INFORMATION SHARING AGREEMENT

Multi-Agency Safeguarding Hub (MASH)

in Bracknell

Between: Bracknell Forest Council, Thames Valley Police, Berkshire Healthcare NHS Foundation Trust, Thames Valley Community Rehabilitation Company, National Probation Service and Berkshire Woman's Aid, collectively known as "the Parties".

PURPOSE

1. The Parties agree to enter into this Agreement for the mutual sharing of personal data as described in Schedule 2.
2. At all times the Parties agree to share data for the purpose and in the manner set out in the Code of Practice set out at Schedule 1.

LEGAL OBLIGATIONS

3. The Parties warrant that they are each registered as a data controller with the Information Commissioner's Office, and agrees to abide by the Data Protection Act, in particular the Eight Data Protection Principles.
4. The Parties agree in sharing the data as described in Schedule 2 that they will do so of their own free will and nothing in this Agreement shall cause them to breach their legal obligations.

SUBJECT ACCESS AND CONSENT

5. The Parties agree to inform data subjects whose data will be shared as per Schedule 1, noting that the data subject's consent is not required for this Agreement to be effective.
6. The Parties agree that they each have appropriate subject access regimes in place to allow data subjects access to the data that is held by each respective Party, either in their own right or in the MASH.

RETENTION OF DATA

7. The Parties agree the retention periods for the data as set out in Schedule 3, and to securely destroy data once outside of those retention periods.

SECURITY OF DATA

8. The Parties agree that they each have appropriate organisational and technical measures in place to protect the security of the data.

BREACH MANAGEMENT

9. The Parties agree that they will notify each other immediately and no later than 24 hours after discovering that data that has been shared with each other may have been breached or lost.

10. The Parties will deploy their breach management procedures to contain and mitigate such losses.

INDEMNITY

11. Subject to Clause 11.1 below, any of the Parties receiving information pursuant to this Agreement undertakes to indemnify any other parties that have disclosed such information to it against any liability, which may be incurred by the disclosing party, as a result of the receiving party breaching the terms of this Agreement in relation to that information.

11.1Provided that this indemnity shall not apply:

(a) Where the liability arises from information supplied by the disclosing party that is shown to have been incomplete or incorrect, unless the disclosing party establishes that the error did not result from any wilful wrongdoing or negligence on his part,
(b) Unless the disclosing party notifies the receiving party as soon as possible of any action, claim or demand to which this indemnity applies, giving the receiving party the sole right to defend and otherwise deal with the action, claim or demand by settlement or otherwise and renders the receiving party all reasonable assistance in connection with that;
(c) To the extent that the disclosing party makes any admission, which may be prejudicial to the defence or settlement of the action, claim or demand.

TERMINATION

12. Any Party may terminate this Agreement by giving each other one month's notice in writing.

Signed & Dated for an behalf of

Party	Name	Signature	Date
Bracknell Forest Council			
Thames Valley Police			
Berkshire Healthcare NHS Foundation Trust			
Thames Valley Community Rehabilitation Company			
National Probation Service			
Berkshire Womens Aid			

Schedule 1

Bracknell Forest Council

Code of Practice on
Sharing information in the
Multi-Agency Safeguarding Hub (MASH)

Summary

This document is the Council's Code of Practice on sharing of personal data in the MASH. It is necessary in order to demonstrate compliance with the Data Protection Act 1998. The principles are set out in Appendix 1.

It is necessary to set out general principles of how data will be shared in order to ensure that no unnecessary sharing takes place, to ensure compliance with legal obligations, to ensure good and reliable outcomes for individuals, to put into practice good information governance and to inform affected individuals of the reasons and method for sharing their data.

Guidance on MASH office security is at Appendix 2.

It is subject to annual review.

