ISA Ref:

Purpose Specific Information Sharing Agreement

Version 7 - October 2019

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

Freedom of Information Act Publication Scheme	
Protective Marking	Not Protectively Marked
Publication Scheme Y/N	Yes
Title	A purpose specific information sharing agreement documenting sharing within Merton MASH
Version	7
Summary	An agreement to formalise information sharing arrangements within Merton MASH, between London Borough of Merton Children's Services, Merton Borough Police, Central London Community Healthcare NHS Trust, NHS South West London & St George's Mental Health Trust, St George's Healthcare NHS Trust, Merton Clinical Commissioning Group, Merton General Practices, Epsom & St Helier NHS Trust, London Probation Trust, London Community Rehabilitation Company and Merton Voluntary Service Council for the purpose of identifying and assessing risks to children's wellbeing and welfare in the borough. WDP and Victim Support
Author	Nicole Miller Updated by Helen Smith February 2020
Date Issued	October 2018
Review Date	October 2020

Generic guidance document:

Protective marking	Not Classified
Suitable for Publication Scheme Y/N	Y
Purpose	Generic guidance document for use by boroughs engaged in the MASH project
Author	MASH ODG
Date created	October 2018
Review date	2 years

Contents

Section 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, probation, voluntary agencies 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:

1. **Information Sharing: Guidance for practitioners and managers (2008)**

Information Sharing: Further guidance on legal issues (2009) 3 United

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 Data Protection Act 2018 identifies six key principles in relation to the sharing of personalised data.

The London Child Protection Procedures and Working Together to Safeguard Children (2018) should also be viewed as useful guidance in this area.

<u>Scope of the Agreement</u>

This agreement is endorsed by the Multi–agency signatories identified in Section 5 (page21) 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:

1. Facilitate the sharing of information in accordance with this agreement.

2. Ensure that staff are fully aware of the process for information sharing and will comply with all legal requirements.

3. Ensure information held is kept secure at all times.

Section 2: Specific purpose for sharing information

For many years, the sharing by police of appropriate information about children who come to their notice with local authority social services has been vital in ensuring that as far as is possible the welfare of children is safeguarded. Research and experience has demonstrated the importance of information sharing across professional boundaries.

The Children Act 2004 emphasises the importance of safeguarding children by stating that relevant partner agencies - which include the police, children's services authorities, NHS bodies and others must make sure that functions are discharged having regard to the need to safeguard and promote the welfare of children. The Act also states that they must make arrangements to promote co-operation between relevant partner agencies to improve the well-being of children in their area. Well-being is defined by the Act (and was rephrased into 'outcomes' in the 2004 Government policy 'Every Child Matters') as relating to a child's:

- physical and mental health and emotional well-being ('be healthy');
- protection from harm and neglect ('stay safe');
- education, training and recreation ('enjoy and achieve');
- the contribution made by them to society ('make a positive contribution');
- Social and economic well-being ('achieve economic well-being').

"Children" in terms of the scope of this Act means all children and young people up to the age of 18.

Information upon which safeguarding decisions in relation to children and young people are made are held by numerous statutory and non-statutory agencies. Many sad cases across the UK have highlighted deficiencies within safeguarding partnerships in relation to the sharing of information and communication. Some serious case reviews and inquiries (such as the Laming, Bichard and Baby P inquiries) have directly attributed the lack of good information sharing and communication to the subsequent death of an individual.

In order to deliver the best safeguarding decisions which ensure timely, necessary and proportionate interventions, Decision Makers need the full information picture concerning an individual and their circumstances to be available to them. Information viewed alone or in silos may not give the full picture or identify the true risk.

As such all the information from various agencies needs to be available and accessible in one place. A Multi Agency Safeguarding Hub (MASH) helps ensure this and aids communication between all safeguarding partners. By ensuring all statutory partners have the ability, confidence and trust to share information, those who are subject to, or likely to be subject to, harm can be identified in a timely manner, which will keep individuals safe from harm and assist signatories to this agreement in discharging their obligations under the Act.

