APPENDIX 1

Information Sharing Toolkit *Tier 1*

Framework Document

(Name of Agency:.....)

(*Insert Internal Reference No*)

Effective From: To:

Operational Version 1.0: 01/03/05

INDEX

Definitions/Glossary of words/phrases are referenced in 'Red' (See Appendix 1)
Common abbreviation of words are referenced in 'Blue'
Cross-References & Appendices are referenced in 'Teal'

Change History

Version	Amended by	Amended Date	Main Changes
1.0	01/03/05	JPC	Operational version released

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 (and colleagues working within/with them – you know who you are):

- ***Greater Merseyside Connexions Partnership***
- ***Knowsley ISAP Information Sharing Sub-Group***
- ***Knowsley ISAP Cluster Group***
- ***Various Other Local Authority ISAP Trailblazer & Non-Trailblazer Groups***
- ***Cheshire & Merseyside Strategic Health Authority Information Governance Group***
- ***North Mersey LIS Team***
- ***Merseyside Police (Joint Agency Group)***
- ***Metropolitan Police***
- ***DfES-ISA Information Sharing Reference Group***
- ***Department for Constitutional Affairs – Information Rights Division***
- ***Information Commissioner's Office***

Apologies if anyone has been omitted.

Author:
Joe Colleran
Greater Merseyside Connexions Partnership & Knowsley MBC ISA Programme

Tel (Mobile): 07736 476 957

E-mail: joe.colleran@connexions-gmerseyside.co.uk & joe.colleran@knowsley.gov.uk

1. Introduction

1.1 General

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

1.1.2 This Framework Document is the first (Tier 1) element of the Toolkit. It sets out the rules, values and principles for information sharing between organisations irrespective of the purpose. It is aimed at an organisations 'strategic' level.

1.1.3 The other elements of the Toolkit are as follows:

- **Tier 2: Information Sharing Arrangement (ISA)** – The 'who/why/where/when/what/how' questions. It is aimed an organisations 'tactical/middle management' level.
- **Tier 3: Operational Instruction** – A means of communicating to practitioners the specific operational requirements arising from an ISA. It is aimed at an organisations 'operational/practitioner' level.
- **Tier 4: Privacy, Confidentiality & Consent** – This will cover the range of processes and documentation that will directly impact on service users and could include things such as 'Privacy/Confidentiality Statement', 'Fair Processing Notice', 'Consent', 'Subject Access', etc. It is aimed at an organisations 'service user' level.
- **The Appendices** – This is intended to be the principal reference guide and supports the application of Tiers 1 to 4 of the Toolkit.

1.2 Background

1.2.1. **Partner Organisations/Agencies (Organisation(s))** supplying services to service users who are resident, or accessing services, within ***[Define Area]*** 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 organisation could become involved with a service user(s) but they are unaware of each others involvement.

12.2 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 respon 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.

1.2.3 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.

1.2.4 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.

1.2.5 ***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

1.3.1 There are three broad categories of information relating to service users that organisations may wish to 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 ambit of the Data Protection Act 1998.

- **Depersonalised/Anonymised 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 ambit of the Data Protection Act 1998.

- **Personal Identifiable Information (non-sensitive & sensitive)**
  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'*** and these are:

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

1.3.2. 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 Appendix 2.3)*** 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 Appendices 2.3 & 2.4)***.

1.3.3. There may also be 'Personal Identifiable Information' outside of that defined as 'sensitive' by the Data Protection Act 1998 ***(See Section 1.3.1 above)*** but has been identified by the signatory organisations as being of a personal and sensitive nature. Examples of this include client characteristics (substance misuse, homeless, refugee, truant, etc), opinions or assessment data.

In respect of this 'Professionally Sensitive Information' it is recommended that signatory organisations treat this in the same manner as Sensitive Information and that the agreed (Tier 2) Information Sharing Arrangement reflects this understanding.

2. Scope of the Framework

2.1. General

2.1.1 This 'Framework Document' lays the foundation for the secure and confidential sharing of agreed appropriate **aggregated, depersonalised and personal identifiable information** within and across organisational/authority boundaries.

2.1.2 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 encumbent upon statutory bodies or their sub-contractors ***(See Appendices 5 to 7)***
- The Data Protection Act 1998 ***(See Appendices 2.1 to 2.4 and referenced throughout this document)***
- The Human Rights Act 1998 ***(See Appendix 3)***
- The Freedom of Information Act 2000 ***(See Appendix 4)***
- Common Law duties (e.g. Confidentiality) ***(See Section 5 & Appendix 10.3)***
- The Caldicott Principles ***(See Appendix 8 and referenced throughout this document)***
- Any other relevant statutory and non-statutory regulations and/or guidance ***(See Appendices 5 to 7 and 9 & 10); e.g. NHS Confidentiality Code of Practice***

2.1.3 It is designed to support and supplement the requirements arising from existing legislation and guidance as outlined at ***Section 2.1.2*** above and referenced throughout this document and the other elements of the Toolkit; it does not replace or supplant them.

