Purpose Specific Information Sharing Agreement
Version 6 - April 2016

Sharing of Information within the Merton Multi Agency Safeguarding Hub (MASH) to assist in identifying and assessing risks to children’s wellbeing and welfare in the borough
<table>
<thead>
<tr>
<th>Freedom of Information Act Publication Scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Protective Marking</strong></td>
</tr>
<tr>
<td><strong>Publication Scheme Y/N</strong></td>
</tr>
<tr>
<td><strong>Title</strong></td>
</tr>
<tr>
<td><strong>Version</strong></td>
</tr>
<tr>
<td><strong>Summary</strong></td>
</tr>
<tr>
<td><strong>Author</strong></td>
</tr>
<tr>
<td><strong>Date Issued</strong></td>
</tr>
<tr>
<td><strong>Review Date</strong></td>
</tr>
</tbody>
</table>
Generic guidance document:

<table>
<thead>
<tr>
<th>Protective marking</th>
<th>Not Classified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suitable for Publication Scheme Y/N</td>
<td>Y</td>
</tr>
<tr>
<td>Purpose</td>
<td>Generic guidance document for use by boroughs engaged in the MASH project</td>
</tr>
<tr>
<td>Author</td>
<td>MASH ODG</td>
</tr>
<tr>
<td>Date created</td>
<td>April 2016</td>
</tr>
<tr>
<td>Review date</td>
<td>2 years</td>
</tr>
</tbody>
</table>

Contents:

1. Introduction ........................................................................................................................................4
2. Purpose of this Information Sharing Agreement ...............................................................................4
3. Scope of this Information Sharing Agreement ..................................................................................5
4. Data Controller – Relationships of MASH .........................................................................................5
5. MASH: Legal Basis for Sharing ...........................................................................................................5
6. Duty of Confidence ...............................................................................................................................7
7. Consent ................................................................................................................................................7
8. Fair Processing ....................................................................................................................................8
9. Access and Individual Rights ...............................................................................................................9
Appendix A – MASH Information Sharing Agreement Partner Signatories ............................................10
Appendix B........................................................................................................................................12
Purpose Specific Information Sharing Arrangement - Guidance .............................................................12
Appendix C........................................................................................................................................23
Purpose Specific Information Sharing Arrangement - Process ................................................................23
1. Introduction

Partners are working together to establish a Multi-Agency Safeguarding Hub (MASH) in the London Borough of Merton. The MASH will deal with safeguarding concerns, where someone is concerned about the safety or wellbeing of a child. Within the MASH, information from different agencies will be collated and used to decide what action to take. As a result, the agencies will be able to act quickly in a co-ordinated and consistent way, ensuring that vulnerable children are kept safe.

The MASH will involve representatives from the Local Authority, Police and Health working collaboratively to enable more effective information sharing between agencies to improve the needs of children and their families.

HM Government has published two guidance documents which should be read in conjunction with this agreement and both are an invaluable resource for all safeguarding professionals:

- Information Sharing: Further guidance on legal issues (2009)

Both documents should be considered as an accurate summary of legal principles and of what the law requires for decision making to be lawful concerning the sharing of information and not merely, as guidance.

Attention is drawn to the ‘seven golden rules’ set out in the Information Sharing; Guidance for practitioners and managers 2008 (p11) as a practical exposition of the law relating to information sharing.

The London Child Protection Procedures should also be viewed as useful guidance in this area.

The Data Protection Act 1998 identifies 8 key principles in relation to the sharing of personalised data.

2. Purpose of this Information Sharing Agreement

This information sharing agreement formally documents the legal basis for sharing information through the MASH. This agreement has been developed to:

- Set out the legal gateway through which information will be shared, e.g. Children Act 1989 and 2004, the Data Protection Act 1998, Human Rights Act 1998 and public interest and confidentiality within common law.

This agreement has been developed to:

- Define the specific purposes for which the signatory agencies have agreed to share information.
- Describe the roles and structures that will support the exchange of information between agencies.
- Set out the legal gateway through which the information is shared, including reference to the Human Rights Act 1998 and the common law duty of confidentiality.
- Describe the security procedures necessary to ensure that compliance with responsibilities under the Data Protection Act and agency specific security requirements.
- Describe how this arrangement will be monitored and reviewed. This should be bi-annually.
3. **Scope of this Information Sharing Agreement**

This agreement is endorsed by the Multi-agency signatories identified in Appendix 1 of this document and is based on their opinion of the ethical and legal requirements of information sharing that should be applied. The specific purpose of this document is to clarify that understanding and to provide guidance.

This is not a legally binding agreement and the content should not be taken as legal advice. Where necessary, further advice on information sharing issues should be sought from the relevant Partner’s nominated person and professional legal advice must be sought where appropriate.

Partner agencies subject to this information sharing agreement will agree to:
- Facilitate the sharing of information in accordance with this agreement.
- Ensure that staff are fully aware of the process for information sharing and will comply with all legal requirements.
- Ensure information held is kept secure at all times.