MASH helps deliver three key functions for the safeguarding partnership;

- Information based risk assessment and decision making

Identify through the best information available to the safeguarding partnership those children and young people who require support or a necessary and proportionate intervention.

- Victim identification and harm reduction

Identify victims and future victims who are likely to experience harm and ensure partners work together to deliver harm reduction strategies and interventions.

- Coordination of all safeguarding partners

Ensure that the needs of all vulnerable people are identified and signposted to the relevant partner/s for the delivery and coordination of harm reduction strategies and interventions.

The MASH model was highlighted in the Munro Report into Child Protection (http://www.education.gov.uk/munroreview/downloads/8875_DfE_Munro_Report_TAGGED.pdf) as an example of good practice in multi-agency partnership working because of how it improved information sharing between participating agencies.

There were two Multi agency Conferences in 2011 and 2012 at City Hall with Senior Police, Boroughs, Probation and Health agreed on an information sharing approach. Governance is retained by the LSCB.

The aim of this information sharing agreement is to formally document how, through the MASH set-up, the signatories to this agreement will share information about children who have come to the attention of their organisation for failing at least one of the five outcomes listed above on the previous page.

This agreement does not cover other information sharing arrangements between the signatory agencies that takes place outside of the MASH - these will be covered (where appropriate) by separate information sharing agreements.

<u>Data Controller – Relationships of MASH</u>

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 2018 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.

Section 3: **Legal Basis for Sharing Information and what specifically will be shared**

DPA 2018 First principle – fair lawful and transparent processing – (processed fairly and lawfully and in a transparent manner)

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.

The nature of the information that will be shared under this agreement will often fall below a statutory threshold of S.47 (child protection investigation) or even S.17 Children Act 1989 (Child in Need). If they do fall within these sections of the 1989 Act, then these will be the main legal gateway. However, in addition the LCCP provide guidance and a legal gateway to share without agreement/consent under 'legal obligation' or public task. Privacy notices should be available to families to ensure they are aware of how their data will be used and shared under this legislation.

Sections 10 and 11 of the Children Act 2004 place obligations upon the police, local authorities, NHS bodies and others 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. This piece of legislation gives the statutory power to share information for the purposes of this agreement.

Although the Data Protection Act 2018 does not give a power to disclose information, it does 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 reasons listed above, organisations are then exempt from the usual non-disclosure provisions and may provide the information requested / they wish to proactively share without agreement. This will be decided and recorded though on a case-by-case basis.

Data Sharing

The parties to this Protocol acknowledge and agree that any sharing and processing of personal data or sensitive personal data (as defined in the Data Protection Act 2018) in connection with this Protocol and/or Operation Encompass shall be performed strictly in accordance with all relevant data protection legislation and, further, each party shall only share or process such information pursuant to the terms of an information sharing agreement (ISA).

If any party believes it is not already subject to an applicable ISA it shall inform the relevant disclosing party as soon as it is aware and shall not process such data until it is demonstrates to the disclosing party that it is a signatory to an approved ISA.

Duty of Confidence

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 the 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, it will undergo an assessment check against criteria (included in Child Abuse Investigation Command Standard Operating Procedures) by the MASH Public Protection Desk (MASH PPD). Whilst still applying proportionality and necessity to the decision, 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.

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 agreement has been provided or where there is a strong enough public interest to do so.

Obtaining agreement to share information remains a matter of good practice and, in circumstances where it is appropriate and possible, explicit agreement should be sought and documented from and freely given by the data subject.

However, in many cases the aims of the MASH might be prejudiced if agencies were to seek agreement. In such cases, the disclosing agency must consider whether it is possible to disclose personal information without agreement. It is possible to disclose personal information without agreement if this is in 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 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?

