocol (ISP) if it is felt to be of benefit/necessity. This approach is especially recommended where these bodies are working with statutory sector bodies to provide effective support to service users.

In this context these private and voluntary sector bodies ***must*** have the service users prior consent (explicit if sharing sensitive information) before sharing personal information with other service providers unless this can be overridden due to an exemption as laid out in the Data Protection Act 1998

2.4. Age

This Information Sharing Protocol (ISP) will apply to people of all ages who are, or have been, service-users of the organisations that are signatories to this document and whose information is the subject of any sharing arrangements between those organisations. Age specific requirements will be addressed within the appropriate Information Sharing Arrangement(s) (ISA) and any Operational Arrangement(s) (OA).

2.5. Information Sharing Arrangement (ISA)

This Information Sharing Protocol (ISP) **will** be supplemented by appropriate 'Information Sharing Arrangement(s)' wherever there is a requirement for the processing and/or sharing of personal information within and between a two or more signatory organisations for a common purpose or purposes; e.g. Children's Trust, Crime & Disorder Reduction Partnership, Common Assessment Process, etc.

The Information Sharing Arrangement (ISA) **will:** detail the organisations who are party to it and the group(s) of service users it impacts upon; define the specific purpose(s) for information sharing and the relevant legislative powers; clarify the types of data to be shared; identify any common policies and standards that will apply across the Community including the process for review.

Each Information Sharing Arrangement ***may*** in turn be supplemented by appropriate Operational Arrangement(s) (OA) or equivalent documentation that will specify the relevant business processes which support information processing/sharing between two or more organisations for a specified purpose; e.g. Information Sharing Index, Common Assessment Framework (CAF), ASBO Working Group, Single Assessment Process (SAP), Contact Point etc

2.6 Other Arrangements/Contracts

Wherever it is a requirement to disclose personal identifiable information between organisations as part of a formal funding/contractual arrangement then all parties must be made aware of this as part of the funding/contractual process and not subsequent to the grant/contract being completed.

It is recommended that the Information Sharing Toolkit and any associated Information Sharing Arrangements/Operational Arrangements etc are included as annexes to any such contracts.

3. Parties to the Information Sharing Toolkit & Indemnity

The parties to this Information Sharing Toolkit are those that have signed the Declaration of Acceptance and Participation (DAP) at the end of this document.

A list, along with the details of each organisation's 'Designated Person(s)' as shown on the 'DAP', will be held and regularly updated on the Greater Merseyside Connexions Partnership website www.connexionslive.com

It is important to ensure accountability in the case of a complaint relating to the improper use of personal information supplied as a consequence of an 'Information Sharing Arrangement' and any associated 'Operational Arrangements'

Therefore, each 'Information Sharing Arrangement' will include appropriate arrangements between the signatory organisations which will indemnify those organisations for any action taken against them as a result of unauthorised or inappropriate use of information by one of the other parties to the 'Arrangement' or any associated 'Operational Arrangements'.

Any purported breaches of, or other complaints about, this Toolkit as per 3.2 above will be dealt with in accordance with the processes described at Section 5 of the appropriate Information Sharing Arrangement.

Nothing in this Arrangement confers or purports to confer any third party any benefit or any right to enforce any term of this Arrangement.

4. Requirements

4.1 General

This section outlines the principal requirements that each signatory organisation must work towards. It has been designed to act as a primary checklist of actions and responsibilities which, if fully implemented and adhered to, should help to ensure that the organisation's treatment of their service user's information is compliant with current legislation and good practice.

4.2 Adoption & Approval

Formal adoption and approval of this Information Sharing Protocol and the other aspects of the Toolkit (including any associated Information Sharing Arrangements and/or Operational Arrangement(s)) are the responsibility of each organisation and/or department. A central repository of documentation will be established and held by the MAIGG, and a designated host organisation. (At this time Greater Merseyside Connexions Partnership)

Each signatory organisation agrees to support the adoption, dissemination, implementation, monitoring and review of this Information Sharing Protocol (ISP) and the other associated documents comprising the Information Sharing Toolkit as described at *Section 1.1* in accordance with their own internal, and any other jointly agreed and authorised, information governance standard and/or operational policies and procedures. To facilitate this each organisation must identify a 'Designated Person' (to be detailed on the 'DAP') who shall have this responsibility. (See Section 4.4)

4.3 Information Governance

Each organisation shall have in place appropriate internal information governance and/or operational policies and procedures that will facilitate the effective processing of personal information which is relevant to the needs of the organisation, their managers/practitioners and their service users.