4. **Data Controller – Relationships of MASH**

Each agency to this agreement is the Data Controller for the information they hold and is solely responsible for securing a lawful basis to share. Data controllers sharing personal information data on data subjects for the purpose of the MASH will be responsible for their own or their employee’s actions and will be liable for any breach they incur under the Data Protection Act 1998 and neither agency intends that the other partners shall be liable for any loss it suffers as a result of the breach. The Data Controller for the MASH is the local authority and will follow its own policy and procedures relating to the retaining, sharing and disposing of information.

5. **MASH: Legal Basis for Sharing**

Section 10 of the Children’s Act 2004 places a duty on the MASH agencies to cooperate to improve the wellbeing of children and young people, which includes protection from harm and neglect. This includes the proportionate sharing of information, where appropriate, to make the best decisions for children and young people. It is the responsibility of all agencies to ensure they are aware of their responsibilities in this regard in order to ensure they are able to respond within set time scales to enquiries from the MASH in order to Safeguard Children and Young People.

Section 11 Children’s Act 2004 places a duty to carry out existing functions in a way that takes into account the need to safeguard and promote the welfare of children. This includes:

- All staff in contact with children understand responsibilities and the most effective ways of sharing information if they believe that a child may be in need, including those children suffering or at risk of significant harm.

Section 10 and 11 of the Children Act 2004 create a ‘permissive gateway’ for information to be shared in a lawful manner. Such information sharing must take place in accordance with statutory requirements pertaining to the disclosure of information namely the Data Protection Act 1998, the Human Rights Act 1998 and the Common Law duty of confidentiality.
Section 17 and Section 47 Children’s Act 1989 place a duty on the local authorities to provide services for children in need and make enquiries about any child the area who they have reason to believe make be at risk or significant harm. Section 17 and 47 also enable the local authority to request help from the partner agencies and places an obligation of these agencies to cooperate. This includes providing information about a child, young person or their family where there are concerns about a child’s well-being, contribute to a Section 17 assessment or a child protection enquiry.

Please note that the Act does not require information to be shared in breach of confidence, however, the partner agency should not refuse a request to share without considering the relative risks of sharing information, if necessary without consent, against the potential risk to a child if information is not shared.

Some concerns regarding children where information will need to be shared under this agreement will often fall below a statutory threshold of Section 47 or even Section 17 Children Act 1989. If they do however fall within these sections of the 1989 Act then these sections will be the main legal gateway.

Section 27 Children’s Act 1989 states that the local authority, for assistance in the exercise of its statutory functions (which includes the provision of service for children in need and the sharing of information for these purposes) request the help of the partner agencies within the MASH.

Data Protection Act 1998 deals with the processing of personal data which relates to a living person, including the expression of any opinion or indication about the intentions in respect of the child or young person is considered personal data. The MASH partner agencies are required to comply with the Data Protection principles set out in schedule 1 of the Act. These are detailed in the MASH guidance document. If information enables an individual to be identified, then schedule 2 condition should be met:

- Subject has given consent to share
- Sharing information is necessary to protect the person’s vital interests; or
- to fulfil a legal duty
- to perform a statutory function
- to perform a public function in the public interest

When information is sensitive then schedule 3 condition must be met:

- individual has given explicit consent to share information
- sharing information is necessary to establish, exercise or defend legal rights
- for the purpose of, or in connection with any legal proceedings
- to protect an individual’s vital interests and the person to whom the information relates cannot consent, unreasonable withholds consent, or cannot be reasonable obtained.
- To perform a statutory function
- Substantial public interest and necessary to prevent or detect a crime and consent would prejudice that purpose
- Processing is necessary for medical purposes and is undertaken by a health professional.

Conditions met by Schedule 2

The conditions 3, 4, 5(b) and 6(1) under schedule 2: the processing is necessary for compliance with any legal obligation to which the Data Controller is subject, other than an obligation imposed by contract. The processing is necessary in order to protect the vital interests of the data subject, and
for the exercise of any functions conferred on any person by or under enactment. The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

**Conditions met by Schedule 3**

The conditions 3(aii) and 7(b) under schedule 3: the processing is necessary in order to protect the vital interests of the data subject or another person, in a case where, the data controller cannot reasonably be expected to obtain the consent of the data subject, and also is necessary for the exercise of any functions conferred on any person by or under an enactment.

Section 29 of the Data Protection Act 1998 does not give a direct power to disclose information, it does however state ‘that if not disclosing information would prejudice the prevention/detection of crime and/or the apprehension/ prosecution of offenders, personal data can be disclosed’.

**6. Duty of Confidence**

A duty of confidence may be owed to both the holder of the data and to the data subject.

Much of the police information to be shared will not have been obtained under a duty of confidence as it is legitimately assumed that data subjects will understand that police will act appropriately with regards to the information for the purposes of preventing harm to or promoting the welfare of children. However, as a safeguard before any information is passed on, police information will undergo an assessment check against set criteria (included in Child Abuse Investigation section of Standard Operating Procedures) by the Public Protection Desk (PPD) within the MASH.

Whilst always applying the tests of proportionality and necessity to the decision to share information, the protection of children or other vulnerable persons would clearly fulfil a public interest test when passing the information to a partner agency whose work with the police would facilitate this aim. All information shared with a partner agency must be relevant to the case in point.