The rule of proportionality should be applied to ensure that a fair balance is achieved between the public interest and the rights of the data subject. This should balance the above factors in conjunction with the wishes of the data subject and the wider public interest.

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

All disclosures must be relevant and proportionate to the intended aim of the disclosure.

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. cooperation to improve 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.

If possible, agreement will be obtained by Children's Services before the case of individuals are brought to the MASH. In these cases, individuals will have a legitimate expectation of how their data is going to be used and with whom it may be shared and why. Agreement is obtained verbally and is recorded on the Social Care system.

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 is in addition to the ready availability of the Fair Processing Notices.

Human Rights - Article 8: The right to respect for private and family life, home and correspondence

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.

The sharing of the information with children's services may be in contravention of Article 8 (sub section 1). However, the benefits of an effective sharing of information for the purposes set out in this agreement are to the direct benefit of the citizen and so in the public interest; this will be considered on a case by case basis.

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 European Convention on Human Rights 1998, namely the right to life and the right to prohibition of torture or inhuman or degrading treatment. Where sharing of information takes place, there will be consideration of these articles.

Proportionate –

The amount and type of information shared will only be the minimum necessary to achieve the aim of this agreement. This will be the current presenting issue why the family have come to notice of social care.

Information is always to be considered in terms of its relevance and proportionality in each set of circumstances, but it must always be remembered that the right to life is paramount and an absolute right.

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 NHS bodies and Children's Services also have similar obligations, which are necessary and appropriate in a democratic society.

Please see appendix 3 for details of the 'conditions for processing personal data'.

Fair Processing

- Fairness rests on whether the data subject was deceived or misled as well as whether information was provided about how data will be processed by the signatories to the ISA.

- Signatories agree to ensure that privacy notices (i.e. Being transparent and providing accessible information to individuals about how you will use their personal data) include details of the information sharing described under this ISA and that they satisfy the recommendations of the Information Commissioner's Office Guidance.

- Signatories agree to consider whether obtaining the agreement of the data subjects is appropriate in each case at hand. Agreement for MASH checks is obtained verbally.

- Order 2000, SI 2000/417 provides that, disclosures may be lawfully made where obtaining consent would prejudice the public interest or the prevention or detection of a lawful act as detailed above. Signatories agree that such decisions will be appropriately considered by the MASH Decision Makers, where any decision made to override consent will be proportionate and clearly recorded on the Children's Social Care record.

- Reference to fair processing notices is also contained within the LCCP guidance at http://www.londoncp.co.uk/.

The local authority will publish a service specific MASH Privacy Notice to be read alongside the local authorities unified corporate Privacy Notice, partner organisations will all publish a Unified or service specific 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 councils website; www.merton.gov.uk/mash.

DPA 2018 Second Principle – Purpose Limitation (collected for specified, explicit and legitimate purposes)

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.

All information will only be used within the MASH for the purposes of safeguarding the vulnerable and reducing harm, which is compatible with the reason it was originally collected.

Signatories agree that information shared under this agreement will be used solely for the purposes identified and that any further processing will be compatible with the identified purposes.

DPA 2018 Third Principle – Data Minimisation – (the purpose limitation principle states that personal data collected for one purpose should not be used for a new, incompatible, purpose)

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is 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 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)
- Relevant information obtained from GP and Health records
- Relevant ASB 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. The personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed.

Signatories agree to consider and document the minimum necessary data set to achieve the purposes of the agreement for each sharing decision **at hand**. This should include consideration of how each piece of information would support the lawful basis and how removal of data might prejudice the purposes for sharing.

DPA 2018 fourth Principle – Accuracy – (data must be accurate and kept up to date)

Personal data shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are either erased or rectified without delay

All the information supplied will be obtained from signatories' computer systems or paper records and subject to their own organisations reviews, procedures and validation. Where information shared has been found to be inaccurate or out of date, signatories agree to promptly alert sharing partners to allow for review, amendment and incident management.

Whilst there will be regular sharing of information, the data itself will be 'historic' 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.

