# SAFEGUARDING BOARDS

# DATA EXCHANGE AGREEMENT

1. What is the Purpose of this Data Exchange Agreement?

The purpose of this Agreement is to provide a framework to facilitate the exchange of data and to give guidance for the operation of an effective and co-operative partnership between the signatory parties.

The exchange of information is to enable partner agencies to improve their effectiveness in safeguarding children and vulnerable adults in Herefordshire.

1. What is the Legal Basis for Data Exchange?

It is important to ensure that any partner/individual who receives information and holds and processes such information is able to identify the legal basis for processing as defined by the Data Protection Act 2018 and the General Data Protection Regulations.

Additionally, there may be other legislation under which information can be shared, including the Care Act 2014 and the Children and Families Act 2014; further information is available in the *Information Sharing – Relevant Legal Guidance* document.

The conditions for processing for safeguarding are:

* Necessary for compliance with a legal obligation
* Necessary to protect the vital interests of a data subject or another person where the data subject is incapable of giving consent
* Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

### *Consent / Agreement*

Under the new data protection legislation, consent in this agreement is not in the context of a lawful basis for processing information, but in the context of keeping families informed and asking for their co-operation. It is still the case that, should a family decide not to co-operate and say that they do not wish for their information to be shared, professionals should, as they currently do, consider whether it is necessary/appropriate to do so without their agreement or whether the threshold for sharing without the agreement of the family is risk of significant harm.

Practitioners should not seek consent when they are required by law to share information through a statutory duty or by a court order. Consent should also not be sought if doing so would:

* Place a person (individual, family member, staff or a third party) at increased risk of significant harm; or
* Prejudice the prevention, detection or prosecution of a serious crime; or
* Lead to an unjustified delay in making enquiries about allegations of significant harm to an adult.

Decisions must be recorded and the rights of individuals under data protection legislation must be respected, including the right to be informed about processing of data, the right to amend inaccurate data, the right of access, the right of erasure, the right to restrict data, and the right to data portability where applicable.

### *Capacity to give consent*

When sharing information in respect of children or adults who lack the capacity to provide any required consent, information should only be shared when it is permitted by relevant legislation and is considered to be in the person’s best interests.

Additionally, where a person lacks mental capacity to decide about their own personal information, the Mental Capacity Act 2005 Code of Practicestates that certain other people may be able to request access to that information. This would be somebody with a lasting power of attorney, an enduring power of attorney or who is a deputy appointed by the Court of Protection.

For young children, parents with parental responsibility may be able to give consent on behalf of their child.

Partners also agree to ensure that their actions are in compliance with any other relevant legislation and standards, including:

* The Crime and Disorder Act 1998
* The Common Law of Confidentiality
* The Freedom of Information Act 2000
* Caldicott Principles

If recorded information required to be shared, the form below must be completed to record the sharing, either once for information being routinely shared, otherwise on a case by case basis. If it is in the public interest to share the information, record why you believe the information shared is relevant and proportionate.

Share as much as, but no more information than is necessary and share only on a ‘need to know’ basis.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| SAFEGUARDING INFORMATION SHARING FORM DEA001 | | | | | | | |
| What data is it necessary to exchange? | | | | | | | |
| **Data Set**  eg name, address, dob | **Who from**  Organisation / Team / Person | **Who to**  Organisation / Team / Person | **Why** | **Which Organisation owns the information?** | **Frequency of sharing** | **How will information be exchanged?** | **How long will data be held for by recipient organisation** |
| Name, address, dob of victim / perpetrator together with appropriate and proportionate information necessary to investigate / assess safeguarding needs | Safeguarding partner holding initial information | Safeguarding partners holding relevant information | Protection of risk to individual’s’ safety and/or prevention of crime | The organisation who originally shares the information | As required | It may be exchanged in the following ways:  1.prior to a safeguarding meeting through secure, electronic means or secure hard copies;  2. verbally at a safeguarding meeting, through presentation of the information;  3. paper copies distributed at safeguarding meeting with clear guidance on subsequent security requirements e.g. all copies returned at end of meeting;  NB: all shared information is clearly marked with level of security required. | As determined by the organisation’s retention schedule |
| Details which may include name, address in relation to a concern raised by a member of the public. Data may include information on the correspondent | Organisation contacted by member of public | Safeguarding partners holding relevant information | Protection of risk to individual’s’ safety and/or prevention of crime | Organisation contacted by the member of the public | As required | By secure email | As determined by the organisation’s retention schedule |

If any further data is required over and above that included in this Data Exchange Agreement, contact should be made with the Data Protection Officer or Information Governance Officer of the sending organisation prior to the release of any information.

