TIER 1

INFORMATION SHARING AGREEMENT

Effective : 19th November 2012

Tier 1 Information Sharing Agreement

(Version 1.0 Effective From 19th November 2012)

1 Introduction

1.1 General

The Information Sharing Agreement has been developed to establish a comprehensive and consistent standard within and across organisations/authorities in respect of the treatment of person-identifiable information. It places service users at the centre of how their information is used and all signatory organisations will adopt and work towards implementing it.

This Information Sharing Agreement (ISA) 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 information.

The sharing of relevant and appropriate information on a need-to-know basis between partner organisations and agencies (hereafter referred to as partner organisations) and their staff is vital in ensuring that service users receive the seamless, high quality support they expect and the type and level of support most appropriate to their needs. As such, partner organisations need to have a high degree of confidence and trust in the organisations they share information with. This document sets out the standards expected to provide this assurance.

1.2 Information 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. This is generally outside the remit of the Data Protection Act 1998 (DPA 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 DPA 1998.

Person-Identifiable Information: information (name, address, unique identifiers, etc) relating to a living individual, including their image or voice, that enables them to be uniquely identified. This information is under the remit of the DPA 1998.

The DPA 1998 highlights sensitive data and defines these as:

- ethnicity,
- religious beliefs,
- criminal proceedings,
- physical or mental health,
- sexual life,
- political opinion, and
- trade union membership.

To process any person-identifiable information, at least one of the conditions from Schedule 2 of the DPA 1998 must be met and, if it is sensitive information then at least one of the conditions from Schedule 3 of the DPA 1998 must be met.

There may also be person-identifiable information outside that defined as sensitive data by the DPA 1998, but which has been identified by the signatory organisations as being of a personal and sensitive nature. This is known as professionally sensitive information, but is more often called confidential information. Examples of this include client characteristics (substance misuse, homelessness, refugee, truant, etc) and opinions or assessment information. It is recommended that signatory organisations treat confidential information in the same manner as sensitive data.

2 Scope

2.1 General

This ISA lays the foundation for secure and confidential sharing of agreed appropriate aggregated, depersonalised and person-identifiable information 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:-

- Data Protection Act 1998 (DPA 1998);
- Human Rights Act 1998;
- Freedom of Information Act 2000;
- Access to Health Records Act 1990;
- Caldicott Principles;
- Children Act 1989 and 2004;
- Crime and Disorder Act 1998;
- Criminal Justice and Police Act 2001;
- Data Protection (Processing of Sensitive Personal Data) Order 2000;
- Education Act 2002;
- Protection of Children Act 1999;
- Special Educational Needs and Disability Act 2011;
- Youth Justice and Criminal Evidence Act 1999;
- common-law duties (e.g. confidentiality);
  and
- any other relevant statutory and non-statutory regulations and/or guidance.

This a g r e e m e n t will also complement and support a number of key national projects relating to information sharing, most notably:

Public Sector Data Sharing:
http://www.justice.gov.uk/guidance/freedom-and-rights/data-sharing.htm

2.2 Statutory Sector Bodies

This document is intended to operate across all organisations in the statutory sector including, but not restricted to: criminal justice, health, local authorities, education/learning/training providers, and t h o s e o r g a n i s a t i o n s o p e r a t i n g i n t h e private and voluntary sectors 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 person-identifiable 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.

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 person-identifiable information, and also should consider the issue of service user consent. However, sharing of information must still be in accordance with the service users' statutory rights and legitimate expectations.

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 agreement and become signatories to the ISA 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 user's prior consent (explicit if sharing sensitive information) before sharing person-identifiable information with other service providers, unless this can be overridden due to an exemption as laid out in the DPA 1998.

2.4 Age

This ISA will apply to people of all ages who have accessed services and/or are employees of 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 (ISA) Tier 2.

2.5 Information Sharing Arrangement (ISA) (Tier 2)

This ISA will be supplemented by appropriate ISAs wherever there is a requirement for the processing and/or sharing of person-identifiable information within and between two or more signatory organisations for a common purpose or purposes (e.g. Children's Trust, Crime and Disorder Reduction Partnership, Common Assessment Process, etc).

The 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 information to be shared; and
- identify any common policies and standards that will apply across the community, including the process for review.

2.6 Other Arrangements/Contracts

Where it is a requirement to disclose person-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 ISAs are included as annexes to any such contracts.

3 Parties to the Information Sharing Agreement and Indemnity

It is important to ensure accountability in the case of a complaint relating to the improper use of person-identifiable information supplied as a consequence of an ISA. Therefore, each ISA 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 ISA. Any purported breaches of or other complaints

about this ISA will be dealt with in accordance with the relevant organisation's disciplinary policy.

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 users' information is compliant with current legislation and good practice.

4.2 Adoption and Approval

Formal adoption and approval of this ISA are the responsibility of each organisation. A central repository of documentation will be established and held by Halton Borough Council's Information Governance (IG) Team in ICT Services.

Each signatory organisation agrees to support the adoption, dissemination, implementation, monitoring and review of this ISA in accordance with their own internal, and any other jointly agreed and authorised, IG standards 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.

4.3 Information Governance (IG)

Each organisation shall have in place appropriate internal IG and/or operational policies and procedures that will facilitate the effective processing of person-identifiable information which is relevant to the needs of the organisation, their managers/practitioners and their service users. These should incorporate Caldicott Guardian principles.

In the event of any dispute arising between one or more of the signatories in respect of the ISA and any of its associated documents/related processes then this must be addressed via Halton Borough Council's Information Management Group (IMG).

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. In addition, it is recommended that the designated person should also be responsible for:-

- internal IG and/or operational procedures and processes;
- the dissemination and implementation of, and monitoring and evaluating adherence to, the ISA and related guidance within their organisation;
- facilitating the training, advice and ongoing support to all relevant staff in respect of the ISA and associated guidance;
- 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;
- 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 person-identifiable information without consent, etc;
- deciding upon requests to disclose information, even where the service user has consented, to an organisation that is not a signatory of this, or other appropriate, arrangements;
- liaising with other signatory organisations;
- reviewing and commenting on any amendments to the ISA; and
- ensuring the IG Team keeps the list of signatories up-to-date and appropriately circulated.

4.5 Staff Requirements

The conditions, obligations and requirements set out in the ISA and associated Tier 2 ISAs will apply to all appropriate staff, agency workers and volunteers working within those organisations. All organisations should ensure that their 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 Sections 7.1 and 7.2).

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

4.6 Circulation/Dissemination

This ISA and other associated documents shall be freely available to any representative of any signatory organisation and relevant staff via the most appropriate communications channel. It shall also be available to service users and, wherever possible, to the general public upon request.

4.7 Principal Values Applicable to Information Sharing

Each organisation agrees to comply with the following values when sharing and processing service user and / or employee information.

- Day-to-day operations are conducted in such a manner that person-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 1998 Schedule 1 Principles 1 and 6).

- That every proposal to share person-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 1998 Schedule 1 Principle 2 and Caldicott Principle 1).

- 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 person-identifiable information cannot be justified then it may be permissible to share depersonalised aggregated information, e.g. for research/analytical purposes (Caldicott Principle 2).

- That any shared person-identifiable information must be the minimum information required for the stated purpose, e.g. adequate, relevant and not excessive and be kept accurate and up-to-date (DPA 1998 Schedule 1 Principles and 4 and Caldicott Principle 3).

- That shared person-identifiable information shall not be kept for longer than is necessary in accordance with the agreed purposes (DPA 1998 Schedule 1 Principle 5).

- That access to person-identifiable information will be restricted to a 'need-to-know' basis (Caldicott Principle 4).

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

4.8 Deceased Persons

The DPA 1998 relates to living individuals. As a result, the Act does not oblige an organisation to supply anyone with such information. However, 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 person-identifiable information relating to a deceased person and, if necessary, appropriate managerial/specialist advice must be sought.

4.9 Compliance with the DPA

Each organisation must have an appropriate entry (notification) in the Register of Data Controllers managed by the Information Commissioner's Office (ICO). This will be evidenced by a valid registration number and renewal date on the DAP, which will be checked against the Register[1].

Each organisation must respect the seven rights given to individuals in respect of their own person-identifiable information.

Each organisation must adhere to the eight enforceable principles in respect of the processing of person-identifiable information and, in order to process any person-identifiable information, each organisation must ensure that at least one condition of Schedule 2 is met. Also, in order to process any sensitive information, 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. In addition, a Common Law Duty of Confidentiality may apply in these circumstances and should be considered in conjunction with this requirement.

Each organisation must hold all person-identifiable information 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 of destruction or damage (DPA 1998 Schedule 1 Principle 7).

4.10 Service User Awareness and 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/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 DPA 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. However, this right is not absolute and may be overridden in certain circumstances.

[1] Available: http://www.ico.gov.uk/what_we_cover/promoting_data_privacy/keeping_the_register.aspx

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 person-identifiable information.

Each organisation must ensure that they have appropriate policies and procedures in place to facilitate the exercising of these, and other, rights 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 and Accuracy of Person-Identifiable Information

Each organisation is responsible for the quality and accuracy of the person-identifiable information it obtains, records, holds, uses and shares. As such, all practitioner interventions and their outcomes with service users must be properly recorded within the organisation's case management systems and when information is being recorded, 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;
- whether it comprises fact, opinion, hearsay or a mixture of these; and
- the identity of the person(s) receiving and recording the information (in many instances this may be one and the same).

It is likely that the majority of electronic case management systems/electronic care records 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/electronic care record 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 information exchange in order to establish and maintain a consistent approach to the way that information is collected, stored and shared.

4.12 Use of Person-Identifiable Information for Evaluation and Research Purposes

Each organisation may use person-identifiable information 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 ICO and service users / employees have been made aware of this purpose. If the service users' / employees' implied consent is being relied upon for this purpose, then each organisation must ensure that they comply with the fair and lawful processing principle as defined by the DPA 1998.

Where a change of use has taken place regarding the further use of person-identifiable information then further consent must be sought from the service user / employee.

4.13 Use of Person-Identifiable Information for Marketing and Commercial Purposes

Each organisation may not use person-identifiable information shared between organisations as a result of this ISA or any associated ISAs for the purpose of any marketing and/or commercial activities, unless it is contained within your notification to the ICO and the service users / employees have been made aware of this purpose and appropriate consent has been obtained from each service user / employee to use their information for this particular purpose.

If the service users' / employees' implied consent is being relied upon for this purpose, then each organisation must ensure that they comply with the fair and lawful processing principle as defined by the DPA 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 / employee prior to the use of their information.

4.14 Information Retention

Each organisation must have an Information Retention Policy that accords to the legitimate purposes of that organisation. The policy should make clear the organisation's 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 Information Access and 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, person-identifiable information.

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- or position-based access controls/practitioner access levels, information transfer and receiving and system specific security policies. Ideally, the standard applied should be ISO17799.

Wherever common protective markings are used (then each party organisation should agree the common meaning of these terms and the associated procedures in order to ensure that the transmission/receipt and storage of information thus marked is appropriate to the level of security required.

4.16 Staff Awareness and 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 the following.

- This ISA 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 from these.
- Common law duties (e.g. confidentiality).
- Appropriate Codes of Practice and other associated regulations/guidance (e.g. Confidentiality, Information Security Management, Records Management, etc).

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 (or other person) 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 care records of looked after children.

All staff will be sensitive to the need for interagency confidentiality when discussing service users with other organisations or departments. The relationship between organisation, 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 and 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 the service user's consent, having weighed up the public interests at stake. The key test

is that of proportionality, e.g. whether the proposed sharing is a proportionate response to the need to protect the public interest in question.

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 / employees, when they first engage with the organisation, as to the circumstances by which their information may be gathered, recorded and shared.

As previously stated in Sections 1.2 and 2.2 for statutory sector bodies, and those carrying out statutory functions on their behalf, this must be within a suitable legal context, e.g. a body must have the appropriate express or implied duties, functions or powers to gather, record and share person-identifiable (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 (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, etc.).

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 individual's 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 in 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 Tier 2 ISAs must clearly state the approach to be used by each of the parties in this respect.

7 Monitor and Review

7.1 Non-Compliance (Internal)

Instances of internal non-compliance with this ISA and associated documents and procedures will be logged and reported to the appropriate designated person. They should be dealt with promptly and in accordance with the agreed IG/operational policies and procedures. These should be described in the appropriate Tier 2 ISA. 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; and
- disregard of the views and rights of service users.

7.2 Non-Compliance (Partner Organisations)

Instances of non-compliance with this ISA and associated documents and procedures by a partner organisation will be reported to that organisation's designated person and, if established, the appropriate IG Group. They should be dealt with promptly in accordance with the agreed IG/operational policies and procedures. These should be described in the appropriate Tier 2 ISA. 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; and
- disregard of the views and rights of service users.

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 designed person or IG Group. These should also be described in the appropriate ISA.

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 in Sections 7.1 and 7.2 and in the appropriate ISA.

Any concerns/complaints received from practitioners relating to the operation of this ISA will be referred to their organisation's designed person who will respond in

accordance with the internal policies and procedures of that organisation and the conditions outlined in Sections 7.1 and 7.2 and in the appropriate ISA.

7.4 Formal Review

These arrangements notwithstanding, the ISA and the associated procedures and systems for the sharing of information will be subject to ongoing review and, at a minimum, a formal review by all parties every three years.

New DAPs will only be required should there be a major change to the Agreement or if the main signatory or designated person's details should change.

8 Effective Date

This ISA is effective from 19th November 2012. This document will remain in effect until superseded or formally replaced. It will be reviewed again by 31 October 2015.

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 (e.g. the organisation has a new Chief Executive Officer or Caldicott Guardian), a new DAP will be required to ensure that they are aware of the ISA and agree to its use.

Information Sharing Agreement – Tier 1

DECLARATION OF ACCEPTANCE & PARTICIPATION

I, the undersigned, on behalf of the organisation named below, agree to support the implementation of this Information Sharing Agreement (ISA) and associated Tier 2 ISA(s) 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 ISA and with whom a separate Tier 2 ISA 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: Z4803991

Annual Renewal Date: 04/01/2014

Main Signatory/Principal Person

Name: David Parr Position: Chief Executive

Organisation: Halton Borough Council

Address: Municipal Building, Kingsway, Widnes WA8 7QF

Tel No: 0151 511 6000

E Mail: david.parr@halton.gov.uk

Signature: _____ Date: 10 Jan 2013.

DESIGNATED LIAISON OFFICER

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

Name: Peter Richmond Position: Divisional Manager, Service Improvement (Data Protection Lead Officer/Caldicott Guardian)

Address: Municipal Building, Kingsway, Widnes WA8 7QF

Tel No: 0151 511 7003

E-mail: peter.richmond@halton.gov.uk