Signatories agree to take all reasonable steps to ensure information shared and recorded is a statement of fact and the data is accurate and up to date.

DPA 2018 fifth Principle – Retention

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. There are specific provisions on the processing of personal data for historical, statistical or scientific purposes.

The data will be kept in accordance with signatories' file retention and destruction policies. 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 historic information for risk assessment purposes. However, once information is no longer needed, it should be destroyed. The principle should be read in light of the "right to be forgotten" under which data subjects have the right to erasure of personal data, in some cases sooner than the end of the maximum retention period.

For the avoidance of doubt, this principle relates to information shared for the purpose of this Information Sharing Agreement and not as to each organisation's retention policy. If the information shared for the purpose of this agreement is no longer required, then it should be destroyed. If in some cases it may be information which a party would normally hold, then it would fall under that organisation's retention policy.

Please note, personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Signatories agree to maintain a records retention schedule in accordance with the necessary legal framework and to de-identify records where lawful and appropriate.

DPA 2018 Sixth Principle – Data Security

Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Signatories agree to transfer information using secure and approved methods such as secure email (nhs.net, egress, office 365 secure email etc.). If secure email is not available, then information will be shared via hand or telephone and contemporaneously recorded in the MASH system.

Signatories agree to ensure that all staff sharing information under this agreement have been provided with a copy and have sufficient training in respect to discharging the agreed procedures.

Signatories agree that appropriate access control and audit procedures will be put in place to prevent unauthorised access to information shared under this agreement.

Signatories agree that information incidents related to information shared under this agreement will be managed according to internal procedures and that relevant updates and lessons learned will be shared with the signatories.

Signatories agree to ensure that all employees have employment or other relevant contract clauses that include confidentiality and the necessary sanctions for a breach of confidentiality.

Sharing Protocol

1. Signatories agree to consider the necessary privacy law framework when making a request or agreeing to share information under this agreement.

1. Signatories with direct access to source systems such as GP systems, agree not to directly access the records held in those systems without the approval of the Data Controller (please see appendix 1).

2. Signatories agree to respond within the timescales outlined below to requests and to collaborate with other signatories to support the intention of this agreement in safeguarding the rights and wellbeing of children.

3. Where possible, the signatory releasing information shall be provided with the rationale for the request for information to support their decision to share information under this agreement.

4. Dissemination of information shared under this agreement beyond the MASH environment shall be for the purposes identified under Section 5 of those compatible with them and will be completed with proper consideration of privacy law.

Agreement Governance

1. This agreement will be reviewed annually or sooner in response to an incident or as agreed by the signatories.

2. The signatories agree to meet if required to discuss information sharing under this agreement and the meetings will include discussion of; lawfulness, proportionality, fairness, incidents, legislation change, incidents, complaints, technical and organisational measures in place to protect the data.

Section 4: Description of arrangements including security matters

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 (ie 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 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 with the First Contact Officers in the MASH to see if there is an open case on the Children Services' database Mosaic. Where there is, they will forward the PAC straight on to the MASH referral inbox, whereby the manager will mark the contact as OPEN.

Business Support Staff will then send it on to the responsible case-worker and team. 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 via secure email to the MASH referral co-ordinator.

Upon receiving this information, the MASH Manager or ATM will give a BRAG Rating to the Contact, Business Support will create a contact and assign to the manager to for case direction.

The manager /ATM will assign case directions and pass Contacts with a BRAG of Red or Amber to the senior social workers. If possible, agreement will be obtained by the social worker before the case of individuals are brought to the MASH. In these cases, individuals will have a legitimate expectation of how their data is going to be used and with whom it may be shared and why. Agreement is obtained verbally and is recorded on the Social Care system.

Contacts with a Blue or Green Contact gets passed to the First Contact officers with case directions by the Manager / ATM.