2.1.4 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.

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

- The Information Governance Toolkit (HORUS) developed for the Health and Social Care environments and now to be adopted by Local Government; see www.legsb.gov.uk
- FAME (FrAmework for Multi-agency Environments); see www.fame.org.uk
- RYOGENS (Reducing Youth Offending Generic National System); see www.ryogens.org.uk

2.2. Statutory Sector Bodies

2.2.1 This Framework 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.

2.2.2 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 1.2.5 and Appendices 5 to 7)***

2.2.3 In this context statutory sector bodies, and those carrying out statutory functions on their behalf, should first look for any express or implied powers to share personal (service user) information rather than relying solely upon the service users consent. However this must still be in accordance with their (service user) statutory rights and legitimate expectations ***(See Sections 4.5 & 6)***

2.2.4 However, where a statutory body is bound by their particular legislation, regulation or guidance in respect of service user consent then these must also be adhered to. ***(See Section 6 and Appendices 5 to 7, 10.2 & 10.3)***

2.3. Private and Voluntary Sector Bodies

2.3.1 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 Framework if it is felt to be of benefit/necessity.

2.3.2 This approach is especially recommended where these bodies are working with statutory sector bodies to provide effective support to service users.

2.3.3 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 ***(See Section 6 and Appendix 10.2)*** unless this can be overridden as outlined at ***Appendix 10.3***

2.4. Age

2.4.1 This Framework 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.

2.4.2 Age specific requirements will be addressed within the appropriate **Information Sharing Arrangement(s) (ISA)/Operational Instruction(s).**

2.5. Information Sharing Arrangement (Tier 2)

2.5.1 This Framework **will** be supplemented by individual service/sector specific operational 'Information Sharing Arrangement(s)' wherever there is a requirement for the disclosure and/or sharing of personal information between two or more signatory organisations.

2.5.2 The Information Sharing Arrangement details the specific purpose(s) for information sharing, the group(s) of service users it impacts upon, the relevant legislative powers, what data is to be shared, the consent processes involved (where appropriate), the required operational procedures and the process for review.

2.6. Other Agreements/Contracts

2.6.1 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.

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

3. Parties to the Framework & Indemnity

3.1. The parties to this Information Sharing Framework are those that have signed the **Declaration of Acceptance and Participation (DAP)** at the end of this document ***(See this Document Schedule 1)***. This list, along with the details of each organisation's **'Designated Person(s)'** as shown on the 'DAP', **(*See Section 4.2.3 & appropriate ISA*)**, will be updated and reissued on a regular basis.

3.2. All parties undertake to indemnify each other against all losses, costs, expenses, damages, liabilities, demands, claims, actions or proceedings arising out of failure to apply any of the statements or procedures set out in this Arrangement or associated documents or out of the use of information provided as a result of this Arrangement and the associated Operational Instruction ***unless*** the damage can be shown to arise as result of the original disclosure in which case the originating organisation must bear the consequences.

4. Requirements

4.1 General

4.1.1 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 Management Procedures

4.2.1 Adoption & Approval

4.2.1.1 Formal adoption and approval of this Framework and the other aspects of the Toolkit (including any associated Information Sharing Arrangements/Operational Instruction(s)) is the responsibility of the Chief Officers/Boards and Senior Managers of each organisation or department and, if appropriate, the Caldicott Guardian or equivalent.

4.2.1.2 Each signatory organisation agrees to support the adoption, dissemination, implementation, monitoring and review of this Framework 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 should identify a 'Designated Person' (to be detailed on the 'DAP') who shall have this responsibility. **(See Section 4.2.3)**

4.2.2 Information Governance

4.2.2.1 Each organisation should 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.

4.2.2.2 Where the Information Sharing Toolkit operates jointly across a number of organisations then a 'Multi-Agency Information Governance Group' should be established 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 agreement of all parties. **(See Section 7)**

4.2.3 Designated Person

4.2.3.1 Each organisation should identify 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 agreements; **(Caldicott Principle 6).**

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

- Internal information governance and/or operational procedures and processes **(See Section 4.2.2).**
- 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 4.11).**
- 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 Section 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 4.5).***
- 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 4.2.2.2).***
- Receiving requests for change to any aspect of the Toolkit, circulating them for a response, obtaining agreement for the changes, working with the relevant 'Multi-Agency Information Governance Group' and then reissuing amended documents where necessary. ***(See Section 4.2.2.2).***
- 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).**

4.2.4 Staff Requirements

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

4.2.4.2 Staff contracts must contain appropriate confidentiality clauses that detail the possible consequences of unauthorised or inappropriate disclosure of service user information. ***(See Section 7.1 & 7.2)***

4.2.4.3 Each organisation must ensure that all appropriate staff has the necessary level of CRB clearance.

4.2.5 Dissemination/Circulation

4.2.5.1 The Framework, 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.

4.2.5.2 The Framework, and other completed documents that comprise the Information Sharing Toolkit, shall be readily available to all relevant staff via the most appropriate communication channels.

