

Wokingham Borough Council

# Information Sharing Agreement

Wokingham Multi-Agency Safeguarding Hub

Authors: Thames Valley Police and Wokingham Borough Council.

Commencement Date: 21 March 2016

Document Marking: Public

# Purpose specific Information Sharing Arrangement

Version 3.0

The Children Act 2004 emphasises the importance of safeguarding children by stating that relevant partner agencies must make sure that functions are discharged having regard to the need to safeguard and promote the welfare of children.

In order to deliver the best safeguarding decisions that ensure timely, necessary and proportionate interventions, decision makers need information 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, this document has been put together to formalise information sharing arrangements predominantly within the Wokingham Borough, but also recognise the possibility to protect individuals with the information that may have been obtained from organisations outside the Borough. By sharing information within the Multi-Agency Safeguarding Hub (MASH) this will allow the parties to identify and assess risks to children’s wellbeing and welfare in the area.

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.

## Version record:

Version No	Amendments Made	Authorisation
1.0	First completion and issue of the agreement	
2.0	Updated in line with requirements of GDPR and DPA 2018	
3.0	Updating format to reflect corporate ISA documents and also reviewing terms of the sharing agreement to allow for more efficient process.	

# Contents Page

Page: 03      Section 1: Purpose of the Agreement and Definitions

Page: 05      Section 2: Specific purpose for sharing

Page: 07      Section 3: Legal basis for sharing and specifically what is to be shared

Page: 09      Section 4: Description of arrangements including security matters

Page: 14      Section 5: Agreement signatures

## Section 1: Purpose of the Agreement and Definitions

This agreement has been developed to:

- Define the specific purposes for which the signatory organisations have agreed to share information.
- Describe the roles and structures that will support the exchange of information between parties.
- Set out the legal gateway through which the information is shared.
- Describe the security procedures necessary to ensure that compliance with responsibilities under the Data Protection Act (and UK General Data Protection Regulations (UK GDPR)) and agency specific security requirements.

**The signatories to this agreement will represent the following parties:**

1. Wokingham Borough Council
2. Thames Valley Police
3. Probation Service
4. Berkshire Health NHS Foundation Trust London House, London Road, Bracknell, Berkshire, RG12 2UT, ICO no: Z6964815
5. Cranstoun

### Definitions:

The following definitions and rules of interpretation apply in this Agreement;

**The Act:** In this agreement the Act refers to the Children Act 2004.

**Agreement:** This refers to this Information Sharing Agreement document and any appendices that should accompany it.

**Business Day:** a day other than a Saturday, Sunday or public holiday in England when banks are open for business.

**Agencies:** In this Agreement, this refers to any party other than Wokingham Borough Council in the list in Section 1.

**Data Protection Legislation:** All applicable data protection and privacy legislation in force in the UK including the UK General Data Protection Regulation (UK **GDPR**); the Data Protection Act 2018 (**DPA (2018)**); the Privacy and Electronic Communications Regulations 2003 as amended; any other European Union legislation relating to personal data and all other legislation and regulatory requirements in force which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications).

**Personal Data Breach:** A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Shared Personal Data.

**Shared Personal Data:** This refers to the personal information that can be shared as laid out in Section 2.

**Subject Access:** The exercise of a Data Subject of his or her Rights under Article 15 of the UK GDPR and the DPA 2018.

**Supervisory Authority:** The relevant Supervisory Authority for all parties is the Information Commissioners Office.

**Term:** Means the period on commencement date and this Agreement is open ended so there is no **End Date**. Termination of this Agreement is undertaken by each party issuing a notification to the others of their removal from the Agreement.

**Wokingham Borough Council:** This refers to the Local Authority, any of its owned companies, or any of its contractors who have an existing contract and sharing agreements in place, and are acting on the authority of the Council.

**Controller, Processor, Data Subject, Personal Data, Special Categories of Personal Data, Processing, and 'Appropriate technical and organisational measures'** shall have the meanings given to them in the Data Protection Legislation.

## 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 their welfare 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 agencies such as the police, Children's Services authorities, ICBs and the NHS England 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 2018, 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 18.

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.

The rationale behind having a 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\\_TA\\_GGED.pdf](http://www.education.gov.uk/munroreview/downloads/8875_DfE_Munro_Report_TA_GGED.pdf)) as an example of good practice in multi-agency partnership working because of how it improved information sharing between participating agencies.