Where the Information Sharing Toolkit operates jointly across a number of organisations then a 'Multi-Agency Information Governance Group' shall be established within an agreed timeframe to undertake the responsibility of monitoring and reviewing its effectiveness across those agencies as well as facilitating and managing any alterations required of the Toolkit as a result of changes to law, guidance, ethics or practice.

Such changes would be subject to the arrangement of all parties. (See Section 7)

Where organisations share pooled information then the information governance arrangements must be clearly stated within the appropriate Information Community Arrangement and/or the associated Operational Arrangements.

In the event of any dispute arising between one or more of the signatories in respect of the Toolkit and any of its associated documents/related processes then this must be addressed via the 'Multi-Agency Information Governance Group'. (See Sections 3 & 7)

4.4 Designated Person

Each organisation must nominate a 'Designated Person' (e.g. Caldicott Guardian, Data Protection Officer, Knowledge Officer, other relevant manager, etc. - to be detailed on the 'DAP' with responsibility for ensuring that their organisation complies with legal and other appropriate requirements, obligations and guidance in respect of information processing and sharing, including those outlined in this and other related documents and arrangements; **(Caldicott Principle 6** (See Appendix 4)).

In addition it is recommended that the 'Designated Person' should also be responsible for:

- Internal information governance and/or operational procedures and processes (See Section 4.3).
- The dissemination and implementation of, and monitoring and evaluating adherence to, the Information Sharing Toolkit and related guidance within their organisation.
- Facilitating the training, advice and ongoing support to all relevant staff in respect of the Toolkit and associated guidance (See Section 4.16).
- Dealing with any concerns/complaints that have been raised by service users or practitioners and any other instances of non-compliance, internal or by partners, in accordance with agreed procedures (See Sections 3 & 7).
- Ensuring that the views and rights of service users are respected and acted upon including, but not restricted to: confidentiality, subject access requests, disclosure of personal identifiable information without consent, etc. (See Section 4.10).
- Deciding upon requests to disclose information, even where the service user has consented, to an organisation that is not a signatory to this, or other appropriate, arrangement.
- Liaising with the other signatory organisations and be a member of the relevant 'Multi-Agency Information Governance Group', if established. (See Section 4.2 & 4.3).
- Receiving requests for change to any aspect of the Toolkit, circulating them for a response, obtaining arrangement for the changes, working with the relevant 'Multi-Agency Information Governance Group' and then reissuing amended documents where necessary. (See Section 4.2 & 4.3).
- Ensuring that the list of signatories and other 'Designated Persons' as shown on the 'DAP' are kept up-to-date and appropriately circulated (See Section 3).

4.5 Staff Requirements

The conditions, obligations and requirements set out in the Information Sharing Protocol and associated Information Sharing Arrangement(s) and Operational Arrangement(s) will apply to all appropriate staff, agency workers, and volunteers working within those organisations.

All organisations are strongly advised to ensure that staff have entered into appropriate confidentiality arrangements that detail the possible consequences of unauthorised or inappropriate disclosure of service user information. This may be incorporated into staff contracts if deemed necessary. (See Section 7.1 & 7.2)

Each organisation must ensure that all appropriate staff have the necessary level of CRB clearance in accordance with relevant legislation and Government guidance.

4.6 Circulation/Dissemination

This Information Sharing Protocol (ISP), and other associated documents that comprise the Information Sharing Toolkit, shall be freely available to any representative of any signatory organisation via the most appropriate communications channels.

This Information Sharing Protocol (ISP), and other completed documents that comprise the Information Sharing Toolkit, shall be readily available to all relevant staff via the most appropriate communication channels.

This Information Sharing Protocol (ISP), and other completed documents that comprise the Information Sharing Toolkit, shall be readily available to service users and, wherever possible, to the general public via the most appropriate communication channels.

