

Information Sharing Agreement

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 RBWM MASH
Version	One
Summary	An agreement to formalise information sharing arrangements within RBWM MASH, between Royal Borough of Windsor & Maidenhead, Thames Valley Police, Berkshire Healthcare Foundation Trust, and The Dash Charity for the purpose of identifying and assessing risks to children's wellbeing and welfare in the area.
Author's	Detective Inspector Jackie Phillips/Fiona Watton RBWM
Date Issued	11/5/01/2016
Review Date	Annually from date of issue

Generic guidance document:

Protective marking	Not Classified
Suitable for Publication Scheme Y/N	Y
Purpose	Generic guidance document for use by agencies engaged in the MASH project
Authors	Detective Inspector Jackie Phillips/ Fiona Watton RBWM
Date created	Finalised – 11 th January 2016 (V3)
Review date	1 year from date of issue

Purpose Specific Information Sharing Arrangement

Sharing of Information within the Royal Borough of Windsor & Maidenhead (RBWM) Multi Agency Safeguarding Hub (MASH) to assist in identifying and assessing risks to children's wellbeing and welfare in RBWM.

Version Record

Version No	Amendments Made	Authorisation
2	6 th November 2015	RBWM MASH Strategic Project Board
3	11 th January 2016 (V3)	RBWM MASH Strategic Project Board

Index

Section 1. Purpose of the agreement Page 5

Section 2. Specific Purpose for sharing Page 6

**Section 3. Legal Basis for Sharing and
Specifically what is to be
Shared Page 8**

**Section 4. Description of Arrangements
including security matters Page 17**

Section 5. Agreement Signatures Page 21

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. Royal Borough of Windsor & Maidenhead
2. Thames Valley Police
3. Berkshire Healthcare Foundation Trust
4. The Dash Charity
5. Caldicott Guardians
6. Probation

Section 2. Specific Purpose for Sharing Information

The sharing of appropriate information between agencies about children who come to notice within a local authority area is vital in ensuring the welfare of those 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. Safeguarding and promoting the welfare of children is defined within the “Working Together to Safeguard Children” guide to inter-agency working 2013, as:

- Protecting children from maltreatment.
- Preventing impairment of children’s health or development.
- Ensuring that children grow up in circumstances consistent with the provision of safe and effective care; and
- Taking action to enable all children to have the best outcomes.

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 under the age of eighteen.

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 and Bichard reports) 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 to safeguard children and promote their welfare and well-being.

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.

The primary Information Sharing Protocol between agencies involved in the safeguarding of children within RBWM is contained in the Berkshire Local Safeguarding Children Board (LSCB) Child Protection Procedures 2014. The LSCB document should be seen as the over-arching agreement for all agencies within the Royal Borough of Windsor and Maidenhead. This document has been produced to guide information sharing within MASH.

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

HM Government has published an updated guidance document which should be read in conjunction with this agreement as an invaluable resource for all safeguarding professionals;

- **Information sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers (2015)**

This document 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**' as set out in the **Information Sharing; Guidance for practitioners and managers** as a practical exposition of the law relating to information sharing.

The LSCB Child Protection Procedures 2014 should also be viewed as useful guidance in this area and contains the overarching principles.

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

The 7 Caldicott Principles must also be adhered to for a MASH to be lawful.

1. First Principle¹

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

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

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

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

Section 10 and 11 of the Children Act 2004 create a 'permissive gateway' for information to be shared in a lawful manner. Such information sharing must take place in accordance with statutory requirements pertaining to the disclosure of information

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 amount to a legal obligation to disclose information, it does however provide for a power to share information 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 on individual agencies' systems.

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 within the MASH ensuring that any information shared is necessary and proportionate to the overall aim of safeguarding children.

Health patients have an expectation that their information will be kept confidential. Any subsequent sharing of this information must be assessed against the Caldicott principles and information sharing criteria to make a proper judgement. Any decision to share or not share must be recorded in the original records.

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 is 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 Children Act 1989 (child protection) thresholds do not determinate whether or not consent should be sought within MASH.