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 Wokingham is contained in the Berkshire Local Safeguarding Children Board (LSCB) Child Protection Procedures 2019. The LSCB document should be seen as the over-arching agreement for all agencies within Wokingham Borough. This document has been produced to allow information sharing within the MASH environment.

### Section 3: Legal basis for sharing and what specifically will be shared

Each party shall ensure that it processes the data fairly and lawfully in accordance with this Agreement and within Data Protection legislation as a whole. There is published guidance from Central Government which is invaluable for safeguarding professionals that should be read in conjunction with this agreement.

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/721581/Information\\_sharing\\_advice\\_practitioners\\_safeguarding\\_services.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721581/Information_sharing_advice_practitioners_safeguarding_services.pdf)

Much of the information to be shared between parties to this Agreement will have been obtained under a duty of confidence and individuals would have an expectation that their information will be kept securely and confidentially. Due to the nature of this type of agreement, it is not possible to list all the data that could be shared amongst the parties, but it is reasonable to accept that any and all data *could* be supplied to aid with the MASH work, **so long as it is reasonable, proportionate, fair and lawful, and necessary to the decision making process**. Any decision to share or not must be recorded in the original record(s).

Examples of data that may be shared include; Name of Data Subject (Child); Family members, Carer's, or other persons who have parental responsibilities; Date of Birth and/or Age; Ethnic origin; Nationality and/or languages spoken; GP and/or Health records; Anti-Social Behaviour data; Police intelligence; School or educational setting data; Emergency services data; and Housing data. These examples are not exhaustive and other data will be shared as is relevant and in line with the above.

Information shared within the MASH is done for specific purposes relating to the safeguarding of children. Any further use of that information, for purposes not set out in this agreement, cannot be disseminated further without permission from the relevant Data Controller and covered by a lawful reason.

**The Data Protection Act 2018 (and UK GDPR) do not prevent, or limit, the sharing of information for the purposes of keeping individuals safe.**

#### Personal Data

The organisations for the purposes of the MASH may rely on the following lawful bases for processing data;

- (i) the processing is necessary to comply with the law under Article 6(1)(c), and legislation has been documented within this Agreement.
- (ii) the processing is necessary for the performance of a task carried out in the public interest under Article 6(1)(e) of GDPR;
- (iii) .

#### Special Category Data



The organisations for the purposes of the MASH may rely on the following lawful bases for processing special category data;

- (iv) .
- (v) The processing is necessary in the safeguarding of children (and adults) at risk and therefore is in the public interest; Article 9(2)(g).
- (vi) The processing is necessary in the provision of health or social care services to an individual by a professional in the 'Health' or 'Social Care' profession under Article 9(2)(h).
- (vii) The processing of the data may in some circumstances be used to establish, exercise or defend legal claims or judicial acts and in those circumstances Article 9(2)(f) is relied upon.
- (viii) To be able to process data under Special Categories it needs to have some lawful bases under Schedule 1 of the Data Protection Act 2018; in the case of this Agreement the processing is necessary under Paragraph's 2, 6, 10, and 18 of Schedule 1.

Parties to this Agreement shall undertake to inform the Data Subjects, in accordance with the Data Protection Legislation, of the purposes for which it will process their personal data, the legal basis for such purposes and such other information as is required including;

- giving full information to any Data Subject whose personal data may be processed under this Agreement of the nature of such processing including data processed under this Agreement.
- The fact that Shared Personal Data will be transferred to the other partner organisations and sufficient information about such transfer and the purpose to enable the Data Subject to understand the purpose and risks of such transfer.

## **Section 4: Description of arrangements including security matters**

### **Compliance, Security and Training**

Each party must ensure compliance with applicable Data Protection Legislation at all times during this Agreement.

All signatories to this agreement accept responsibility for ensuring that all appropriate security arrangements are complied with, and that all staff members who have access to the data have an appropriate level of Data Protection training, fully understand the terms of this agreement and their own responsibilities. Each party shall perform its obligations under this agreement at its own cost.

The parties undertake to have in place throughout the Agreement appropriate technical and organisational security measures to:

- (a) prevent:
  - i. unauthorised or unlawful processing of the Shared Personal Data; and
  - ii. the accidental loss or destruction of, or damage to, the Shared Personal Data.
  