The means by which the documents will be circulated and disseminated must be described in the relevant Information Sharing Arrangement.

4.7 Principal Values Applicable to Information Sharing

Each organisation agrees to comply with these values when sharing and processing service user information:

Day-to-day operations are conducted in such a manner that **personal identifiable information** is used in a manner that is fair and lawful **and** that places the service user at the centre of that process - **DPA 98 Schedule 1 – *1st & 6th Principles*** (See Appendix 2).

That every proposal to share personal identifiable information between organisations must have a defined and justifiable purpose **and** the information subsequently obtained shall not be used in a manner that is incompatible with that or other agreed purposes - **DPA 98 Schedule 1 – *2nd Principle*** (See Appendix 2) and **Caldicott Principle 1** (See Appendix 4). This will be supported by the development and implementation of an appropriate Information Community Arrangement(s) and associated Operational Arrangement(s).

That every request for disclosure, whether actioned or not, must be fully recorded and clearly referenced to the evidence and information on which the decision to share/not share was based.

That where the sharing of personal identifiable information cannot be justified then it may be permissible to share depersonalised aggregated data, i.e. for research/analytical purposes. However this must still be described and agreed in the appropriate ICA and/or Operational Arrangement **- Caldicott Principle 2** (See Appendix 4)**.**

That any shared personal identifiable information must be the minimum information required for the stated purpose; i.e. adequate, relevant and not excessive; and be kept accurate and up to date **- DPA 98 Schedule 1 – *3rd & 4th Principles*** (See Appendix 2) and **Caldicott Principle 3** (See Appendix 2)**)**.

That shared personal identifiable information shall not be kept for longer than is necessary in accordance with the agreed purpose(s) **DPA 98 Schedule 1 – *5th Principle*** (See Appendix 2)**.**

That access to personal identifiable information will be restricted to a “need to know” basis **Caldicott Principle 4** (See Appendix 4)

That those accessing personal identifiable information will be made aware of their responsibilities in relation to its handling **- Caldicott Principle 5** (See Appendix 4)

4.8 Deceased Persons:

Even though the Data Protection Act 1998 does not apply to those who are deceased there may still be issues about confidentiality, access to records (by relatives or other parties) and the retention of records. Therefore, careful consideration must be given to the disclosure of 'personal information' relating to a deceased person and, if necessary, appropriate managerial/specialist advice must be sought. These arrangements must be reflected within the relevant Information Community Arrangement and/or Operational Arrangement.

The Data Protection Act relates to living individuals. As a result, the Act does not oblige an organisation to supply anyone with such information. However, there may be a right to access a deceased person's data through the "Access to Health Records Act". Department of Health website for further information or It may be appropriate to request such information through the Freedom of Information Act.

4.9 Compliance with the Data Protection Act 1998

(Notification, Rights of Individuals, Principles of Good Practice and Schedules 2 & 3 Conditions)

Each organisation must have an appropriate entry (Notification) in the 'Register of Data Controllers' managed by the Information Commissioners Office (ICO). This will be evidenced by your 'Registration Number' and 'Renewal Date' on the 'DAP'.

Each organisation must respect the seven rights given to individuals in respect of their own personal data *(See Appendix 6)*

In Addition:

Each organisation must adhere to the eight enforceable principles in respect of the processing of Personal Information. *(See Appendix 2)*

and

In order to process any personal information *(See Section 1.3)* each organisation must ensure that at least one condition from Schedule 2 is met. *(See Appendix 3)*

and

In order to process any sensitive personal information *(See Section 1.3)* each organisation must ensure that at least one condition from Schedule 2 is met **and** at least one condition from Schedule 3 is also met *(See Appendix 3)*. In addition, a common law duty of confidentiality may apply in these circumstances and should be considered in conjunction with this requirement *(See Section 5)*

and

That all personal identifiable information must be held in a safe and secure environment, including the means by which it is transmitted or received between partner organisations; **and**, in so far as it is reasonably practicable, be free from: unauthorised or unlawful access or interception, accidental loss or destruction or damage - **DPA 98 Schedule 1 – *7th Principle*** *(See Appendix 2).*

4.10 Service User Awareness & Rights

Each organisation has a duty to ensure that all service users are aware of the information that is being collected and recorded about them, the reasons for doing so (including any statistical/analytical purposes), with whom it may be shared and why. This can be achieved by the issuing of a ***Fair Processing Notice or Privacy Notice***

Each organisation has a duty to ensure that all service users are aware of their rights in respect of information processing/sharing, including any limits and/or restrictions, in respect of the Data Protection Act 1998, the Human Rights Act 1998, *the Common Law Duty of Confidentiality* and, where appropriate, the Freedom of Information Act 2000 and how these may be exercised.