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

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

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

The Public Interest Criteria include:

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

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

- i) Is the intended disclosure proportionate² 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?

² "Proportionate" is the critical issue.

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

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

Once a decision is made by the Local authority decision-maker based on this shared information picture they, 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.

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 is a relatively closed and controlled environment and this is one factor a practitioner can consider when determining what is proportionate to share with or without consent on a case by case basis. It is not however a single overriding reason in the determination of consent.

All disclosures must be relevant and proportionate³ to the intended aim of the disclosure.

Further disclosure and use of information shared between agencies in the MASH

All staff are reminded that information shared within the MASH is done so for specific purposes relating to the safeguarding of children. Any further use of that information, for example use by the police of Local Authority documentation or information in criminal proceedings would require the permission of the Local Authority to do so. Similarly Information shared within the context of the MASH cannot be disseminated further without reference to the relevant partner agency. Please refer to the Thames Valley Disclosure Protocol which sets out the procedures to follow where criminal proceedings are contemplated or post charge.

The consent of the maker of any document or subject to any document likely to be disclosed will be sought in all cases, unless impracticable or a decision has been made not to seek consent. If such a decision is made, it must be based on legal advice and recorded in writing. Practitioners are reminded that the Article 8 Right to Privacy is 'person specific' and consideration should always be given, where age appropriate, to obtaining the consent of the child.

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

Fair Processing

The Data Protection Act 1998 requires the fair processing of information unless an exemption applies. In particular, fairness involves being open with people about who is processing their data and how their data is being used. Put simply, a data subject should not be 'surprised' by their information being shared under this agreement, where the data controller has had reasonable opportunity to inform them of this. For the purposes of the MASH, all agencies party to this agreement will ensure that their own organisation's Fair Processing Notices contain:

- (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 Fair Processing Notices of each MASH partner will be made available to the public in line with individual organisational practices.

Section 29 of the Data Protection Act 1998 provides authority 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 information by police fulfils a policing purpose, as defined in the Statutory Codes of Practice on the Management of Police Information and Authorised Professional Practice, 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 (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.

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 benefit⁴ 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.

An activity appropriate and necessary in a democratic society –

All agencies within the MASH are obliged to do all that is reasonable to ensure the welfare of the most vulnerable and this is something that is 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.

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

⁴ Benefit does not always equate to real public interest, and when it does, it still has to be 'proportionate'

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 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 7.1(b), ‘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, Police Act 1997.

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

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.

Information exchanged under this agreement will not be processed in a manner incompatible with the second principle. Each agency involved in the MASH will collect information for specified purposes; all information will only be used within the MASH for the purposes of safeguarding the vulnerable and reducing harm.

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 South Central Ambulance Service or Berkshire 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. 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 having taken into account any statutory retention periods.

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.

If a party to this agreement receives a subject access application under section 7 of the Data Protection Act 1998 and personal data is identified as having originated from another signatory partner, it will be the responsibility of the receiving agency to contact that partner to determine whether the latter wishes to advise use of any statutory exemption under the provisions of the Data Protection Act 1998, or to consider further sharing on live matters.

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.

Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to-

(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and

(b) the nature of the data to be protected.

Measures to satisfy the Seventh Principle, with regard to security, will comply with the published security policies and procedures of every MASH organisation, e.g. for RBWM they can be found at:

http://www3.rbwm.gov.uk/info/200133/strategies_plans_and_policies/116/information_security.

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.

Section 4. Description of arrangements including security matters.

Business Processes

Everyone who works within government has a responsibility to respect the confidentiality and integrity of information they access and must safeguard it in line with the Government Security Classification policy. The majority of information shared via the MASH will be classified as 'Official'.

Information entering the MASH

Not all contacts received by the local authority where there are concerns about the welfare of a child/young person will be considered by the MASH. Where there is a clear child protection concern, the local authority decision maker will immediately initiate a Section 47 enquiry. Where the local authority decision maker is clear that there is no evidence of significant harm, the contact will be processed through non MASH channels e.g. single assessment, early help assessment or no further action. Only cases where more information would enable the decision maker to make a more informed and speedier decision will be taken through the MASH process.