Each Partner to this Agreement must ensure that:

* The data being exchanged is accurate and where necessary up-to-date
* A record is kept of what information has been exchanged
* The process as agreed and documented in the form above (DEA001) for the secure exchange of information is followed
* The length of time that the information that has been exchanged will be kept for by the receiving organisation as per the form above (DEA001)
* Appropriate standards of security are in place for the processing of sensitive information.
* Protective marking standards will be used to indicate how securely the information needs to be stored
* If the information that has been exchanged is to be routinely shared with another party this will also be documented on the form above (DEA001), or if shared as an exception the sharing will be documented appropriately with the reasons for sharing and following the same standard of security as required by this agreement
* Partner organisations will ensure that their staff are trained adequately to understand and operate the Agreement.
* This agreement will be reviewed every 3 years or sooner if there are changes to legislation or best practice guidance.

1. Breach of Confidentiality

In the event that this agreement is breached by either partner or any named third party who has received data under this agreement the appropriate lead officer should be notified within 24 hours.

Depending upon the seriousness of the breach this may be reported to the Information Commissioners Office within 72 hours of the breach being discovered and where criminal action is involved the Police may also be informed.

Where staff have failed to comply with organisational policies and procedures disciplinary action will be taken against them and in the case of a criminal offence legal proceedings may be taken against those responsible for the breach.

1. Complaints Procedures

Each partner must be committed to having procedures in place to address complaints relating to inappropriate disclosure or failure to disclose personal information. Individuals must be provided with information about these procedures.

1. Access to Information

The Data Protection Act provides individuals the right to have access to information held about them with limited exemptions. It is necessary to ensure that only appropriate access to information is granted, therefore the organisations party to this agreement have responsibilities to ensure individuals’ rights are met appropriately. This will usually be done by sending the requests to the appropriate officers in the organisation who deal with access requests.

1. Closure/Termination of Agreement

Any partner organisation can suspend this Data Exchange Agreement for 45 days if security has been seriously breached. This should be in writing and be evidenced.

Any suspension will be subject to a Risk Assessment and Resolution meeting, the panel of which will be made up of the Signatories of this agreement, or their nominated representative. This meeting to take place within 14 days of any suspension.

Termination of this Data Exchange Agreement should be in writing to Partner Organisations, giving at least 30 days’ notice.

1. Requests for Disclosure of Information Received under this Agreement

All recorded information held by public sector agencies is subject to the provisions of the Freedom of Information Act 2000, the Data Protection Act 2018 and the General Data Protection Regulations. Whilst there is no requirement to consult with third parties under the Freedom of Information Act, the parties to this Agreement will consult the party from whom the information originated and will consider their views to inform the decision making process. All decisions to disclose must be recorded by the disclosing organisation.

1. Appropriate Signatories

Name ­­­­­­­­­­­­­­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Organisation\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Organisation \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**One copy of the Agreement must be sent to each partner organisation’s Data Protection Officer or Information Governance Team, and the original signed copy must be retained by the Safeguarding Board.**

# Appendix 1: Processing of personal data under the Data Protection Act

The processing of personal data will only be lawful if it satisfies at least one of the following conditions:

* Consent of the data subject
* Necessary for the performance of a contract with the data subject or to take steps preparatory to such a contract
* Necessary for compliance with a legal obligation
* Necessary to protect the vital interests of a data subject or another person where the data subject is incapable of giving consent
* Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
* Necessary for the purposes of legitimate interests – *this condition can no longer be relied on by public authorities.*

The grounds for processing the special categories of personal data must satisfy at least one of the following conditions:

* Explicit consent of the data subject, unless reliance on consent is prohibited by law
* Necessary for the carrying out of obligations under employment, social security or social protection law, or a collective agreement
* Necessary to protect the vital interests of a data subject who is physically or legally incapable of giving consent
* Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
* Data manifestly made public by the data subject
* Necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
* Necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguarding measures
* Necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional
* Necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
* Necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)