This will include providing appropriate support in order that service-users may best exercise those rights; e.g. providing service users with information in alternative formats or languages or assisting them with a ***Subject Access Request***

All service users have a right to expect that information disclosed by them or by other parties about them to an organisation will be treated with the appropriate degree of respect and confidence. This is covered by a ***Common Law Duty of Confidentiality***. *(See Appendix 5)*.

However this right is not absolute and may be overridden in certain circumstances. *(See Appendix 5)*.

In addition, all service users must be made aware under what circumstances their consent will be required, and the procedure by which it will be sought, in order to obtain and share their personal information. *(See Section 6)*

Each organisation must ensure that they have appropriate policies and procedures in place to facilitate the exercising of these, and other, right(s) and will apply these rights in a fair and consistent manner and in accordance with any specific legislative requirements, regulations or guidance

4.11 Quality & Accuracy of Personal (Service User) Data

Each organisation is responsible for the quality and accuracy of the personal data it obtains, records, holds, uses and shares.

Thus:

All practitioner interventions, and their outcomes, with service users must be properly recorded within the organisation's case management systems;

and

When recording information, in whatever format (e.g. electronic or hard copy), then each piece of information must contain:

the date created or recorded, the identity of the source of the information and whether it comprises fact, opinion, hearsay or a mixture of these together with the identity of the person(s) receiving and recording the information (in many instances this may be one and the same); except where this (information) is self-evident, e.g. a health professional making a note in the medical records.

It is likely that the majority of electronic case management systems will hold these various elements as part of an individual record

If a practitioner discovers that information they hold is inaccurate then they must ensure that their case management system is updated accordingly and should advise all other interested parties that they know has received or holds that information.

Wherever desirable and practicable partner organisations are encouraged to adopt a standard format for data exchange in order to establish and maintain a consistent approach to the way that information is collected, stored and shared.

4.12 Use of Personal (Service User) Data for Evaluation & Research Purposes

Each organisation **may use** personal data for the purpose of evaluation and research, including the use of agents acting on your behalf, provided that it is contained within your notification to the Information Commissioner's Office and service users have been made aware of this purpose.

If the service users 'implied consent' is being relied upon for this purpose then each organisation must ensure that they comply with the 'fair & lawful processing' principle as defined by the Data Protection Act 1998.

Where a change of use has taken place regarding the further use of personal data then further consent must be sought from the service user.

4.13 Use of Personal (Service User) Data for Marketing/Commercial Purposes

Each organisation **may not** use personal data shared between organisations as a result of this Information Sharing Protocol (ISP) or any associated Information Community Arrangement and/or Operational Arrangement for the purpose of any marketing and/or commercial activities ***unless*** it is contained within your notification to the Information Commissioner's Office, service users have been made aware of this purpose and that appropriate consent has been obtained from each service user to use their information for this particular purpose.

If the service users 'implied consent' is being relied upon for this purpose then each organisation must ensure that they comply with the 'fair & lawful processing' principle as defined by the Data Protection Act 1998.

Where a change of use has taken place regarding the further use of personal data then further consent must be sought from the service user.

4.14 Data Retention

Each organisation or department must have a data retention policy that accords to the legitimate purposes of that organisation, details of which must be included in the appropriate Information Community Arrangement(s)/Operational Arrangement(s).

The policy document will make clear the organisations/departmental approach to the retention, storage and disposal of records, only keeping information for as long as is necessary in relation to the original purpose(s) for which it was collected

4.15 Data Access & Security

Each organisation must ensure that appropriate technical and organisational measures are in place that protect against unauthorised or unlawful processing of personal information and against accidental loss or destruction of, or damage to, personal information.