Information held by other agencies that will be shared in the MASH may have been gathered where a duty of confidence is owed. Duty of confidence is not an absolute bar to disclosure, as information can be shared where consent has been provided or where there is a strong enough public interest to do so.

**7. Consent**

The starting point in relation to sharing information is that practitioners will be open and honest with families and individuals from the outset about why, what, how and with whom information will or could be shared.

It may be necessary and desirable to deviate from the normal approach of seeking consent from a family in cases where practitioners have reasonable grounds for believing that asking for consent would be unsafe or inappropriate. For example if there is an emergency situation or if seeking consent could create or increase a risk of harm.

There must be a proportionate reason for not seeking consent and the person making this decision must try to weigh up the important legal duty to seek consent and the damage that might be caused
by the proposed information sharing on the one hand and balance that against whether any, and if so what type and amount of harm might be caused (or not prevented) by seeking consent.

There is no absolute requirement for agencies in the MASH to obtain consent before sharing information nor there a blanket policy of never doing so. There is an obligation to consider on all occasions and on a case by case basis whether information will be shared with or without consent. This determination by a practitioner should always be reasonable, necessary and proportionate. It should always be recorded together with the rationale for the decision.

Under this agreement, if not disclosing information to the MASH would prejudice the situations listed above, organisations are then exempt from the usual non-disclosure provisions and may provide the information requested / they wish to share proactively.

All decisions to share or not share information must be decided on a case-by-case basis and recorded.

This information sharing agreement specifies the legal basis for sharing information by all partner agencies within MASH. For further information on how the legal basis specified above are applied and associated guidance, please review the MASH Process Document and the MASH Guidance document.

8. Fair Processing

It is a requirement of the Data Protection Act 1998 and common law duty of confidence that all organisations that process personal data should have what is now known as a fair processing notice. This will inform individuals about how their personal data will be used by that organisation. This notice will cover:

- The identity of the data controller.
- If the data controller has nominated a representative for the purposes of the Act, the identity of that representative.
- The purpose or purposes for which the data are intended to be processed.
- Any further information necessary, taking into account the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair. Examples of further information are the likely consequences of the processing and whether the personal data may be disclosed to a third party.
- Access to their personal information and mechanism by which individuals can dissent their information from being shared.

The local authority will publish a Unified Privacy Notice specifically identifying the MASH within it and partner organisations will all publish a Unified Privacy Notice in their normal manner. The notice will explain the concept of MASH and how it works in Merton, including Merton Council’s Unified Privacy Notice is available on the council’s website; [www.merton.gov.uk/mash](http://www.merton.gov.uk/mash).

Further information on the Unified Privacy Notice is detailed within appendix B, the MASH Information Sharing Guidance Document.
9. **Access and Individual Rights**

**Subject Access Requests**

Subject access request under the Data Protection Act (1998) from service users/patients or their authorised representatives must be dealt by the data controller under the terms of their local confidentiality / data protection policy.

**Freedom of Information Requests**

Freedom of Information requests under the Freedom of Information Act (1998) from members of the public must be dealt by the data controller under the terms of their local Freedom of Information Policy.
Appendix A – MASH Information Sharing Agreement Partner Signatories

The agencies signing this agreement accept that the procedures laid down in this document 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 procedures and structures set out in this agreement.
- Ensure that where these procedures are complied with, then no restriction will be placed on the sharing of information other than those specified within this agreement.
- Engage in a review of this agreement with partners bi-annually.

We the undersigned agree that each agency/organisation that we represent will adopt and adhere to this information sharing agreement:

<table>
<thead>
<tr>
<th>Agency</th>
<th>Post Held</th>
<th>Name</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>London Borough of Merton</td>
<td>Chief Executive</td>
<td>Ged Curran</td>
<td></td>
<td>4 May 2016</td>
</tr>
<tr>
<td>London Borough of Merton</td>
<td>Director of Children, Schools &amp; Families</td>
<td>Yvette Stanley</td>
<td></td>
<td>4 May 2016</td>
</tr>
<tr>
<td>Metropolitan Police Service, Merton borough</td>
<td>Acting Borough Commander</td>
<td>Steve Wallace</td>
<td></td>
<td>4 May 2016</td>
</tr>
<tr>
<td>Merton Clinical Commissioning Group</td>
<td>Chief Executive</td>
<td>Adam Doyle</td>
<td></td>
<td>12 May 2016</td>
</tr>
<tr>
<td>National Probation Service</td>
<td>Assistant Chief Officer</td>
<td>Adam Kerr</td>
<td></td>
<td>3 May 2016</td>
</tr>
<tr>
<td>CRC</td>
<td>Chief Executive</td>
<td>Helga Swidenbank</td>
<td></td>
<td>10 June 2016</td>
</tr>
<tr>
<td>CLCH</td>
<td>Chief Executive</td>
<td>Peter Coles</td>
<td></td>
<td>12 May 2016</td>
</tr>
<tr>
<td>Merton Voluntary Service Council</td>
<td>Chief Executive</td>
<td>Khadiru Mahdi</td>
<td></td>
<td>3 May 2016</td>
</tr>
<tr>
<td>South West London &amp; St George’s Mental Health Trust</td>
<td>Chief Executive</td>
<td>David Bradley</td>
<td></td>
<td>4 May 2016</td>
</tr>
<tr>
<td></td>
<td>Service Director</td>
<td>Gillian Moore</td>
<td></td>
<td>20 May 2016</td>
</tr>
<tr>
<td>St George's University NHS Foundation Trust</td>
<td>Chief Executive</td>
<td>Professor Simon Mackenzie</td>
<td>27 May 2016</td>
<td></td>
</tr>
<tr>
<td>Epsom and St Helier University Hospitals Trust</td>
<td>Chief Executive</td>
<td>Daniel Elkeles</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Merton General Practices</td>
<td>Chair of the LMC</td>
<td>Marek Jarzembowski</td>
<td>Dr Marek Jarzembowski</td>
<td>17 June 2016</td>
</tr>
</tbody>
</table>
Appendix B