4.2.5.3 The Framework, 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.

4.3 Principal Values Applicable to Information Sharing

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

4.3.1 That 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*)**

4.3.2 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*) (Caldicott Principle 1).**

4.3.3 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.

4.3.4 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 ISA **(Caldicott Principle 2).**

4.3.5 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 accurate and objective **(DPA 98 Schedule 1 – *3rd & 4th Principles*) (Caldicott Principle 3).**

4.3.6 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*).**

4.3.7 That access to personal identifiable information will be restricted to a "need to know" basis **(Caldicott Principle 4).**

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

4.3.9 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*).**

4.4 Compliance with the Data Protection Act 1998 – Notification, Rights of Individuals, Principles of Good Practice and Schedules 2 & 3 Conditions

4.4.1 Each organisation must have an appropriate entry **(Notification)** in the 'Register of Data Controllers' managed by the Information Commissioner **(IC).** This will be evidenced by your 'Registration Number' and 'Renewal Date' on the 'DAP'. It is the responsibility of each organisation to ensure that its entry is kept current, up-to-date and accurate.

4.4.2 Each organisation must respect the seven rights given to individuals in respect of their own personal data ***(See Section 4.4 and Appendix 2.1)*** **In Addition:**

4.4.3 Each organisation must adhere to the eight enforceable principles in respect of the processing of Personal Information. ***(See Appendix 2.2)*** **And:**

4.4.4 In order to process any personal information ***(See Section 1.3 and Appendix 10.1)*** each organisation must ensure that at least one condition from Schedule 2 is met. ***(See Appendix 2.3)*** **And**

4.4.5 In order to process any sensitive personal information ***(See Section 1.3 and Appendix 10.1)*** each organisation must ensure that at least one condition from **both** Schedule 2 and Schedule 3 are met. ***(See Appendices 2.3 & 2.4)***

4.5 Service User Awareness & Rights

4.5.1 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** ***(See Tier 4)*** and the DCA's **Citizens Charter** ***(See Appendix 9.1)***.

4.5.2 Each organisation has a duty to ensure that all service users are aware of their rights in respect of the Data Protection Act 1998 ***(See Appendices 2.1)***, the Human Rights Act 1998 ***(See Appendix 3)*** and, where appropriate, the Freedom of Information Act 2000 ***(See Appendix 4)*** 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** ***(See Appendix 10.4)***.

4.5.3 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*. However this right is not absolute and may be overridden in certain circumstances ***(See Section 5 & Appendix 10.3)***.

4.5.4 In addition, all service users must be made aware as to under what circumstances their consent will be needed and subsequently gained in order to obtain and share their personal information, the possible consequences of refusing or withdrawing that consent and the circumstances by which this may be overridden ***(See Section 6 & Appendices 10.2 & 10.3)***.

4.5.5 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 ***(See Appendices 2 to 4 and 9 & 10)***

4.6 Quality & Accuracy of Personal (Service User) Data

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

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

4.6.3 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).

4.6.4 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.

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

4.7.1 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 aware of this purpose.

4.7.2 If the service users 'implied consent' ***(See Appendices 10.2 (6) & (7))*** 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.

4.7.3 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.

4.8 Use of Personal (Service User) Data for Marketing and/or Commercial Purposes

4.8.1 Each organisation **may not** use personal data shared between organisations as a result of this Framework or any associated Information Sharing Arrangement for the purpose of any marketing and/or commercial activities ***unless*** it is contained within your notification to the Information Commissioner's Office and service users have been made aware of this purpose.

4.8.2 If the service users 'implied consent' ***(See Appendices 10.2 (6) & (7))*** 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.

4.8.3 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.

4.9 Data Retention

4.9.1 Each organisation 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 Sharing Arrangement(s)/Operational Instruction(s).

4.9.2 The policy document will make clear the organisations 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

4.10 Data Access & Security

4.10.1 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:**

4.10.2 Each organisation must have in place a level of security commensurate with the sensitivity and classification of the information to be stored and shared.

4.10.3 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.

6.9.4 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 Sharing Arrangement(s)/Operational Instruction(s).