- (b) ensure a level of security appropriate to:
  - i. the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage; and
  - ii. the nature of the Shared Personal Data to be protected.

It is the responsibility of each party to ensure that its staff members are appropriately trained to handle and process the shared Personal Data in accordance with appropriate technical and organisational security measures together with any other applicable national data protection laws and guidance and have entered into confidentiality agreements relating to the processing of personal data.

### **Subject Access**

The Parties each agree to provide such assistance as is reasonably required to enable the other party to comply with requests from Data Subjects to exercise their rights under the Data Protection Legislation within the time limits imposed by the Data Protection Legislation.

The signatory for each party is responsible for maintaining a record of individual requests for information, the decisions made and any information that was exchanged. Records must include copies of the request for information, details of the data accessed and shared and where relevant, notes of any meeting, correspondence or phone calls relating to the request.

### **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 may be published with 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 Section 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.

## **Resolution of disputes with data subjects or the Supervisory Authority**

In the event of a dispute or claim brought by a data subject or the Supervisory Authority concerning the processing of shared Personal Data against either or all parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

The parties agree to respond to any generally available non-binding mediation procedure initiated by a Data Subject or by the Supervisory Authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes. Each party shall abide by a decision of a competent court in the jurisdiction of England and Wales.

## **Business Process**

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 Strategy discussion. Only cases where threshold is unclear and more information would enable the decision maker to make a more informed decision will be taken through the MASH process. The Police will have limited access to the Mosaic system to be able to search the database to see if a particular individual or family is known to the local authority and who the allocated worker that individual has been assigned to.

All parties to this Agreement 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. 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 provided the information.

Information will be sent and received electronically to ensure there is an audit trail of its movement. Any e-mail communication when Personal Data is included will be by way of secure, appropriate and approved methods.

Information will be stored in secured premises, e.g. not in areas where the public have access. 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 usernames and passwords. Parties confirm that permission to access information shared as part of this agreement will be granted on a strict 'need-to-know' basis.

It is not the intention of this agreement that information will be produced in physical format. If information is printed off, it will be the individual party'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.

All information is to be recorded centrally on Mosaic; the local authorities social care electronic recording and management system. No other agency will have access to this, 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.

## **Business Continuity**

All parties to this Agreement will provide 2 contacts (primary and back up) to the Local Authority to compile a list of contacts that would deal with queries and requests for information under this Agreement. The back up nominated persons will act as the point of contact to ensure continuity in the absence of the primary point of contact.

In the event that access to the shared Personal Data is not possible via the primary transfer method; that the signatories, or the nominated representatives, will as soon as reasonably possible liaise with all other parties to agree an alternative method of transferring the information to ensure that the processing of the shared Personal Data can continue during this period. This alternative processing should be in compliance with the clauses of this Agreement.

## **Retention and Disposal of information**

Each party shall not retain or process the shared personal data for longer than is necessary to carry out the agreed purpose, as laid out in Section 2.

Notwithstanding the clause on Subject Access, parties shall continue to retain Shared Personal Data in accordance with any statutory or professional retention periods applicable in their industry. 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.

Each party shall ensure that any Shared Personal Data are returned to the originating partner organisation or destroyed in the following circumstances;

- a) on termination of the Agreement;
- b) on expiry of the Term of the Agreement; or
- c) once processing of the shared Personal Data is no longer necessary for the purposes it was originally shared for, as set out in Section 2.

It is not the intention of this agreement that information will be produced in a physical format. If information is printed off an electronic system, it will be the printing party's responsibility to dispose of the information in an appropriate secure manner i.e. shredding, once it is no longer needed.

Following the deletion, or destruction, of the shared Personal Data, each party shall notify the originating party organisation that the shared Personal Data in question has been deleted if the originating party requires confirmation of such.

### **Personal data breaches and reporting**

The parties shall each comply with its obligation to report a Personal Data Breach to the appropriate Supervisory Authority with 72 hours (if necessary) and (where applicable) to Data Subjects under Article 33 of the GDPR. Each Party shall inform the other party/parties of any Personal Data Breach irrespective of where there is a requirement to notify any Supervisory Authority or Data Subject(s). The Information Commissioners Office has a self-assessment tool which aids in identifying if a data breach needs to be reported to them – they have advised that not every breach needs to be raised with the ICO.

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.

The parties agree to provide reasonable assistance as is necessary to each other to facilitate the handling of any Personal Data Breach in an expeditious and compliant manner. Any breach should be reported to the signatory as soon as possible.

### **Changes to the applicable law**

If during the Agreement the Data Protection Legislation change in a way that this document is no longer adequate for the purpose of governing lawful data sharing exercises, the Parties agree that the signatories will negotiate in good faith to review the Agreement in the light of the new legislation.

### **Third Party Rights**

No-one other than a party to this agreement, their successors and permitted assignees, shall have any right to enforce any of its Terms.

At its own expense, each party shall, and shall use all reasonable endeavors to procure that any necessary third party shall, promptly execute and deliver such documents and perform such acts as may be required for the purpose of fulfilling this Agreement.

### **Force Majeure**

No party shall be in breach of this Agreement, nor liable for delay in performing, or failure to perform, any of its obligations if such delay or failure results from events, circumstances or causes beyond its reasonable control. In such circumstances the

time for performance shall be extended by a period equivalent to the period during which performance of the obligation has been delayed or failed to be performed.

The signatory of the party, or their representative, must inform the other parties once they become aware of any event, circumstance, or cause beyond their control which results in them being unable to fulfil their obligations so that business continuity plans can be considered where necessary.

## **Notice**

Any notice or communication given to a party under or in connection with this agreement shall be in writing, addressed to the signatories and shall be:

- (a) delivered by hand or by pre-paid first-class post or other next working day delivery service at its registered office (if a company) or its principal place of business (in any other case); or
- (b) sent by email to the signatory.

Any notice or communication shall be deemed to have been received:

- (a) if delivered by hand, on signature of a delivery receipt or at the time the notice is left at the proper address; and
- (b) if sent by pre-paid first-class post or other next working day delivery service, at 9.00 am on the second Business Day after posting or at the time recorded by the delivery service; and
- (c) if sent by email, at the time of transmission, or if this time falls outside business hours in the place of receipt, when business hours resume. Business hours means 9:00 to 17:00 Monday to Friday on a day that is not a public holiday in the place of receipt.

This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

## **Variation**

No variation of this agreement shall be effective unless it is in writing and signed by the signatories (or their authorised representatives).

## Section 5: Agreement to abide by this arrangement

The parties signing this Agreement accept that the procedures laid down in this document provide a secure framework for the sharing of information in a manner compliment with their statutory and professional responsibilities.


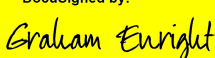
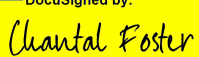
Parties to this agreement acknowledge that the wrongful disclosure of personal data (obtained under this Agreement) to other organisations or persons may amount to a criminal offence under the Data Protection Act 2018.

This Agreement has been written to ensure compliance with applicable Data Protection principles in the UK 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 Information Commissioners Office or other litigation, and the suspension or termination of this Agreement. Signatories to this Agreement agree to provide the Information Commissioners Office with all the 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 other third party, for a purpose not covered by this agreement, without obtaining the express authority of the originating partner agency, unless failure to do so would result in a safeguarding issue.
- Engage in a review of this agreement with parties as necessary and within the next review date.

**We the undersigned agree that each organisation that we represent will adopt and adhere to this Information Sharing Agreement:**

Organisation and address (contact details)	Full Name and Post Held	Signature
Wokingham Borough Council	Emma Cockerell, Wokingham BC Shute End, RG101BN	Signed by:  8DE516124878403...
Thames Valley Police	Please add your name and post details here	DocuSigned by:  9D29BC58585F4C9...
National Probation Service	Chantal Foster Head of Probation Delivery Unit west Berkshire	DocuSigned by:  1489884D58A04AA...

<p>Berkshire Health NHS Foundation Trust London House, London Road, Bracknell, Berkshire, RG12 2UT</p>	<p>Dr Minoo Irani Caldicott Guardian</p>	<p>Signed by: <i>Minoo Irani</i> 9BD4C7D65551464...</p>
<p>Cranstoun</p>	<p>Katie Lloyd - Service Manager Cranstoun Domestic Abuse Support Services.</p>	<p>DocuSigned by: <i>Katie Lloyd</i> A504E25D2C5F4AA...</p>