Purpose Specific Information Sharing Arrangement - Guidance
Version 6

Sharing of Information within the Merton Multi Agency Safeguarding Hub (MASH) to assist in identifying and assessing risks to children’s wellbeing and welfare in the borough
Contents:

1 MASH Guidance .................................................................................................................................................. 14
2 First Principle ..................................................................................................................................................... 14
3 Duty of Confidence ............................................................................................................................................. 14
4 Consent .............................................................................................................................................................. 15
5 Section 47 .......................................................................................................................................................... 15
6 Unified Privacy .................................................................................................................................................. 17
7 Legitimate Expectation .................................................................................................................................. 17
8 Human Rights Act 1998 - Article 8 ............................................................................................................... 18
9 Schedule 2, Data Protection Act 1998 ........................................................................................................... 19
10 Schedule 3, Data Protection Act 1998 ............................................................................................................ 19
11 Second Principle ............................................................................................................................................. 19
12 Third Principle ................................................................................................................................................ 19
13 Fourth Principle .............................................................................................................................................. 20
14 Fifth Principle ................................................................................................................................................ 20
15 Sixth Principle ............................................................................................................................................... 21
16 Seventh Principle .......................................................................................................................................... 21
17 Eighth Principle ............................................................................................................................................ 21
18 Information Entering the MASH from Police ............................................................................................... 21
19 Information Entering the MASH from Non-Police Sources ........................................................................ 22
1. **MASH Information Sharing Guidance**

This process document should be read in conjunction with the MASH Information Sharing Agreement and the MASH Process document.

This document provides guidance the MASH process and how the legal basis for sharing information is applied.

2. **First Principle**

The first data protection principle states that data must be processed lawfully and fairly.

A public authority must have some legal power entitling it to share the information.

Some concerns regarding children where information will need to be shared under this agreement will often fall below a statutory threshold of Section 47 or even Section 17 Children Act 1989. If they do however fall within these sections of the 1989 Act then these sections will be the main legal gateway.

Sections 10 and 11 of the Children Act 2004 place new obligations upon Local authorities, police, clinical commission groups and the NHS Commissioning Board to co-operate with other relevant partners in promoting the welfare of children and also ensuring that their functions are discharged having regard to the need to safeguard and promote the welfare of children.

Section 10 and 11 of the Children Act 2004 create a ‘permissive gateway’ for information to be shared in a lawful manner. Such information sharing must take place in accordance with statutory requirements pertaining to the disclosure of information namely the Data Protection Act 1998, the Human Rights Act 1998 and the Common Law duty of confidentiality.

Section 29 of the Data Protection Act 1998 does not give a direct power to disclose information, it does however state ‘that if not disclosing information would prejudice the prevention/detection of crime and/or the apprehension/ prosecution of offenders, personal data can be disclosed’.

Under this agreement, if not disclosing information to the MASH would prejudice the situations listed above, organisations are then exempt from the usual non-disclosure provisions and may provide the information requested / they wish to share proactively.

All decisions to share or not share information **must** be decided on a case-by-case basis and recorded.

3. **Duty of Confidence**

A duty of confidence may be owed to both the holder of the data and to the data subject.

Much of the police information to be shared will not have been obtained under a duty of confidence as it is legitimately assumed that data subjects will understand that police will act appropriately with regards to the information for the purposes of preventing harm to or promoting the welfare of children. However, as a safeguard before any information is passed on, police information will undergo an assessment check against set criteria (included in Child Abuse Investigation section of Standard Operating Procedures) by the Public Protection Desk (PPD) within the MASH.

---

1 In accordance with the Data Protection Act 1998
Whilst always applying the tests of proportionality and necessity to the decision to share information, the protection of children or other vulnerable persons would clearly fulfil a public interest test when passing the information to a partner agency whose work with the police would facilitate this aim. All information shared with a partner agency must be relevant to the case in point.

Information held by other agencies that will be shared in the MASH may have been gathered where a duty of confidence is owed. Duty of confidence is not an absolute bar to disclosure, as information can be shared where consent has been provided or where there is a strong enough public interest to do so.

4. Consent

The starting point in relation to sharing information is that practitioners will be open and honest with families and individuals from the outset about why, what, how and with whom information will or could be shared.

It may be necessary and desirable to deviate from the normal approach of seeking consent from a family in cases where practitioners have reasonable grounds for believing that asking for consent would be unsafe or inappropriate. For example if there is an emergency situation or if seeking consent could create or increase a risk of harm.