It should be read in conjunction with the Information Sharing Agreement regarding MASH entered into between all the stakeholder organisations, who are:

1. Bracknell Forest Council
2. Thames Valley Police
3. Berkshire Healthcare NHS Foundation Trust
4. Thames Valley Community Rehabilitation Company
5. National Probation Service
6. Berkshire Womens Aid

If you have any questions or enquiries about it, you can contact

Information Management and Security Officer

Information Compliance Team

Legal Services

Bracknell Forest Council

Easthampstead House

Town Square

Bracknell RG12 1AQ

E-mail: iso@bracknell-forest.gov.uk

Tel: 01344 353071

1. Deciding to share personal information

The law says:

Any information sharing must be necessary. Any information shared must be relevant and not excessive.

What the MASH does:

1. The MASH is a group of professionals from each of the stakeholder organisations. The group sit together in a room based at Easthampstead House, Bracknell. Each of the professionals has access to their own organisation's case management system. Their purpose collectively is to be the town's first point of contact for new safeguarding concerns, and by working together in a way where information flows between them, they and their organisations are able to help protect vulnerable children and adults from harm, neglect and abuse.
2. It reports to the Local Safeguarding Children Board.
3. By sharing personal data about individuals who are reported to the MASH, whether that individual is a vulnerable child, a vulnerable adult or a perpetrator who is suspected of harming or neglecting a child or adult, the organisations can work together to take action and direct the right support to those affected. Individuals can report concerns to the MASH directly, or through other sources, such as GP surgeries, schools etc. Those third party sources can also report concerns to MASH where they feel it is appropriate to do so and in line with their statutory obligations on safeguarding.
4. Whichever of the stakeholder organisations receives the information has the primary responsibility for ensuring that the data is handled properly. In particular, that organisation must make sure that sharing its information will not cause real unfairness or unwarranted detriment to individuals.
5. Each organisation will ensure that a Fair Processing Notice, which informs individuals how their data will be used and shared, exists in relation to the information they collect and share with the MASH.
6. The information that the MASH will need to share to achieve its objective will include basic personal data, for example names, addresses and dates of birth (DoB) of individuals reporting concerns, and the individuals those concerns are about. Those concerns may include much more detailed and sensitive personal data. In order to meet its objective, the information that is shared in the MASH cannot be anonymised, and must be able to identify the individuals involved and the organisations that need to be involved. However, where the objective can be achieved without personal data being shared, then this will be done. Further, the organisations within the MASH will only share data that is relevant, necessary and proportionate to its objective. This may mean that not all of the departments in the stakeholder organisations will be able to access the information.
7. Consent is covered in further detail below, please see section 2 (Fairness and Transparency) paragraph 4 onwards.
8. The Data Protection Act 1998 (DPA) restricts the sharing of data where it would be a breach of any of the eight "Principles" listed in the DPA. For sharing of data to be compliant with the Act, there are a number of conditions that must be met, this includes where it is in the data subject's vital interests to do so, or where data may be shared where there is a separate legal obligation or power to do so. These are the most relevant conditions that apply to sharing within the MASH, though are not exhaustive.

9. There are various legal obligations or statutory powers that apply to the stakeholder organisations including as follows:
    a. Children Act 2004
        i. Section 10 requires each local authority to make arrangements to promote co-operation between the authority and its partners who exercise functions or are engaged in activities in relation to children, with a view to improving the wellbeing of children, which includes protection from harm and neglect.
        ii. Section 11 places duties on organisations to make arrangements for ensuring that their functions are discharged with regard to the need to safeguard and promote the welfare of children.
        iii. Section 13 requires each local authority to establish an LSCB, and Section 14 prescribes the objectives of the LSCB, through the Local Safeguarding Children Board Regulations 2006. These include co-ordinating information to safeguard children.
    b. Borders, Citizenship and Immigration Act 2009
        i. Section 55 requires the Secretary of State to make arrangements for ensuring that functions relating to immigration, asylum, nationality and customs are discharged with regard to the need to safeguard and promote the welfare of children in the UK.
    c. Children Act 1989 (as amended)
        i. Section 27 requires organisations to co-operate with each other to provide support for children.
        ii. Section 47 places a duty on local authorities to investigate and make inquiries into the circumstances of children considered to be at risk of 'significant harm' and, where these inquiries indicate the need, to decide what action, if any, it may need to take to safeguard and promote the child's welfare.
    d. The Police Act 1996
        i. The Code of Practice on the Management of Police Information, made under Sections 39 and 39a, places a duty on Police Forces to obtain and use a wide variety of information in order to discharge their responsibilities effectively. This includes the sharing of information for the following policing purposes: Protection of Life and Property, preventing the commission of offences, and any duty or responsibility arising from common or statute law.

2. Fairness and transparency

The law says

Personal information shall be processed fairly. The processing won't be fair unless the person has, is provided with, or has readily available:

- information about your identity
- information about the purpose the information will be processed for, and
- any other information necessary to enable the processing to be fair.

What the MASH does

1. Fair processing notices, or 'privacy policies' as they are sometimes known, are intended to inform the people the information is about how it will be shared and what it will be used for. Each organisation should have a Fair Processing Notice that informs individuals how their information will be shared within the MASH. A full fair processing notice will be available on Bracknell Forest Council's website specifically within the MASH information page.
2. Each organisation's Fair Processing Notice will be freely available and genuinely informative of how information will be shared. They will be updated where necessary.
3. Each organisation will have a system in place for dealing with requests for information and enquiries about the way the data is held by them, including in the MASH.
4. 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.
5. 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.
6. 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.
7. 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.
8. BHFT will have a separate ISA with acute health and with the CCG (who will sign on behalf of primary care) to hold and proportionately share the information in the MASH.

3. Information standards

The law

Information shall be adequate, relevant, not excessive, accurate and up to date.

What the MASH does:

1. Whilst it is not always possible to check the accuracy of all information shared in the MASH, the organisations will do the following to ensure the accuracy of the information it holds.
    a. Spot checks.
    b. Inaccurate data where spotted to be corrected within a reasonable timeframe and stakeholder organisations to be informed of the same.
    c. Irrelevant, disproportionate or out-of-date data to be removed in accordance with each organisation's retention schedule.

4. Retention of shared information

The law

Personal information shall not be kept for longer than is necessary.

What the MASH does:

1. Each organisation must have a retention schedule for the type and class of data they hold and share in the MASH. The retention periods for the different types of information held, including retention times for the various items held within a record, are set out in each organisation's retention schedule.
2. The retention schedules should be reviewed organisationally annually.
3. Where information has been supplied by another organisation, each organisation must consider whether to delete the data or return it once the purpose has been met.

5. Security of shared information

The law

Personal information shall be protected by appropriate technical and organisational measures.

What the MASH does

1. Each organisation will work to adopt the ISO27001:2013 security standard and the government's protective marking scheme, or equal or greater standards, in order to keep data consistent and secure
2. Each organisation will ensure that it has appropriate organisational and technical security arrangements in place to protect the information that it has access to.
3. Each organisation is aware that where sensitive personal data is shared between parties via email, that secure encrypted email should be used, for example .gsi, .pnn, .cjsm. .Gcsx
4. The use of fax to transfer sensitive personal data should only be used in cases of operational emergency and with appropriate security safeguards.
5. Each organisation will ensure that where it shares information with another entity outside the MASH, whether it employs another organisation to process data on its behalf, or whether it outsources part of its functions to that organisation, that it will ensure that all entities that it shares data with will have appropriate organisational and technical arrangements in place to protect the information.
6. Parties to the MASH will retain Data Controller responsibility for data held on their individual agency systems and/or removable devices (to include hard copy files, USB's, laptops, tablets, and smartphones) and remain accountable for Senior Information Risk, and Information Asset Ownership for those systems/devices, and data held within.
7. Where there is a security breach, or suspected security breach, resulting in the loss, or suspected loss of any data shared in the MASH, the organisation responsible for the breach must inform the other stakeholder organisations.