Thus:

Each organisation must have in place a level of security commensurate with the sensitivity and classification of the information to be stored and/or shared, including information transferred to/received from other organisations.

Each organisation must ensure that mechanisms are in place to address the issues of: physical security, security awareness and training, security management, systems development, role based security/practitioner access levels, data transfer and receiving and system specific security policies. Ideally the standard applied *should be* ISO17799.

Wherever 'Common Protective Markings' are used (e.g. Unrestricted, Confidential, Restricted, Secret, Top Secret) then each party organisation should agree the common meaning of these terms and the associated procedures in order to ensure that that the transmission/receipt and storage of information thus marked is appropriate to the level of security required.

Evidence must be in the form of a local Strategy/Information Security Policy and reference as to how these issues will be addressed must be made in the appropriate Information Community Arrangement(s)/Operational Arrangement(s).

4.16 Staff Awareness & Training

Each organisation has a responsibility to ensure that all relevant staff receive training, advice and ongoing support in order to be made aware, and understand the implications, of:

- This Information Sharing Protocol (ISP) and any other associated documents (e.g. Partnership Arrangement, the ISA, the 'Operational Arrangement', etc). This is to include any associated operational requirements arising from the implementation of these.
- The underpinning and organisation specific legislation and associated regulations/guidance in respect of information sharing and any express or implied powers arising therefrom
- Common Law duties (e.g. Confidentiality) *(See Section 5 & Appendix 5)*.
- Appropriate Codes of Practice and other associated regulations/guidance (e.g. NHS Confidentiality Code of Practice).

5. Confidentiality

Confidential information is information of some sensitivity, which is not already in the public domain or readily available from another public source and which has been shared in a relationship where the service user giving it understood that it would not be shared with others without their express consent. This is covered by the *Common Law Duty of Confidentiality*. In some cases there may also be a statutory obligation to maintain confidentiality; e.g. in relation to the case files of looked after children.

All staff will be sensitive to the need for inter-agency confidentiality when discussing service users with other organisations or departments. The relationship between organisations, practitioners and service user must be based on the assumption that their relationship is for the benefit of the service user.

All staff will need to be guided by their organisation's policies and procedures on information sharing, any relevant Information Community Arrangements/Operational Arrangements and, where applicable, to their professional codes of conduct and/or practice in this respect.

However, all staff will need to bear in mind that the duty of confidentiality is not absolute. Even where staff are not compelled by law to disclose information there may be circumstances where it is appropriate to do so, in the absence of service users consent, having weighed up the public interests at stake. The key test is that of proportionality; i.e. whether the proposed sharing is a proportionate response to the need to protect the public interest in question. *(See Section 6)*

6. Consent

As stated throughout this document the service user should be at the centre of what happens to their information. Therefore, as part of this, organisations and their practitioners should proactively inform service users, **when they first engage with the service**, as to the circumstances by which their information may be gathered, recorded and shared. *(See Section 4.10)*

As previously stated at *Sections 1.2 & 2.2* for **statutory sector bodies**, and those carrying out statutory functions on their behalf, this must be within a suitable legal context; i.e. a body must have the appropriate express or implied duties, functions or powers to gather, record and share personal (service user) information.

The approach to securing consent to share information must be transparent and respect the individual giving it. Consent should, if appropriate, be obtained at the first engagement.

It must be 'informed' (i.e. the service user knows what is happening and why) and either 'explicit' (preferably written) or 'implicit' (e.g. continuous medical support, a referral from one organisation to another).

Organisations and their staff need to be aware that there may be circumstances where it is not practicable or desirable to obtain consent to share information because to do so would, for example; place a person at serious risk of harm, prejudice the prevention or detection of a serious crime or there is a statutory duty or court order in place.

Where consent is sought but not given, information can still be disclosed where the individuals right to privacy is outweighed by an overriding public interest in disclosure or where the personal safety of any individual is at unacceptable risk.

This approach does not remove the service user's right to withhold or withdraw their consent but they must be made aware of the possible consequences of such a decision and that there are certain circumstances where even this may be overridden

As previously stated at *Section 2.3* private and voluntary sector bodies who are not undertaking statutory functions ***must*** have their service user's prior consent to share information unless this can be overridden.