There must be a proportionate reason for not seeking consent and the person making this decision must try to weigh up the important legal duty to seek consent and the damage that might be caused by the proposed information sharing on the one hand and balance that against whether any, and if so what type and amount of harm might be caused (or not prevented) by seeking consent.

There is no absolute requirement for agencies in the MASH to obtain consent before sharing information nor there a blanket policy of never doing so. There is an obligation to consider on all occasions and on a case by case basis whether information will be shared with or without consent. This determination by a practitioner should always be reasonable, necessary and proportionate. It should always be recorded together with the rationale for the decision.

5. Section 47 Thresholds do not determinate whether or not consent should be sought within MASH.

It is inherent in the idea of seeking consent that it will be refused. If professionals consider it justifiable to override the refusal in the interests of the welfare of the child then they can and must do so. This decision must be proportionate to the harm that may be caused by proceeding without consent.

Where it is believed the aims of the MASH might be prejudiced if agencies were to seek consent the disclosing agency must consider the grounds to override the consent issue.

The disclosure of personal information without consent is legally justifiable if it falls within one of the defined category of public interest:
The Public Interest Criteria include:

i) The administration of justice;
ii) Maintaining public safety;
iii) The apprehension of offenders;
iv) The prevention of crime and disorder;
v) The detection of crime;
vi) The protection of vulnerable members of the community.

When judging the public interest, it is necessary to consider the following:

i) Is the intended disclosure proportionate\(^2\) to the intended aim?
ii) What is the vulnerability of those who are at risk?
iii) What is the impact of disclosure likely to be on the individual?
iv) Is there another equally effective means of achieving the same aim?
v) Is the disclosure necessary to prevent or detect crime and uphold the rights and freedoms of the public;
vi) Is it necessary to disclose the information, to protect other vulnerable people?

As previously stated a proportionality test must be applied to ensure that a fair balance is achieved between the public interest and the rights of the data subject.

Information is shared initially within the MASH with or without consent in order to assess risk and harm which in turn identifies the proportionate level of response required.

Once a decision is made based on this shared information picture the local authority decision maker together with the relevant partner may hold back within the MASH any information which is deemed by the originating organisation to be too confidential for wider dissemination. Should it be decided to retain confidential information within the MASH then it will always be sign posted to any professional who may receive a referral or request for service.

When overriding the duty of confidentiality the MASH must seek the views of the organisation that holds the duty of confidentiality and take into account their views in relation to breaching confidentiality. The organisation may wish to seek legal advice if time permits.

The MASH processes if followed correctly are relevant in relation to the determination of consent. The MASH comprises a relatively closed and controlled environment, this being a factor a practitioner can weigh in the balance to some extent in an appropriate case as one factor that can add to the conclusion that it is proportionate not to seek or to dispose with consent. It is not however a single overriding reason in the determination concerning consent.

All disclosures must be relevant and proportionate\(^3\) to the intended aim of the disclosure.

6. **Unified Privacy\(^4\)**

It is a requirement of the Data Protection Act 1998 that all organisations that process personal data should have what is now known as ‘Unified Privacy Notice’ which will inform individuals about how their personal data will be used by that organisation.

---

\(^2\) “Proportionate” is the critical issue.

\(^3\) The implication here is that full records should not be routinely disclosed, as there will usually be information that is not relevant.

\(^4\) Previously known as; ‘fair processing’.
This notice will cover:

(a) The identity of the data controller
(b) If the data controller has nominated a representative for the purposes of the Act, the identity of that representative
(c) The purpose or purposes for which the data are intended to be processed.
(d) Any further information which is necessary, taking into account the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.

The local authority will publish a Unified Privacy Notice specifically identifying the MASH within it and partner organisations will all publish a Unified Privacy Notice in their normal manner. The MPS Unified Privacy Notice is published on the external MPS Publication Scheme and is also displayed within police station front offices and custody suites. It states that personal information will be used for the purposes of ‘Policing’ and also states that the MPS may share this information with a variety of other agencies for the purposes of Policing.

A notice explaining the concept of MASH and how it works in Merton, including Merton Council’s Unified Privacy Notice (previously known as Fair Processing Notice) is available on the councils website; www.merton.gov.uk/mash.

Section 29 of the Data Protection Act 1998 allows agencies to share information if complying with the fair processing conditions i.e. telling individuals how their data will be processed/shared; would be likely to prejudice the purposes of the prevention or detection of crime and/or the apprehension and prosecution of offenders.

If staff of signatory agencies receive information and they believe that by NOT disclosing this information the police will be unable to prevent or detect a crime, or the police will be unable to apprehend or prosecute an offender, then they may fairly share that information with the police. This decision will be taken on a case-by-case basis and recorded.

7. Legitimate Expectation

The sharing of the information by police fulfils a policing purpose, in that it will be done in order to protect life in some circumstances and in others it will fulfil a duty upon the police provided by statute law (Children Act 2004) i.e. co-operation to safeguard or promote the well being of children.

It can reasonably be assumed that the persons from whom information is obtained will legitimately expect that police will share it appropriately with any person or agency that will assist in fulfilling the policing purposes mentioned above.