8. Each organisation will have its own procedure for handling and managing security breaches. Where a breach relates to data shared in the MASH, the other organisations should participate in managing the breach where it is appropriate to do so.
9. Where necessary, the organisation will review its procedures on security and may be asked to change its procedures.

6. Access to personal information

The law

Individuals have a right of access to information about them.

What the MASH does

1. Each organisation will have a procedure by which an individual can access data that is held about themselves. Such procedure, usually called a Subject Access Request (SAR) regime, must be well-publicised. If a party to the MASH receives a SAR in relation to data held within the MASH, without it specifying data held by a particular organisation, it will be the responsibility of the receiving agency to consult with MASH partners as to the handling of the request, and whether any other party wishes to apply a statutory exemption under the Act.
2. The procedure must include the mechanism for individuals to make enquiries or to complain about the data that is held or the way in which their SAR was dealt with.
3. The procedure must indicate what exemptions are available from the right of subject access, that is, cases where information will be withheld from a person who makes a request for access. For example, where data includes third party data which cannot be separated from the individual's data, or where disclosure would cause substantial damage and distress to an individual or their physical or mental wellbeing.
4. The data that is shared in the MASH may be subject to disclosure under a SAR even where it is held by an organisation only by virtue of it having been received from another organisation in the MASH.

7. Freedom of Information

The law

The Freedom of Information Act 2000 (FOI Act) gives everyone the right to ask for information held by a public authority, to be told whether the information is held, and, unless exempt, to have a copy of the information.

What the MASH does

1. The way that the MASH works is subject to enquiries under the FOI Act. Information that is personal data cannot be disclosed under the FOI Act and is therefore subject to an exemption. Parties must be careful to handle FOI requests so that only information that is held by that organisation is disclosed.
2. Each organisation must have procedures in place for dealing with FOI requests for information about the MASH.
3. Some organisations may choose to publish this information in a Publication Scheme.

8. Review

The organisations will collectively review the sharing of information to ensure the following:

1. The sharing of information is meeting the purposes of the MASH.
2. The fair processing notices still provide an accurate explanation of the information sharing activity.
3. The procedures for ensuring the quality of information are being adhered to and are working in practice.
4. Organisations that information is being shared with are also meeting agreed quality standards.
5. Retention periods are being adhered to and continue to reflect business need.
6. Security remains adequate and, if not, whether any security breaches have been investigated and acted upon.
7. Individuals are being given access to all the information they are entitled to, and that they are finding it easy to exercise their rights.

Appendix 1 -

The data protection principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless;

    (a) at least one of the conditions in Schedule 2 is met; and

    (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. 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.

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

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

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

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

7. 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.

8. 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 for the rights and freedoms of data subjects in relation to the processing of personal data.

Schedule 2 [*to be confirmed by business process]*

Bracknell MASH to partner agencies:	**Family Composition and Identifying Details:** For each member of the household: • Forename • Surname • Date of Birth • Address **Significant person not in the household:** For each person: • Forename • Surname • Date of Birth • Address **Presenting Problem** Details of the concern raised **Feedback to referrer** **Outcome of the enquiry – only to professionals or if the referrer has parental responsibility – outcome does not include analysis of the case or information shared by partner agencies:** • Checks were completed and signposted referrer to community resources • No Further Action • Transferred to Access and Assessment • Transferred to Early Help
Information to Bracknell MASH from partner agency:	**Whether Child/ Family/ Significant Person Known to agency** **Concerns identified in relation to safeguarding enquiry**

Schedule 3 [*to be confirmed – work ongoing to resolve]*

<table>
<tr>
<td>Bracknell Forest Council</td>
<td>Children in Need 6 years unless CP
CP & LAC 100 years-includes carers records as this links with LAC record
<table>
<tr><th>Area</th><th>Retention period from closure unless stated otherwise</th></tr>
<tr><td>Looked after or adopted children</td><td>100 years