The appropriate Information Sharing Arrangement(s) and Operational Arrangement(s) must clearly state the approach to be used by each of the parties in this respect.

7. Monitor & Review

7.1 Non-Compliance (Internal)

Instances of internal non-compliance with this Toolkit and associated documents and procedures will be logged and reported to the appropriate 'Designated Person' *(See Section 4.2)*.

They should be dealt with promptly in accordance with the agreed information governance/operational policies and procedures. These should be described in the appropriate Information Sharing Arrangement in Section 5

Incidents that should be logged and reported include, but are not restricted to:

- Inappropriate refusal to disclose information
- Conditions being placed on disclosure
- Inappropriate, unauthorised or unlawful disclosure
- Disregard of the agreed policies and procedures
- Disregard of the views and rights of service users

7.2 Non-Compliance (Partner Organisations)

Instances of non–compliance with this Toolkit and associated documents and procedures by a partner organisation will be reported to that organisation's 'Designated Person' and, if established, the appropriate 'Multi-Agency Information Governance Group' (MAIGG) *(See Section 4.2)*. They should be dealt with promptly in accordance with the agreed information governance/operational policies and procedures. These should be described in the appropriate Information Sharing Arrangement in Section 5

Examples of the incidents to be reported are as those detailed above.

In addition each organisation will also inform such regulatory bodies as need to know, or they are required to inform, of any breaches; this should be the responsibility of the 'Designated Person' or MAIGG. *(See Section 4.2).* These should be described in the appropriate Information Sharing Arrangement Section 5

7.3 Service User/Practitioner Concerns

Any concerns or complaints received from service users relating to the processing/sharing of their personal information should be dealt with promptly in accordance with the internal complaints procedure of that organisation and, where appropriate, the conditions outlined at *Sections 7.1 & 7.2* and in the appropriate Information Sharing Arrangement Section 5.

Any concerns/complaints received from practitioners relating to the operation of this Toolkit will be referred to their organisation's 'Designated Person' who will respond in accordance with the internal policies and procedures of that organisation and the conditions outlined at *Sections 7.1 & 7.2* and in the appropriate Information Sharing Arrangement Section 5.

7.4 Formal Review

These arrangements notwithstanding the Toolkit and the associated procedures and systems for the sharing of data will be subject to on-going review and, at a minimum, a formal review by all parties on a biannual basis *(See Section 8)*.

New DAP's will only be required should there be a major change to the protocol or if the main signatory or designated persons details should change.

8. Effective Date

This Information Sharing Protocol (ISP) is effective from an agreed common implementation of **1st January 2010**. This document will remain in effect until superseded or formally replaced.

The document will be reviewed on agreed timescales no longer than a biannual basis.

Should any major changes in legislation or Good Practice Guidelines occur all "Designated Persons" will be notified by email of the change and that a new DAP is required

Should the main signatory to the DAP no longer remain the principal person, (i.e. the organisation has a new Chief Executive Officer), a new DAP will be required to ensure that they are aware of the Information Protocol and agree to its use.

Information Sharing Protocol

DECLARATION OF ACCEPTANCE & PARTICIPATION

I, the undersigned, on behalf of the organisation named below, agree to support the implementation of this Protocol and associated Information Sharing Arrangement in accordance with the conditions detailed in this document

I also understand that my organisation may share relevant data with other Partner Organisations who are signatories to this Protocol and with whom a separate Information Sharing Arrangement is in place.

I declare that we have given notification to the Office of the Information Commissioner and that the said notification is up-to-date and it reveals our current use and storage of data and compliance with the Data Protection Act 1998.

Organisations Registration Number: _____ Annual Renewal Date ____/_____
Day Month

Main Signatory/Principal Person

Name: Position:

Organisation:

Address:

Tel No:

Signature: _____ Date:

DESIGNATED LIAISON OFFICER

The person named below is the nominated contact for this organisation in respect of any enquiries relating to this Protocol. These details will be distributed to all other Partner Organisations who are signatories to this Protocol

Name: Position:

Address:

Tel No: Fax No:

e-mail:

or: