Freedom of Information Act Publication Scheme	
Protective Marking	
Publication Scheme Y/N	
Title	A purpose specific information sharing agreement documenting sharing within Southampton MASH
Version	February 2014 Version 2
Summary	An agreement to formalise information sharing arrangements within Southampton MASH, between Southampton City Council Children's Services, Hampshire Constabulary, Hampshire Probation Trust, Solent NHS Trust, University Hospital Southampton Foundation Trust, Southern Health Foundation Trust, Southampton City Clinical Commissioning Group, Southampton City Council Adult Services, Southampton City Council Housing and Southampton City Council Adult Services for the purpose of identifying and assessing risks to children's wellbeing and welfare in Southampton.
Author	
Date Issued	February 2014
Review Date	March 2015

Generic guidance document:

Protective marking	Not Classified
Suitable for Publication Scheme Y/N	Yes
Purpose	Generic guidance document for use by Agencies and organisations engaged in Southampton MASH
Author	
Date created	February 2014
Review date	*March 2015*

ISA Ref:

Purpose Specific Information Sharing Arrangement

Version 2

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

Hampshire Probation Trust
Working together to reduce offending

Solent NHS
NHS Trust

NHS
Southampton City
Clinical Commissioning Group

University Hospital Southampton NHS
NHS Foundation Trust

Southern Health NHS
NHS Foundation Trust

SOUTHAMPTON CITY COUNCIL

LSCB
Southampton
Local
Safeguarding
Children Board

HAMPSHIRE CONSTABULARY

Southampton *Voluntary* Services

Index

Section 1. Purpose of the Agreement

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 after six months initially and annually thereafter**.**

The signatories to this agreement will represent the following agencies/bodies:

1. **Director of Peoples Services, Southampton City Council**
2. **Chief Constable Hampshire Constabulary**
3. **Southampton City Clinical Commissioning Group**
4. **Southern Health NHS Foundation Trust**
5. **Solent NHS Trust**
6. **University Hospital Southampton NHS Foundation Trust**
7. **Hampshire Probation Trust**
8. **Southampton Voluntary Services**
9. **Southampton Local Safeguarding Children's Board**
10. **Caldicott Guardian**

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, Clinical Commissioning Groups and the NHS Commissioning Board - 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 as relating to a child's:

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

Although most commonly used to refer to young people aged 16 or under, 'children' in terms of the scope of this Act means those aged nineteen or under.

Information upon which safeguarding decisions in relation to children and young people are made is held by numerous statutory and non statutory agencies. Many tragic cases across the UK have highlighted deficiencies within safeguarding partnerships in relation to the sharing of information and communication. Serious case reviews and inquiries (such as the Laming, Bichard) 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 that 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 is unlikely to give the full picture or identify the true risk.

Therefore all the relevant 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 to share information, it will help to identify those who are subject to, or likely to be subject to, harm 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;

1. **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.

2. **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.

3. **Co ordination 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 co ordination 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.

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

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

Section 3. Legal Basis for sharing and what specifically will be shared

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)**
2. **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 Southampton 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.

1. First Principle[1]

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 commissioning groups and the NHS England 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

[1] In accordance with the Data Protection Act 1998

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.

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.

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.

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 may 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.

[2] "Proportionate" is the critical issue.

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 a 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.

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. 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 Hampshire Constabulary Unified Privacy Notice is published on the external Hampshire Constabulary 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 Hampshire Constabulary *may* share this information with a variety of other agencies for the purposes of Policing.

[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'.

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.

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.

In circumstances not satisfying the above, the individual should be notified at the earliest, reasonable opportunity unless reasonable steps to do so could not have been taken.

There is a difference between being aware that something may happen, and knowing that it is happening. In this case, while we should not state the obvious, a privacy notice should actively be communicated when either:

1. Sensitive personal data is disclosed/obtained

2. Intended use is unexpected or objectionable (to the subject)

3. There is an element of significant affect on the individual, from the sharing or lack of sharing or

4. The sharing is unexpected

The above applies unless an exemption to fairness applies or the sharing is a statutory obligation.

Human Rights Act 1998 - 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.

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.

Schedule 2, Data Protection Act 1998

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.]

Schedule 2, condition 6 will apply where the legitimate interests pursued by the data controllers or a third party or parties to whom the data are disclosed are cited: for example, where common law policing powers allow sharing outside of statue law. This must meet the test of being a warranted intrusion, with the interests of the data controller and recipients balanced against the rights and freedoms or legitimate interests of the data subject.

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.]

By virtue of condition 10 of Schedule 3, Statutory Instrument 417/2000 allows processing of sensitive personal data for (paragraph 1) the prevention or detection of an unlawful act where the matter is in the substantial public interest and requires that the matter is not prejudiced by seeking the consent of the data subject, and also (paragraph 10) where necessary for exercising common law policing powers.

2. 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 Hampshire Constabulary Recording Management System 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.

3. 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 ASB data*
- *Relevant data from Southampton Ambulance Service or Southampton 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.

4. 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.

5. 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[6]. 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.

6. Sixth Principle

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

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.

7. 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.

These points will be addressed in Section 4.

8. 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.

[6] See Annex A for details how this is done locally

Section 4. Description of arrangements including security matters.[7]

Business Processes

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 Child, Young Persons at Risk Report (CYPR) will be entered on to the Record Management System(RMS).

Police officers based in the MASH will review these CYPR's 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) PARIS. The police access to PARIS will only be to identify if an 'open case' exists and for no other reason. Where there is an open case, the police will forward the CYPR 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 RMS has relating to the welfare of the child. They will send the initial CYPR and subsequent research 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 PARIS and see what information the CSC hold on any Local Authority database 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 risk 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 CYPR forwarded by the MASH Police Sergeant 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 a 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 (ie, Child Protection Investigation, referral to 0-4 or 5-19 team, placement on a early intervention option etc). Relevant information will then be passed on to agencies who 'need-to-know' that information when interacting with that child.

