SAFEGUARDING ADULTS

PROTOCOL

FOR SHARING INFORMATION

BETWEEN

AGENCIES IN TAMESIDE

September 2014

GENERAL PROTOCOL FOR SHARING INFORMATION BETWEEN AGENCIES IN TAMESIDE

Contents

SECTION 1

1. INTRODUCTION

The Parties

THIS AGREEMENT is made on the 1st May 2014.

BETWEEN

- TMBC, Community, Children, Environment, Adults and Health Services
- Tameside Hospital NHS Foundation Trust
- Clinical Commissioning GroupTameside and Glossop
- Stockport Foundation Trust-Tameside and Glossop Community Healthcare Business Group
- Pennine Care NHS Foundation Trust, Tameside and Glossop
- Fire and Rescue Service, Tameside
- Greater Manchester Police
- Victim Support
- Healthwatch
- The National Probation Service
- Probation-Community Rehabilitation Companies
- Carers Action Group

2. PURPOSE OF THE DOCUMENT

This document is the Information Sharing Protocol for agencies working in Tameside and all partners are committed to complying with the requirements of the agreement. It provides guidance for sharing relevant personalised information between these agencies. "No Secrets", produced by the Department of Health in relation to adult protection, provides guidance on developing and implementing multi-agency policies and procedures to safeguard adults from abuse. The purpose of this document is to provide a legal and policy framework to facilitate the legitimate inter-agency sharing of information, in relation to safeguarding adults at risk of abuse. It is acknowledged that there is no legal contractual relationship or contract of employment between these partners and no partner can enter into any contractual arrangement on behalf of the other partners,

. It is accepted from practice, experience and research that the sharing of information between professionals helps to ensure that adults and children in need receive the care, protection and support they need. Sharing personal information between partner agencies is vital to the provision of co-ordinated and seamless care for individuals. In addition the sharing of information can help achieve statutory and local initiatives designed to prevent crime and disorder. Legislation does not prevent the sharing of information between agencies delivering services, although there are important rules and safeguards to be observed.

All professionals who are party to this agreement accept their continuing obligation to comply with their professional codes of conduct.

It is expected that individual agencies will prepare their own operational procedures specific to particular purposes. However, all agencies that are party to this general protocol agree to ensure that operational procedures are compliant and consistent with this document.

The Purpose of Information Sharing

The purpose of information sharing with reference to this document is to safeguard adults at risk of abuse and may only be used for this purpose.

SECTION 2

3. KEY LEGISLATION AND GUIDANCE

The Data Protection Act 1998 – Introduction

Since 1st March 2000 the key legislation governing the obtaining, protection and use of identifiable personal information has been the Data Protection Act 1998 (The DPA). This does not apply to information relating to the deceased.

The key difference between the DPA and the previous legislation is that it applies not only to automatically processed personal data but also to manual personal data.

The Data Protection Act Principles

The DPA sets out eight principles which must be complied with when obtaining and using personal data. These principles are as follows: -

First Principle
Obtain and process personal data fairly and lawfully.

Second Principle
Hold data only for the lawful and specified purposes.

Third Principle
Personal data shall be adequate, relevant and not excessive in relation to the purposes for which it is processed.

Fourth Principle
Personal data must be accurate and where necessary, kept up to data.

Fifth Principle
Hold data for no longer than necessary.

Sixth Principle
Personal data shall be processed in accordance with the rights of data subjects under the Act

Seventh Principle
Measures should be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction or damage to personal data.

Eighth Principle
Personal data shall not be transferred to a country outside the European Economic Area unless that country ensures an adequate level of protection for the rights of freedoms of data subjects regarding the processing of personal data.

The use of personal information by agencies must therefore comply with these principles.

The Lawful Use of Information

When sharing information, compliance with the first DPA principle is crucial to ensuring the sharing of information is carried out lawfully.

To ensure personal information is processed in a lawful manner one of several specified conditions, which are set out in Schedule 2 of the DPA, must be complied with. These conditions are as follows: -

- The individual has given his/her consent to the processing
- The processing is necessary to comply with a legal obligation
- The processing is necessary in order to protect the vital interests of the individual (this is envisaged to be a life and death scenario)
- The processing is necessary in order to pursue the legitimate interest of the organisation or certain third parties (unless prejudicial to the interests of the individual)
- The processing is necessary for the entering into a contract at the request of the individual or performance of a contract to which the individual is a party.

Therefore, as a general rule, if one of the above conditions is satisfied, the processing of information is likely to be lawful. However, if the information to be processed is what is described as "sensitive personal data" then there are extra conditions that must be satisfied before the processing of information is lawful.

Sensitive personal data is information that relates to: -

- The racial or ethnic origin of the individual
- Their political opinions
- Their religious beliefs of a similar nature
- Whether they are a member of a trade union
- Their physical or mental health or condition
- Their sexual life / preference / orientation
- The commission or alleged commission by them of any offence
- Any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings of the sentence of any Court in such proceedings.

Therefore, should the information processed come within one of the categories of sensitive personal data, one of the following conditions, which are contained in Schedule 3 of the DPA, must be satisfied before processing that information.

The main conditions are as follows:

- That the individual has given their explicit consent to the processing of the personal information

- That the processing is necessary to perform any legal right or obligations imposed on the organisation in connection with employment

- The processing is necessary to protect the vital interests of the individual or another person, where consent cannot be given by the individual, or the organisation cannot be reasonably expected to obtain consent or consent is being unreasonable withheld where it is necessary to protect the vital interest of another

- The information contained in the personal information has been made public as a result of steps deliberately taken by the individual

- The processing is necessary in connection with legal proceedings, dealings with legal rights or taking legal advice

- The processing is necessary for the administration of justice or carrying out legal or public functions

- The processing is necessary for medical purposes

Where information is given to professionals in confidence, then in addition the the common law duty of confidentiality must also be considered. This is summarised at paragraph 16 below.

Individuals' Rights under the Act

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

- Rights of subject access

- Rights to prevent processing likely to cause damage or distress

- Rights to prevent processing for the purposes of direct marketing

- Rights in relation to automated decision making

- Right to take action for compensation if the individual suffers damage

- Right to make a request to the Commissioner for an assessment to be made as to whether any provision of the Act have been contravened

Individuals' Rights of Access to Information

Subject to certain exceptions, any living person who is the subject of information held and processed by an organisation has a right of access to that information. Where access is refused, the individual may appeal. There are certain statutory exemptions, which may limit access rights. These include for example where access to perpetrators details would prejudice the prevention or detection of crime.

Organisations – indemnity

- *Reporting breaches*
  Any information security breaches, incidents of unlawful processing, accidental loss, destruction or damage to data should be reported immediately to the party identified as being the data owner.

- *Subject access consultation clause*
  If any Party receives a request under the Subject Access provisions of the Data Protection Act 1998 and Personal Data is identified as belonging to or originating from, another Party, the receiving Party will contact the other Party to determine if the latter wishes to claim an exemption under the provisions of the Act.

- *Section 10 notice consultation clause*
  Where any Party receives a Notice under Section 10 of the Data Protection Act 1998, and the Personal Data to which the Notice applies is identified as belonging to or originating from another Party, the receiving Party will contact that other Party to ascertain whether or not they wish to make any representations about a response to, or compliance with, that Notice. All Parties recognise that a response to such a notice must be provided within 21 days and agree to make any representations as soon as possible to enable this deadline to be met.

- *Indemnity clause*
  In consideration of these arrangements for sharing information for the Purpose any party receiving information undertakes to indemnify and keep indemnified any party that has disclosed information to them against any liability, which may be incurred by the disclosing party, as a result of the receiving party breaching the terms of this agreement.

Provided that this indemnity shall not apply:

a) Where the liability arises from information supplied by the disclosing party that is shown to have been incomplete or incorrect, unless the disclosing party establishes that the error did not result from any wilful wrongdoing or negligence on his part

b) Unless the disclosing party notifies the receiving party as soon as possible of any action, claim or demand to which this indemnity applies, commits the receiving party to deal with the action, claim or demand by settlement or otherwise and renders the receiving party all reasonable assistance in so dealing;

c) To the extent that the disclosing party makes any admission, which may be prejudicial to the defence of the action, claim or demand

The Common Law Duty of Confidentiality

Information has a necessary quality of confidence when it is of a confidential character. This does not mean that the information need be particularly sensitive, but simply that it must not be publicly or generally available. Information is not confidential if it is in the public domain. To decide whether an obligation of confidence exists, the following must be considered: -

- Whether the information has a necessary quality of confidence

- Whether the circumstances of the disclosure have imposed an obligation on the confidante to respect the confidence. This usually means considering whether the information was imparted for a limited purpose.

Most of the information used by the parties to this agreement will be of a confidential nature. Therefore, as a general rule this confidential information should not be disclosed without the consent of the subject. However, the Law permits the disclosure of confidential information where there is an overriding public interest or justification for doing so.

Examples of this might be child protection or the prevention and detection of crime or public safety.

The Human Rights Act 1998

Article 8 (1) provides that: -

Everyone has the right to respect for his private and family life, his home and his correspondence.

However, this is a qualified right and Article 8 (2) states that: -

There should be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interest of national security, public safety or the economic wellbeing of the country, for the protection of the rights and freedoms of others.

Therefore, disclosure of information will need to take Article 8 into consideration. The sharing of information may be necessary, for example, for the protection of health or morals, for the prevention of the rights and freedoms of others or for the protection of disorder and crime.

The Crime and Disorder Act 1998

This Act was introduced to provide measures to prevent crime and disorder and anti-social behaviour in the community. Section 115 of the Act provides that any person can lawfully disclose information where necessary or expedient for the purposes of any provision of the Act, to a chief officer or police, a police authority, a local authority, a probation service or a health authority, even if they do not otherwise have this power. This power also covers disclosure to people acting on behalf of any of the named bodies. The “purposes” of the Act include a range of measures such as local crime audits, youth offending team, anti-social behaviour orders, sex offender orders and local child curfew schemes. However, the use of Section 115 must be considered on a case by case basis, and must still be compliant with the principles of the DPA.

The Care Standards Act 2000

This Act established the National Care Standards Commission. Part V11 is specifically concerned with the protection of children and vulnerable adults. Section 81 of the Act obliges the Secretary of State to keep a list of individuals Who are considered unsuitable to work with vulnerable adults. Section 82provides that a person who provides care for vulnerable adults shall refer a care worker to the Secretary of State for the following reasons: -

> That the provider has dismissed the worker on the grounds of misconduct (whether or not in the course of his employment) which harmed or placed at risk of harm vulnerable adults;
>
> That the worker has resigned, retired or been made redundant in circumstances such that the provider would have dismissed him, or would have considered dismissing him, on such ground if he had not resigned, retired or been made redundant;
>
> That the provider has, on such grounds, transferred the worker in a position which is not a care position;

That the provider has, on such grounds suspended the worker or provisionally transferred him to a position which is not a care position but has not yet decided whether to dismiss him or to confirm the transfer.

The Independent Safeguarding Authority is a non-departmental public body. The Independent Safeguarding Authority's (ISA) role is to help prevent unsuitable people from working with children and vulnerable adults. They **assess** those individuals working or wishing to work in regulated activity that are referred to us on the grounds that they pose a possible risk of harm to vulnerable groups. Any person who is to be considered for an employment placement which involves working with vulnerable adults will, as a statutory requirement, have to be police checked and also the ISA will be checked. If the person is on the list the employer can not employ the person in a care position. The ISA has legal responsibilities to: -

- To maintain a list of individuals barred from engaging in *regulated activity* with children;
- To maintain a list of individuals barred from engaging in *regulated activity* with vulnerable adults;
- To maintain both barred lists; and
- To reach decisions as to whether to remove an individual from a barred list.

The Caldicott Principles

The Caldicott Principles laid down by the NHS Executive, must also be followed by those employed by the Trust. The principles are as follows: -

Principle 1 – Justified purpose.
Every proposed use or transfer of patient identifiable information within or from an organisation should be clearly defined and scrutinized, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2 – Don't use patient identifiable information unless it is Absolutely necessary.
Patient identifiable information items should not be used unless there is no alternative.

Principle 3 – Use the minimum necessary patient identifiable information.
When use of patient identifiable information is considered to be essential, individual items of information should be justified with the aim of reducing identifiably if possible.

Principle 4 – Access to patient identifiable information should be in the strict need to know basis.
Only those individuals who need access to patient identifiable information should have access to it, and they should only have access to the information items that they need to see.

Principle 5 –Everyone should be aware of their responsibilities.
Action should be taken to ensure that those handling patient identifiable information, both clinical and non-clinical staff are aware of their responsibilities and obligations to respect patient confidentiality

Principle 6 – Understand and comply with the Law
Every use of patient identifiable information must be lawful. Someone in each of these organisations should be responsible for ensuring the organisation complies with relevant legal requirements.

Freedom of Information Act

The Freedom of Information Act 2000 provides public access to information held by public authorities.

It does this in two ways: -

Public authorities are obliged to publish certain information about their activities; and members of the public are entitled to request information from public authorities.

The Act covers any recorded information that is held by a public authority in England, Wales and Northern Ireland, and by UK-wide public authorities based in Scotland. Information held by Scottish public authorities is covered by Scotland's own Freedom of Information (Scotland) Act 2002.

Public authorities include government departments, local authorities, the NHS, state schools and police forces. However, the Act does not necessarily cover every organisation that receives public money. For example, it does not cover some charities that receive grants and certain private sector organisations that perform public functions.

Recorded information includes printed documents, computer files, letters, emails, photographs, and sound or video recordings.

The Act does not give people access to their own personal data (information about themselves) such as their health records or credit reference file. If a member of the public wants to see information that a public authority holds about them, they should make a subject access request under the Data Protection Act 1998

Government Protective Marking Scheme

The Parties agree to apply appropriate security measures, commensurate with the requirements of The Seventh Data Protection Principle, which states that: "appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data". In particular, they shall ensure that measures are in place to do everything reasonable to:

- Make accidental compromise or damage unlikely during storage, handling, use, processing transmission or transport
- Deter deliberate compromise or opportunist attack, and
- Promote discretion in order to avoid unauthorised access

In particular, the Parties are required to handle all data received in accordance with the protective marking shown, if no marking is shown the data should be handled in accordance with at least RESTRICTED GPMS marking.

For example, all manual papers should be stored within a lockable cabinet within a secure building, with access only granted to those individuals pursuant to the Purpose.

SECTION 3

4. PRINCIPLES GOVERNING THE SHARING OF INFORMATION

Principles governing the sharing of information in Tameside

In seeking to share information to improve services and support to the population of Tameside, agencies in Tameside will adhere to the following principles: -

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

(b) Non-Health and Social Care organisation recognise the requirements that Caldicott imposes on Health and Social Care organisations an will ensure that requests for information from Health and Social Care organisations are dealt with in a manner compatible with these requirements.

(c) Information is provided in confidence when it appears reasonable to assume that the provider of the information believed that this would be the case. It is generally accepted that most (if not all) information provided by patients/clients is confidential in nature. All organisations which are party to this protocol accept this duty of confidentiality and will not disclose such information without the consent of the person concerned, unless there are statutory grounds and an overriding justification for so doing. In requesting the release and disclosure of information from members of partner organisations, staff in all organisations will respect this responsibility and not seek to override the procedures which each organisation has in place to safeguard against information being disclosed illegally or inappropriately.

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

(e) Organisation/agencies are fully committed to ensuring that they share information in accordance with their statutory duties. They will seek to put in place procedures which ensure that the principles of the Data Protection Act 1998 are adhered to and underpin the sharing of information between their agencies. They recognise the sensitivity of information about a person's racial or ethnic origin, political opinions, religious or other similar beliefs, trade union membership, physical and mental health, sexuality, the commission or alleged commission of offences and any proceedings for any offences committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings and will adhere to the requirements of Schedule 3 of the DP Act. Organisations, which have obtained information in these categories about an individual, in the course of their direct contact with that person, will seek to obtain the explicit consent of that person to disclose that information to another organisation. If consent is not given, because the person is either unable or unwilling to give that consent, then the information will only be released if there are statutory grounds for doing so and one of the remaining conditions of Schedule 3 can be demonstrated.

(f) Individuals in contact with organisations/agencies will be fully informed about information, which is recorded about them. If an organisation has statutory grounds for restricting an individual's access to information relating to them, then the individual will be told that such information is held and on what grounds it is restricted. Other than this, they will be given every opportunity to gain access to information held about them and to correct any factual errors that have been made. Similarly, where opinion about them has been recorded and the services users feels this opinion is based on incorrect factual information, they will be given every opportunity to correct the factual error and record their disagreement with the recorded opinion.

(g) Where professionals request that information supplied by them be kept confidential from the person, the outcome of this request and the reasons for taking the decision will be recorded. Such decisions will only be taken on statutory grounds. Further explanation to this can be found at paragraph 34.

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

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

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

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

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

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

(n) Procedures will be put in place to ensure that decisions to disclose personal information without consent have been fully considered regard to applicable legislation and Schedules 2 or, in the case of sensitive information, Schedule 3 or the DP Act 1998, and that these decisions can be audited and defended.

(o) Staff will be made aware that disclosure of personal information which cannot be justified on statutory grounds and under Schedules 2 or, in the case of sensitive information, Schedule 3 or the DP Act 1998, whether inadvertent or intentional will be subject to disciplinary action.

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

SECTION 4

5. PROCEDURES FOR THE DISCLOSURE OF PERSONAL INFORMATION

Obtaining Consent

The general principle is that people should be fully informed as possible. Therefore, as a general rule, in every practical circumstance, the individual's consent should be obtained before sharing identifiable information.

In most cases the consent to share information will be sought at the first contact with an individual. The member of staff should inform the person who their employer is, why the information sought is to be shared, and which agencies the information might be shared with. If, in the professional judgement of the staff member concerned, to address these issues at the time of first contact, then the reason for doing so should be recorded and arrangements agreed to complete this task at the first available opportunity.

Should it become necessary to share information with other agencies other than as originally agreed with the service user, or to share information for other purposes other than originally agreed, then the renewed consent of the individual be obtained unless disclosure can otherwise be justified as being in the public interest where the information is of a confidential nature, and within the conditions permitted in Schedule 2 and Schedule 3 of the DPA 1998.

Each agency agrees to work towards a situation whereby in most cases, where practically possible, especially in the case of sensitive information, the consent of the individual is given in writing. If consent can only be taken verbally, then the details of this consent should be recorded on an individual's file. An individual should be given a copy of any written consent given by them, and a further copy placed on the individual's file. Any refusal of consent or limited consent should also be recorded on the file.

Where it is necessary to seek the renewed consent of the individual, for example, because the purpose for which the information is to be shared has changed, or information is to be given to different agencies other than originally agreed with the service user, then the agencies agree to work towards obtaining a fresh written consent of the service user, where practical to do so.

Individuals should be made aware that use of information is necessary to enable the organisation to meet its statutory obligations in relation to the particular service and the individual, to ensure the individual is not misled.

Responsible steps should also be taken to ensure that individuals are informed of their right to seek access to the information held about them. It is therefore important that staff having direct contact with the individual ensure that the information they gather is accurate, coherent and as comprehensive as is needed, and properly recorded.

Where an individual does not have the capacity to make an informed decision, and are incapable of managing their own affairs, or where the individual is too young to understand, consent should be obtained from the person with legal authority to act on under the person's behalf. Legal advice may be necessary in cases of uncertainty. Reference to the Mental Capacity Act 2005 should be made when considering capacity.

Disclosure Without Consent

Although it is regarded as good practice to seek the consent of the individual, disclosure without the consent of the individual is lawful where the conditions set out in Schedule 2 of the DPA are met, and where the data is sensitive, where one of the conditions set out in Schedule 3 is met. Disclosure without consent of confidential information should only be made however where it is in the public interest to do so. The information may, for example, need to be shared to ensure the performance of public functions or a legal obligation. Organisations will need to ensure that anyone who is given access to personal information is aware of the need to treat the information as confidential.

In other cases, consent should not be sought, as least initially, to the obtaining and sharing of information, provided the criteria under Schedules 2 and 3 are met, where it would be against the public interest to seek consent at this point.

"No Secrets", produced by the Department of Health in relation to adult protection states at Section 3.6 that the interagency framework must: -

"…*balance the requirements of confidentiality with the consideration that, to protect vulnerable adults, it may be necessary to share information*".

At Section 5.6 it goes on to say: -

"*Confidentiality must not be confused with secrecy; informed consent should be obtained but if this is not possible and vulnerable adults are at risk, it may be necessary to override this requirement".*

In other cases, disclosure might prejudice permitted objectives, such as the prevention of detection of crime or the apprehension or prosecution of offenders. Legal advice should be taken in cases of uncertainty.

In certain cases, the consent of an individual may be sought to disclose the information, but that consent is refused. That refusal of consent can be overridden provided the requirements of the DPA are met, and in the case of confidential information, where it is in the public interest to disclose. Taking into account the Human Rights Act, a balancing exercise needs to be carried out between the individuals right to confidentiality, and the public interest in disclosure. The refusal of consent and the reasons for overriding that refusal should be recorded on the client's file.

Each organisation should refer to their own internal confidentiality guidelines on seeking consent.

SECTION 5

6. ACCESS AND SECURITY PROCEDURES

Each agency who is party to this agreement will ensure procedures are prepared to enable the person to be given access to personal information held about them. In the case of joint records, either organisation can provide access to the joint record, provided the individual is informed that the information is held jointly. Agencies in joint record holding arrangements therefore agree to ensure they have in place procedures to enable the individual to be made aware that he/she is not obliged to apply to all of the agencies for access, and to ensure that each agency is informed that access has been given.

Where information relating to an individual is shared between the agencies, each agency shall take all reasonable steps to ensure this information is transferred and shared in a secure manner.

Agencies shall ensure that appropriate security measures are taken to ensure that data is stored and held in a secure manner. These measures will ensure that access to the information can only be obtained by those with the need and the right to know.

Records held on behalf of TASP will be retained in line with the Local Authority Retention guidance.

SECTION 6

7. MONITORING AND REVIEWING PROCEDURES

This Protocol will be subject to annual review. The day-to-day operation of the Protocol will be reviewed at appropriate intervals by Tameside Adults Safeguarding Partnership.

This Protocol will be agreed by each signatory agency through its own appropriate mechanism for dealing with data protection and information sharing issues.

Each agency is aware that this Protocol may need modifying should there be further legislative changes. Legal advice will be sought by TASP before any major changes to the protocol are considered.

Copies of this protocol will be held by the allocated TASP lead Data Protection Officer for each agency.

SECTION 7

8. PARTNERSHIP UNDERTAKING

Undertaking

The parties to the Protocol accept that the principles laid down in this document will provide a secure framework for the sharing of information between their agencies in a manner compliant with their statutory and professional responsibilities.

As such they undertake to: -

- Implement and adhere to the principles set out in this Protocol.
- Ensure that all **operational procedures** established between their agencies for the sharing of information relating the population of Tameside are consistent with the **General Protocol**.
- Ensure that where these procedures are adopted then no restrictions will be placed on the sharing of information other than those specified within **operational procedures**.

This agreement must be signed by TASP Leads for each of the TASP organisations prior to information sharing taking place: -

- Tameside MBC; Communities, Childrens, Adults and Health
- Tameside and Glossop Clinical Commissioning Group
- Stockport NHS Foundation Trust Community Healthcare Business Group
- Pennine Care NHS Foundation Trust
- Tameside Hospital NHS Foundation Trust
- Greater Manchester Police
- Greater Manchester Fire and Rescue Service
- The National Probation Service
- Probation-Community Rehabilitation Companies
- Healthwatch
- Victim Support
- Carers Action Group

Signatory

Review Date: September 2015