As previously identified consent will have been considered before the individual’s case is brought to the MASH. In cases, where consent has been granted individuals will have a legitimate expectation of how their data is going to be used and with whom it may be shared and why.

Details of this and most other non-sensitive information sharing agreements will be published in line with the requirements of the Freedom of Information Act 2000, on the MPS Publication Scheme. This will also allow members of the public to understand how their personal information may be used by the MPS.
This agreement is published on the Merton Council website at www.merton.gov.uk/mash/mash-data.


There shall 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 interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Consent is relevant to the rights of those to whom confidential information relates, and thus to legal obligations such as the Human Rights Act 1998.

The sharing of information with children’s services may engage Article 8 however there will be no contravention provided that an exception within Article 8(2) applies.

The benefits of effective sharing of information for the purposes set out in this agreement are to the direct benefit\(^5\) of the citizen and so in the public interest. This agreement is:

**In pursuit of a legitimate aim –**

The promotion of the welfare and wellbeing of children and ensuring they achieve all five outcomes is, by virtue of S.11 of Children Act 2004, a legitimate aim and major responsibility of the signatories to this agreement. The sharing of information under this agreement is also in line with Articles 2 and 3 of the Human Rights Act 1988, namely the right to life and the right to prohibition of torture or inhuman or degrading treatment.

**Proportionate –**

The amount and type of information shared will only be that necessary to achieve the aim of this agreement. Information is always to be considered in terms of its proportionality in each set of circumstances, but it must always be remembered that the right to life is paramount.

**An activity appropriate and necessary in a democratic society –**

The police are obliged to do all that is reasonable to ensure the welfare of the most vulnerable of citizens and this is something that is necessary and appropriate in a democratic society. Other signatories to this agreement such as Clinical Commissioning Groups and Children’s Services also have similar obligations, which are necessary and appropriate in a democratic society.


In addition to the legal criteria set out above, the information sharing arrangement must satisfy at least one condition in Schedule 2 of the Data Protection Act in relation to personal data.

\(^5\) Benefit does not always equate to real public interest, and when it does, it still has to be ‘proportionate’
Schedule 2 is satisfied in the case of this agreement by condition 5(b) (the exercise of functions conferred under statute) as there is an implied gateway available for the sharing of information in these circumstances under S.11 Children Act 2004, which obliges the relevant agencies to ensure that its “functions are discharged having regard to the need to safeguard and promote the welfare of children”.

Where the consent of the individual is received, Condition 1 (data subject has given consent to the processing of their data) will apply.]

10. Schedule 3, Data Protection Act 1998

If the information is “sensitive” (that is, where it relates to race, ethnic origin, political opinions, religion or belief system, membership of a trades union, physical/mental health or sexual life, the commission or alleged commission of any offence, proceedings relating to the offence) you must satisfy at least one condition in Schedule 3.

Schedule 3 is satisfied in the case of this agreement by condition 7, ‘the processing is necessary for the exercise of any functions conferred on any person by or under an enactment’ i.e. as mentioned above, Children Act 2004.

Where the consent of the individual is received, Condition 1 (data subject has given explicit consent to the processing of their data) will apply.]

11. Second Principle

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

The MPS information exchanged under this agreement was obtained for policing purposes. Under this arrangement it will not be processed in any manner contradictory to that purpose. Likewise, other agencies also collect information for other purposes.

All information will only be used within the MASH for the purposes of safeguarding the vulnerable and reducing harm, which is not incompatible with the reason it was originally collected.

12. Third Principle

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Due to the complexity of the MASH, providing a prescriptive list of data fields to be shared is difficult.

Any information that is shared into and within the MASH Hub will be decided on a case-by-case basis and must be relevant to the aims of this agreement.

Examples of data that may be shared include:
• Name of subject (child) and other family members, their carers and other persons whose presence and/or relationship with the subject child or children, is relevant to identifying and assessing the risks to that child.
• Age/date of birth of subject and other family members, carers, other persons detailed.
• Ethnic origin of family members.
• Relevant Police information and intelligence
• School and educational information (to include family members where appropriate and relevant)
• GP and health records (to include family members where appropriate and relevant)
• Relevant Anti Social Behaviour data
• Relevant data from London Ambulance Service or London Fire Brigade
• Housing and other partnership data relevant to the child and family who may affect the welfare of that child.

Not all of the above information will be shared in every case; only relevant information will be shared on a case-by-case basis where an organisation has a ‘need-to-know’ about the information.

13. Fourth Principle

Personal data shall be accurate and, where necessary, kept up to date.

All the information supplied will be obtained from signatories’ computer systems or paper records and subject to their own organisations reviews, procedures and validation. Any perceived inaccuracies should be reported to the contact at that agency for verification and any necessary action.

Whilst there will be regular sharing of information, the data itself will be ‘historical’ in nature. Specifically this means that the data fields exclusively relate to individual actions or events that will have already occurred at the time of sharing. These are not categories of information that will substantially alter or require updating in the future. The exception to this will be that of the unborn child.

14. Fifth Principle

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

The data will be kept in accordance with signatories’ file destruction policy. It is acknowledged that there is a need to retain data for varying lengths of time depending on the purpose and also in recognition of the importance of historical information for risk assessment purposes. However, once information is no longer needed, it should be destroyed.