4.11 Staff Awareness & Training

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

- This Framework and any other associated documents (e.g. **Partnership Agreement**, the ISA, the 'Operational Instruction', 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 ***(See Appendices 2 to 8)***.
- Common Law duties (e.g. Confidentiality) ***(See Section 5 & Appendix 10.3)***.
- Appropriate Codes of Practice and other associated regulations/guidance (e.g. NHS Confidentiality Code of Practice) ***(See Appendices 2 to 10)***.

5. Confidentiality and Professional Ethics

5.1 Confidentiality

5.1.1 There is a ***Common Law Duty of Confidentiality***. In practice this means information given or received in confidence for one purpose may not be used for a different purpose or passed to anyone else without the consent of the provider of the information.

5.1.2 All staff will be sensitive to the need for inter-agency confidentiality when discussing service users with other organisations. 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.

5.1.3 However, all staff need to bear in mind that this is not an absolute right and that they are still obliged to disclose information where the law says we must or there is an overriding public interest. ***(See Appendix 10.3)***

5.2 Professional Ethics

5.2.1 Whilst all staff will adhere, where applicable, to their ***professional codes of conduct and/or practice*** in respect of information given in confidence these must not become unnecessary barriers to effective information sharing and improved services to service users.

6. Consent

6.1 As stated throughout this document the service user should be at the centre of what happens to their information and, as part of this, to be fully aware as to the circumstances by which their information may be shared with, and obtained from, other organisations. ***(See Section 4.5)***

6.2 The ideal would be for organisations and their practitioners to seek the consent of the service user each time they plan to share. However, it has been recognised by a number of major bodies (e.g. DCA, ICO, etc) that 'consent' is not always, from an operational perspective, particularly easy to obtain and subsequently manage.

6.3 **Thus**, as previously stated at ***Sections 1.2.5, 2.2.2 & 2.2.3*** **statutory sector bodies**, and those carrying out statutory functions on their behalf, should first look for any express or implied duties or powers to share personal (service user) information and to then properly inform their service users of this.

6.4 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. These exemptions are outlined at ***Appendix 10.3***

6.5 As previously stated at ***Section 2.3.3*** **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 as outlined at ***Appendix 10.3***

6.6 However, where client consent is considered to be prerequisite then partner organisations will work in accordance with their existing guidance or, if this is not available, they will work towards implementing the processes outlined at ***Appendix 10.2.***

6.7 The appropriate Information Sharing Arrangement(s)/Operational Instruction(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)

7.1.1 Instances of internal non-compliance will be logged and reported to the appropriate 'Designated Person' *(See Sections 4.2.3)*. They should be dealt with promptly in accordance with the agreed information governance/operational policies and procedures.

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

- 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)

7.2.1 Instances of non–compliance by a partner organisation will be reported to that organisation's 'Designated Person' and, if established, the appropriate 'Multi-Agency Information Governance Group'. They should be dealt with promptly in accordance with the agreed information governance/operational policies and procedures. ***(See Section 4.2.2)***

7.2.2 The incidents to be reported are as those detailed at ***Section 7.1.2.***

7.2.3 In addition each organisation will also inform such regulatory bodies as need to know of any breaches.

7.3 Service User/Practitioner Concerns

7.3.1 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.***

7.3.2 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*** as appropriate.

7.4 Formal Review

7.4.1 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 an annual basis *(See Section 8)*.

8. Effective Date

8.1 This Framework is considered to be effective from *a) the date the organisation signed the 'DAP' or *b) an agreed common implementation of **[*Insert Date*]** (*delete as appropriate)

8.2 This Framework will cease to be current, and therefore in need of a formal review, on an agreed common review date of **[*Insert Date*]** *(ideally this should be no later than 12 months from the implementation date at 8.1)* **(See Section 7.4)**

8.3 Both dates should be entered onto the frontispiece of this document.

[1] See articles 12 and 13 of the Convention.

Information Sharing Framework

(Insert Title & Reference Number)

DECLARATION OF ACCEPTANCE & PARTICIPATION

Signed by, for and on behalf of: ***Page 1 of***

Organisation	
Name	
Position	
Contact Details; i.e. **- Phone No** **- E-mail**	
Signature	
Date	

Organisation Contact for Information Sharing	
Position	
Contact Details; i.e. **- Phone No** **- E-mail**	
(DPA98)Registration No & Date of Renewal	

Framework Document Continuation Sheet for Other Signatories

(Insert Title & Reference Number)

Signed by, for and on behalf of: ***Page of***

Organisation	
Name	
Position	
Contact Details; i.e. **- Phone No** **- E-mail**	
Signature	
Date	

Please insert, print and sign additional continuation sheets where there are more than 2 signatories

Information Sharing Framework

List of Partnership Organisations & their Signatory Person's

(Insert Reference Number)

PARTNERSHIP MEMBER	SIGNATORY PERSON & POSITION	CONTACT DETAILS Include Telephone Number & E-Mail Address

Please insert, complete and print additional sheets where required