Using the collated police and council information, a screening of the contact will be undertaken to see if the child is suitable to be considered for a MASH checks to assist with a multi-agency risk assessment. This will be clearly recorded on Mosaic. Upon completion of either a screening of the contact or completion of the MASH referral when all information has been received back and analysed the decision will be taken as to what may be the most suitable course of action. Relevant information will then be passed on to agencies on a 'need-to-know' basis when interacting with that child.

Information entering the MASH from non-police sources:

Information about a child where there are concerns about their welfare will be passed to the MASH referral inbox.

Similar to the police process, the Duty Social Worker / ATM / Manager will check to see if there is an open case, and if so, it will be marked as "Open" and Business Support will forward that information on to the relevant case-worker and

team. Where there is not an open case, the managers will apply a BRAG rating proportionate to the MWBM threshold document whereby Business Support will create all family members and create a contact on the youngest child.

The Manager / ATM will give the initial case directions, assign Contacts with a RED and AMBER BRAG to senior social workers and Blue and Green Contacts to First Contact Officers.

Before considering if the case should continue though the MASH process, the Practice Manager 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 sergeant and an investigation started.

This needs to be done on a case by case basis and is not a standard rule for every case received from a non-non police source

A decision will then be taken as to whether action can be taken by the MASH then or they should wait for the conclusion of the police investigation.

There will be instances whereby the police may decide a crime has been committed, however as social care has to work with the family the police cannot refuse to complete research when a MASH check is requested.

MERTON Timescales

Red: 2hours

Amber 6 hours

Green 24 hours

Rights of data owner and confidential information – 2nd & 3rd Core elements of a MASH

MASH is a confidential 'fire walled' environment and access to it should only be by those authorised to work within it for the purpose of information sharing in order to assess referrals and make decisions.

Information in a MASH must be classed by the organisation providing it as either confidential or non-confidential. Both types of information will be revealed within the hub to the MASH Manager/Decision Maker in order they can see the full information picture upon which to make a decision. Only the data owner and the MASH Practice

Manager/Decision Maker for a given case should be able to see information provided for the purpose of supporting assessment decisions.

MASH operates a core principle that any organisation revealing confidential and non-confidential information within a MASH for the purposes of MASH assessment will always retain the duty of care over the data and remain the data owner.

In practice, this means the organisation owning the information or data owner has the right to decide not to allow information to leave the MASH after assessment if they believe it to be of a confidential nature and are not prepared to have it shared openly. This decision which can be discussed with the MASH Team Manager on a case by case basis remains at all times with the data owner and must be recorded.

MOSAIC makes provision for agencies to decide whether they want information to be confidential or not

In the case of an unresolved disagreement in relation to information sharing, the designated safeguarding person for the service will be informed.

Should information be held back within the MASH at the request of a data owner it must be clearly signposted on any document leaving the MASH in order that operational staff become aware at the earliest opportunity that it exists and who/where they can approach to discuss it further. The information can then be discussed in confidence between the data owner and operational staff on a clear 'need to know' basis.

Please note that information shared by partner agencies is for MASH risk assessment purposes only and is not to be used for any subsequent assessments outside the MASH process and not to be released without the express permission of the data holder.

Requests for data from MASH records

Should information be requested from MASH records by way of any judicial process the original data owner must be advised and requested to decide on disclosure or not and manage any specific process required to protect confidential information and its sources. Legal advice should be sought at the earliest opportunity.

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 (or orally, and recorded contemporaneously in the MASH).

All information will be recorded in the MASH on the Children's System . However, other agencies can and are encouraged to keep local records so that their organisation is aware of how its information is being used.

Confidentiality and Vetting

The information to be shared under this agreement is classified as 'RESTRICTED' under the Government Protective Marking System (GPMS). 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 will be DBS vetted. What is required at this 'RESTRICTED' level access is a strict 'need-to-know' attitude towards practice within the MASH and all information and intelligence.

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 policing purposes, safeguarding and supporting the wellbeing of children.