15. Sixth Principle

Personal data shall be processed in accordance with the rights of data subjects under this Act.

---

6 See Annex A for details how this is done locally
Partners to this arrangement will respond to any notices from the Information Commissioner that imposes requirements to cease or change the way in which data is processed.

Partners will comply with subject access requests in compliance with the relevant legislation.

16. Seventh Principle

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.

Measures to satisfy the Seventh Principle are detailed in the Baseline Security Assessment document, prepared as part of the development of this agreement and included in Section Four of the purpose specific agreement, “Description of Arrangements including security matters”.

17. Eighth Principle

Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data.

Under the terms of this agreement no information will be passed outside of the European Economic Area unless specific requirement exists and the originating organisation makes that decision for a particular reason in relation to the safeguarding of a child, young person or adult with a safeguarding need. Legal advice may be necessary in these cases.

18. Information entering the MASH from Police:

Where it has come to the police’s attention that a child is in circumstances that are adversely impacting upon their welfare or safety i.e. failing at least one of the 5 Every Child Matters outcomes, a Pre-Assessment Checklist (PAC) report will be placed by the reporting police officer on to the MPS IT system MERLIN.

Police officers based in the MASH will review these PACs to see if there is a need to inform children services that the child has come to police attention. They will check to see if there is an open case about the child on Children Social Care’s (CSC) database; CareFirst (via the CSC navigator). Where there is an open case, the police will forward the PAC straight to the MASH referral co-ordinator, who will send it on to the responsible case-worker. Where there is no open case on the child, the police officers will conduct further research about what other relevant information the MPS has relating to the welfare of the child. They will send the initial PAC and subsequent research on Form 87M via secure email to the MASH referral co-ordinator.

Upon receiving this information, the MASH referral co-ordinator will create a new case record on CareFirst and see what information Merton CSC hold that is relevant to the MASH enquiry. CSC may also request other organisations to search their respective databases accessible within the MASH for relevant information but each organisation will need to consider consent at this stage. Using the collated police, partner organisations and council information, a MASH assessment will be done to
see if the child is suitable to be considered in the MASH environment, and which other agencies (represented within the MASH or outside) should be approached for further information.

If the decision is made to seek information held outside the MASH the local authority decision maker will consider the issue of consent in respect of any PAC forwarded by the MPS for which they intend to seek further information from another partner.

These agencies will then be asked to provide relevant information to the MASH, for use in interacting with the child and safeguarding the child’s well-being. This information is required so that a full picture as possible is known about the child, meaning the best and most appropriate assistance can be given to them. Based on an assessment of all the information gathered, the local authority decision maker will then decide what the most suitable course of action will be (i.e., referral to social services, placement on an early intervention option etc). Relevant information will then be passed on to agencies who ‘need-to-know’ that information when interacting with that child.

19. Information entering the MASH from non-police sources:

Information about a child where there are concerns about its welfare will be passed to the MASH referral co-ordinator. Similar to the police process, they will check to see if there is an open case, and if so, forward that information on to the relevant case-worker. Where there is not an open case, they will create a new case record; identify if there is any other relevant information held by the local authority CSC and conduct a MASH assessment.

Before considering if the case should continue through the MASH process, the local authority decision maker of the MASH will consult with the police sergeant based within the MASH to see if a crime has been committed. If one has, this will be recorded by the police and an investigation initiated. A decision will then be taken as to whether action can be taken by the MASH at this time or whether this should wait for the conclusion of the police investigation.

If it is decided that the case should continue through the MASH process, other relevant agencies (both inside and outside the MASH, including the police) will be asked to provide relevant information to the MASH so that the local authority decision maker will have as full a picture as possible when assessing and making decisions as to what the best and most appropriate assistance and interaction with the child should be. Once they have decided what this is, the local authority decision maker will refer the child to that service, passing across relevant information that the agency they have been referred to ‘need-to-know’.
Appendix C

Purpose Specific Information Sharing Arrangement - Process
Version 6

Sharing of Information within the Merton Multi Agency Safeguarding Hub (MASH) to assist in identifying and assessing risks to children’s wellbeing and welfare in the borough
## Contents:

1. **MASH Process** .................................................................................................................. 25
2. **Business Continuity** ........................................................................................................ 25
3. **Confidentiality and Vetting** ............................................................................................ 25
4. **Compliance** ..................................................................................................................... 25
5. **Sanctions** ........................................................................................................................ 26
6. **Training / Awareness** ...................................................................................................... 26
7. **Partner's Building and Perimeter Security** ........................................................................ 26
8. **Movement of Information** ............................................................................................... 26
9. **Storage of Information on Partner's System** ................................................................. 26
10. **Storage of Papers** .......................................................................................................... 27
11. **Disposal of Electronic Information** ................................................................................ 27
12. **Disposal of Papers** ........................................................................................................ 27
13. **Review** ............................................................................................................................ 27
14. **Freedom of Information Requests** .................................................................................. 27
15. **Reporting Procedures** .................................................................................................... 28
1. MASH Information Sharing Process Document

This guidance document should be read in conjunction with the MASH Information Sharing Agreement and the MASH Information Sharing Guidance document.