[7] Annex A contains details of the practical arrangements made in the NHS to ensure security, around, for example, holding and storing electronic data, encryption and use of mobile devices

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 Children's Social Care and conduct a MASH risk assessment.

Before considering if the case should continue though 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 the appropriate service, passing across the relevant 'need-to-know' information.

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 PARIS. 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.

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' basis, 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).

All staff will also have signed a confidentiality statement.

Compliance

The Information Governance Lead, People Directorate, will be the Senior Information Risk Owner (SIRO) for the MASH and will ensure delivery of the requirements below. The SIRO will ensure that the necessary arrangements are in place and are being implemented by the MASH partners. Each partner agrees that they will put into effect the requirements of the SIRO in order that the following points are complied with:

1. Risk assessment of the vulnerability of the premises to burglary and theft.

2. Appropriate information security protocols are followed to protect personal data.

3. Laptop computers or other portable electronic storage devices or removable media used by staff working in the MASH are encrypted to protect any personal data processed on such devices.

4. All staff accessing information follow the principles and standards that have been agreed and incorporated within this Purpose Specific Information Sharing Agreement.

5. Staff accessing the IT systems of another agency are appropriately trained for that use.

6. The appropriate confidentiality agreement/form of undertaking has been signed by all staff working in the MASH.

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.

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 line manager and forwarded to the Hampshire Constabulary Information Assurance Team 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.

It is the responsibility of the SIRO to ensure all staff in the MASH are appropriately trained.

Partner's Building and Perimeter Security

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

Each partner reserves the right to conduct security inspections in relevant buildings.

Movement of Information

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

Any e-mail communication or electronic transfer of information will only take place of where a secure encrypted e-mail facility exists and in these cases the information will not be above the RESTRICTED marking, as defined in the Government Protective Marking Scheme (GPMS). The following are recognised encrypted secure email pathways: .PNN, .xGSI, .GSI, .GSX, .GSE, .NHS, .CJSM,.SCN and Anycoms+

Storage of Information on Partner's System

The MASH enquiry records will be stored on the Children's Services electronic recording system; PARIS.

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.

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.

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 using an appropriate secure method.

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.

Review

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

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.

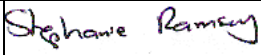
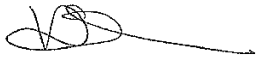
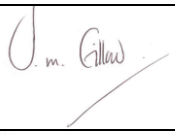
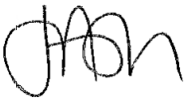
Section 5. Agreement to abide by this arrangement

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:

- 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 initially after 6 months from signature then at least annually.

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
Southampton City Council People Directorate	Director	Alison Elliott		18th February 2014
Hampshire Constabulary	Head of Public Protection Department	Detective Superintendent Nigel Lecointe		26 February 2014
Southampton City Clinical Commissioning Group	Director of Quality and Integration	Stephanie Ramsey		13th March 2014
Southern Health NHS Foundation Trust	Chief Medical Officer	Dr Helen McCormack		24th March 2014
Solent NHS Trust	Director of Nursing & Quality, Caldicott Guardian	Judy Hillier		19/02/14
University Hospital Southampton NHS Foundation Trust	Director of Nursing/OD & Caldicott Guardian	Judy Gillow		11th March 2014
Hampshire Probation Trust	Director	Maria Galovics		21.03.14
Southampton Voluntary Services	Chief Executive	Jo Ash		3rd March 2014
Caldicott Guardian	Director	Alison Elliott		18th February 2014
NHS England (Wessex ARFG Team)	Assistant director of Nursing	Nicky Preist		21st March 2014

Annex A: guidance on handling information in the MASH from an NHS point of view

Version	2
Date	February 2014
Author	Based on London MASH draft ISA)

1. Information entering the MASH from non-police sources

1.1 Information about a child where there are concerns about their welfare will be passed to the local authority decision maker in the MASH (i.e. the person who co-ordinates the MASH enquiry). Similarly to the police process, they will check the relevant information system (usually – but not always – the Council's Children's Services PARIS system) 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, see if there is any other relevant information held by Southampton City Council Children's Services and conduct a MASH risk assessment.

1.2 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 sergeant and an investigation started. 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.

1.3 If it is decided that the case can 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 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. For example, the contact for health is the health professional who forms part of the MASH team who will contact other health partners to obtain information to assist in the risk assessment. Once they have decided what this is, the local authority decision maker will refer the child to that service, passing across relevant information to the agency they have been referred to on a 'need-to-know'.

2. Business Continuity

2.1 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.

2.2 If secure email is not available, then information will be shared via hand or fax [or orally, and recorded contemporaneously in the MASH].

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

3. Confidentiality and Vetting

3.1 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 will be Enhanced DBS vetted. What is required at 'RESTRICTED' level access is a strict 'need-to-know' basis, which all staff viewing shared information will have.

3.2 Signatories to this Information Sharing Agreement agree to seek the permission of the originating agency if they wish to disseminate shared information outside 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.

4. Movement of Information

4.1 Information will be sent and received electronically to ensure there is an audit trail of its movement. All information shared over the phone should be recorded contemporaneously in the MASH records.

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

5. Storage of Information on Partner's System

5.1 The MASH case records normally will be stored on Southampton City Council PARIS system. 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.

5.2 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.

6. Storage of Papers

6.1 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 where MPS information in particular is only assessed when needed and stored correctly and securely when not in use.

7. Disposal of Electronic Information

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

7.2 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.

7.3 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

8. Disposal of Papers

8.1 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 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.

9. Reporting procedures

9.1 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.