For any case going through the MASH process, all MASH agencies will be asked to research and 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. All MASH partners whether co-located or virtual will be required to provide information to the MASH on request. The MASH contact for health will be the single point of contact for all other health professionals and will gather and collate information on behalf of all health partners to provide to the MASH. The local authority decision maker will decide the best and most appropriate assistance and interaction for the child and when referring the child on will pass any relevant MASH information to that service with the agreement of the MASH partner who has provided the 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.

All partners to this agreement, who are sending or receiving sensitive personal data electronically, must have a secure e-mail established. If secure email is not available, for example, due to technical failure, then information will be shared via hand. Fax will only be used to transfer information in circumstances of operational emergency, and only with due caution and appropriate safeguards in place. A test fax should be sent ahead of the information in question, to a named recipient who is stationed next to the destination fax machine. Confirmation of safe receipt should be sought before sending the sensitive information.

The outcome of the discussion and the decision made by the local authority decision maker will be recorded centrally on the secure MASH case note in Paris, the social care management system.

Confidentiality and Vetting

The information to be shared under this agreement is classified as 'OFFICIAL' under the Government Secure Classification (GSC). Vetting is not mandatory to view this grade of information; however all police staff working within the MASH environment will be vetted to CTC level and non police staff working in non police premises must have an 'Enhanced' DBS check. All staff accessing OFFICIAL level data must do so on a strict 'need to know' basis. Information must only be accessed by authorised staff if it is for the purposes outlined in this agreement, and necessary for the performance of these functions.

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.

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.

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. In Health this will be through the Caldicott Guardians.

Non-compliance and/or breaches of the security arrangements with regards to police information will be reported to the police information managements units and reviewed with regards for any risk in the breach. These should be reported to:

Thames Valley Police – Information.management@thamesvalley.pnn.police.uk

Royal Borough of Windsor and Maidenhead – On RBWM hyperwave as a security information incident.

Berkshire Healthcare Foundation Trust and Probation will use their normal procedures . 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 have an appropriate level of Data Protection training, and fully understand 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 information must be done via secure email, meaning only email addresses with .pnn, .gcsx, .cjsm, .gsi and nhs.net or egress will be used.

Storage of Information on Partner's System

The record of the MASH decision will be stored on the Children social care system, PARIS.

However, other agencies or services may be passed information from the MASH case record, where appropriate, when further interaction with a child is required. This information may be stored electronically within that agency or service recording systems.

All signatories to this agreement must have adequate security measures on their electronic systems that will allow MASH information from partners to be transferred to them securely. MASH information stored on partner's electronic systems must 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 accessed 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.

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.

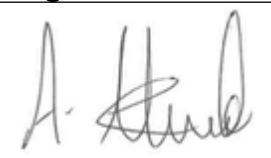

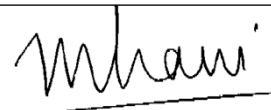
Partners to this agreement acknowledge that the wrongful disclosure of personal data (obtained under this agreement) to other organisations or persons may amount to a criminal offence under section 55 of the Data Protection Act 1998.

This agreement has been written to ensure compliance with the data protection principles and failure to abide by this agreement may lead to an organisation acting in breach of that act and thereby be subject to a penalty levied by the Office of the Information Commissioner or other litigation, and the suspension or termination of this agreement. Signatories to this agreement agree to provide the Office of the Information Commissioner with all necessary assistance in identification of the source of any breach.

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.
- Not release information to any third party, for a purpose not covered by this agreement, without obtaining the express authority of the partner.
- 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	Name / Post Held	Signature/ Comment	Date
RBWM	Alison Alexander		07/01/16
RBWM	Simon Fletcher		07/01/2016
TVP	Linda York	DCI Linda York	9/1/16
BHFT Caldicott Guardian	Minoo Irani		07/01/2016

Caldicott Guardians	Sarah Bellars Martin Tubbs	Have confirmed that signature not an issue, but have not returned it.	
DASH	Jayne Donnelly	Not Returned document.	
Probation	JOHN ENNIS	Jm Ennis	11-01-16