In the event of the data holder wishing to seek advice prior to the release of information when agreement has been overridden within MASH, the designated safeguarding professional for the organisation is informed. If that designated safeguarding professional is unavailable, then the CCG safeguarding team will be made aware for advice purposes prior to them seeking legal advice.

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.

Signatories shall have in place throughout the period of the agreement an Information Security Management Procedure and shall ensure that all relevant employees are made aware of and trained in regards to the Procedure.

Signatories undertake within twenty-four (24) hours, to notify the other partner bodies of any information security breach and/or any breach of the obligations pursuant to the DPA and/or the GDPR, together with the steps the partner body who suffers the breach shall take to rectify the breach and to avoid any future such breaches occurring.

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.

Non-compliance and/or breaches of the security arrangements with regards to police information will be reported to the relevant MPS Borough Operational Command Unit 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.

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.

Partner's building and perimeter security

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

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 any information must be done via secure and encrypted email examples include pnn, .gcsx, .cjsm, .gsi and nhs.net, egress. This is not an exhaustive list.

Storage of information on partner's system

The MASH case records normally will be stored on the relevant Integrated Children's System . Other secure solutions might be used locally; however, other agencies may be passed information from the MASH case record if approved by the original data owner where appropriate for further interaction with a child, which may also be stored electronically on Mosaic or other partner agency systems.

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 of an electronic system, it will be the partners' 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 were MPS information in particular is only assessed when needed and stored correctly and securely when not in use.

All signatories to this agreement confirm that there are adequate security measures on their electronic systems that information from partners may be transferred (but only on a strict need-to know basis). 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.

Disposal of electronic information

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

Police and probation return checks via email which is uploaded via the social workers / FCO's under their table on the MASH return checks

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.

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, it will be the partners' responsibility to dispose of the information in an appropriate secure manner (i.e. shredding, through a 'RESTRICTED' waste system) once it is no longer needed; and record the fact that the hard copy has been destroyed.

Reporting Procedures

There needs to be an agreed procedure for using identifiable 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.

For further information regarding MASH processes, please refer to the LSCB website.

Review

The arrangements held within this document will be reviewed every two years

Freedom of information requests

This document and the arrangements it details will be disclosed 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.

Data subject rights

Irrespective of the terms of this Specific Agreement, a data subject may exercise his or her rights under data protection legislation in respect of and against each of the named Parties. For example, if a data subject wishes to delete or amend their records these requests will be dealt with under the provisions of the Data Protection Act 2018.

Section 5: Agreement to abide by this arrangement

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:

1. Implement and adhere to the procedures and structures set out in this agreement.

2. 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.

3. Request feedback from partners initially after 6 months from signature then a review at least every two years.

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

Agency	Post Held	Name	Signature	Date
London Borough of Merton	Chief Executive	Ged Curran		October 2020
London Borough of Merton	Director of Children, Schools & Families	Rachael Wardell		October 2020
Metropolitan Police Service, Merton borough	Borough Commander	Sally Benatar		October 2020
Merton Clinical Commissioning Group	Chair	Dr Andrew Murray		October 2020
National Probation Service	Assistant Chief Officer	Adam Kerr		October 2020
CRC	Chief Executive	Helga Swidenbank		October 2020
CLCH	Chief Executive	Andrew Ridley		October 2020
Merton Voluntary Service Council	Chief Executive	Simon Shimmens		October 2020
South West London & St George's Mental Health Trust & CAMHS	Chief Executive Service Director	David Bradley		October 2020
St George's University NHS Foundation Trust	Chief Executive	Jaqueline Totterdale		October 2020
Epsom and St Helier University Hospitals Trust	Chief Executive	Daniel Elkeles		October 2020
Merton General Practices	Chair of the LMC	Marek Jarzembowski		October 2020
Victim Support	Josephine Feeney	Josephine Feeney		October 2020
WDP	Operational Manager	Liz Campbell		October 2020