(15 years if child dies under 18)</td></tr>
<tr><td>Children subject to other orders who have never been LAC such as Supervision Orders, Residence Orders or Special Guardianship etc</td><td>100 years</td></tr>
<tr><td>Private Fostering</td><td>6 years</td></tr>
<tr><td>Adoptive carers and associated records</td><td>100 years</td></tr>
<tr><td>Unsuccessful Adoptive Applicants</td><td>25 years</td></tr>
<tr><td>Other LA LAC placed in Reading</td><td>6 years</td></tr>
<tr><td>Approved Foster carers</td><td>100 years</td></tr>
<tr><td>Unsuccessful Foster carer applicant</td><td>6 Years</td></tr>
<tr><td>Children who have had active CP Plans</td><td>100 years</td></tr>
<tr><td>Children who have had advice and support (Non Statutory work)- this could include Initial Assessment up to S47 but were not made subject to a CP Plan</td><td>6 years</td></tr>
<tr><td>Children in Need supported included Core Assessments</td><td>6 years unless CP

involvement</td></tr>
<tr><td>Substance Misusing Children</td><td>6 Years</td></tr>
</table>
</td>
</tr>
</table>

	Enquiries NFA	6 years
	Missing children from Reading	6 years
	Missing children from other LA's	Destroy after 1 year after consulting with the originating LA
	Risk to children/ Schedule 1 Offenders	70 years
	ADD IN ADULTS	
Thames Valley Police	Retention of data for policing purposes will comply with the Statutory Code of Practice on the Management of Police Information 2005 (MOPI) and be governed by Authorised Professional Practice on Information Management. http://www.app.college.police.uk/app-content/information-management/management-of-police-information/retention-review-and-disposal-of-police-information/	
Berkshire Healthcare NHS Foundation Trust	BHFT need to comply with the following codes of practice with regards to retention schedules and disposal of records Note that Rio Records live whilst the patient is All paper records are archived for 7 years before being destroyed https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200138/Records_Management_-_NHS_Code_of_Practice_Part_1.pdf https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200139/Records_Management_-_NHS_Code_of_Practice_Part_2_second_edition.pdf	
Thames Valley Community Rehabilitation Company	Retention periods for the data provided from Thames Valley CRC to the MASH will be in line with the NPS retention schedules and disposal of records policy.	
National Probation Service	Data is retained for 6 years unless life term.	
Berkshire Woman's Aid	Information on clients is generally kept until a year has lapsed since the last contact with the client. Where a file relates to any child subject to a protection plan, the file is retained indefinitely.	

Appendix 2 – Mash Office Security

Access At the end of the day, ensure doors and windows are locked. Challenge anyone entering the building without their ID on display, and ensure visitors are signed in and provided with the appropriate ID. Visitors should be escorted where necessary.

Clear Desk At the end of each day and when not in use, information including printed documents, paper files, CD's, Disc's, and USB memory sticks should be stored in suitable locked safes, cabinets or drawers. If these are not available, office doors should be locked when unattended. Ensure sensitive or protectively marked information is cleared from printers, faxes and photocopiers straight away. Sensitive or protectively marked information, including copies, must be appropriately destroyed either in the confidential waste bags provided or by shredding when no longer required.

Screen Locks Always ensure screens are locked when left unattended to ensure it cannot be read, printed or copied by anyone else. Wherever possible, computer screens should be angled away from the view of others who are not authorised to view the information. If appropriate, close blinds and use screen shields to protect information from views through windows.

Passwords Always use strong passwords, ideally 8 alphanumeric characters long, with a mixture of upper and lower case, numbers and punctuation. Do not choose words that could be easily guessed by someone that knows you. Do not share your password or allow someone else to use a system that you are logged into.

Transit of Information Ensure adequate security measures are taken when moving sensitive information, for example between sites or partner agencies, be it that in hard copy, or stored on laptops, mobile phones, or tablets. Encrypted USB sticks can be used for transferring sensitive electronic data securely. Keep portable devices in sight at all times when using public transport. During car journeys keep devices locked in the boot out of site, and where practical remove them when leaving the vehicle unattended. Use Security cases where available.