This document is to provide detailed guidance to the employees working with partner agencies signed up to the MASH Information Sharing Agreement.

2. Business Continuity

All partners to this agreement will provide a list of contacts to deal with queries and requests for information under this agreement. The organisations will also nominate persons to act as the contact to ensure continuity in the absence of the original points of contact.

If secure email is not available, then information will be shared via hand or fax. All information will be recorded centrally in the MASH on CareFirst/Totalview. However, other agencies can and are encouraged to keep their own records so that each organisation is aware of which and how its information is being used.

3. Confidentiality and Vetting

The information to be shared under this agreement is classified as ‘RESTRICTED’ under the Government Protective Marking System. Vetting is not mandatory to view this grade of information; however staff working within the MASH environment will either be vetted to CTC level or have an ‘Enhanced’ DBS check. What is required at ‘RESTRICTED’ level access is a strict ‘need-to-know’ the information, which all staff viewing shared information must have.

Signatories to this agreement agree to seek the permission of the originating agency if they wish to disseminate shared information outside of the MASH environment. Such permission will only be granted where proposed sharing is within the agreed principles: i.e. for safeguarding and supporting the wellbeing of children or for policing purposes, (page 9).

4. Compliance

All signatories to this agreement accept responsibility for ensuring that all appropriate security arrangements are complied with. Any issues concerning compliance with security measures will form part of the annual review of this agreement.

5. Sanctions

Any unauthorised release of information or breach of conditions contained within this agreement will be dealt with through the internal discipline procedures of the individual partner agency.
Non-compliance and/or breaches of the security arrangements with regards to police information will be reported to the MPS Borough and reviewed with regards for any risk in the breach.

All parties are aware that in extreme circumstances, non-compliance with the terms of this agreement may result in the agreement being suspended or terminated.

6. Training / Awareness

All partners will hold a copy of this agreement. It is the responsibility of each partner to ensure that all individuals likely to come in contact with the data shared under this agreement are trained in the terms of this agreement and their own responsibilities.

7. Partner’s Building and Perimeter Security

Information will be stored in secured premises, e.g. not in areas where the public have access.

8. Movement of Information

Information will be sent and received electronically to ensure there is an audit trail of its movement.

Any e-mail communication will be by way of secure, appropriate and approved methods. The sharing of information must be done via secure email, meaning only email addresses with .pnn, .gcsx, .cjsm, .gsi and nhs.net or egress will be used.

9. Storage of Information on Partner’s System

The MASH enquiry records will be stored on the CSC system; CareFirst & MASH Totalview. However, other agencies may be passed information from the MASH case record where appropriate for further interaction with a child, which may also be stored electronically.

All Signatories to this agreement confirm that there are adequate security measures on their electronic systems that information from partners may be transferred to. Information can only be accessed via username and password. Partners confirm that permission to access to MASH information held electronically by partners will be granted on a strict ‘need-to-know’ basis once it is contained within partners’ electronic systems.

10. Storage of Papers

It is not the intention of this agreement that information will be produced in a hard format. If information is printed off an electronic system, it will be the partner’s responsibility to keep the information secure by measures such as storing documents in a locked container when not in use. Access to printed documents must be limited only to those with a valid ‘need to know’ that information. There should also be a clear desk policy and particular information from any agency is only assessed when needed and stored correctly and securely when not in use.
11. Disposal of Electronic Information

Once information contained within emails is transferred to partner’s electronic systems, the emails will be deleted.

Information will be held in electronic systems until the information is no longer required. Information provided as part of this agreement will be the subject of review by the partner agencies. Information will be destroyed in accordance with each agencies code of practice in handling information and with regards to their responsibilities under the Data Protection Act.

If information is stored by partners electronically on their systems, information must be overwritten using an appropriate software utility e.g. Norton Utilities or CD discs physically destroyed.

12. Disposal of Papers

As mentioned previously, it is not the intention of this agreement that information will be produced in a hard format. If information is printed off an electronic system, it will be the partner’s responsibility to dispose of the information in an appropriate secure manner i.e. shredding or through a ‘RESTRICTED’ waste system, once it is no longer needed.

13. Review

The arrangements held within this document will be reviewed initially after six months and then annually thereafter.

14. Freedom of Information Requests

This document and the arrangements it details will be disclosable for the purposes of the Freedom of Information Act 2000 and so will be published within the signatories’ Publication Schemes.

Any requests for information made under the Act that relates to the operation of this agreement should, where applicable, be dealt with in accordance with the Code of Practice under S.45 Freedom of Information Act 2000.

This Code of Practice contains provisions relating to consultation with others who are likely to be affected by the disclosure (or non-disclosure) of the information requested. The Code also relates to the process by which one authority may also transfer all or part of a request to another authority if it relates to information they do not hold.

15. Reporting procedures

There needs to be an agreed procedure for using non-anonymised information for service planning, commissioning, statutory returns and review, either:

- The parties will anonymise information before they make it available for service planning, commissioning, statutory returns and review purposes; or
• Sharing information for service planning, commissioning, statutory returns and review purposes will follow the local procedure, which should have been approved by the Parties’ respective Caldicott Guardians, data protection officers or equivalent.