West Sussex
Information Sharing Agreement
for
Safeguarding Partners and Agencies working with
Children and Young People

Contents

1. Purpose

The purpose of this agreement is to provide a clear framework to facilitate the sharing of information between partner agencies, relevant persons and bodies with responsibility for delivering services for children and young people (*henceforth referred to as 'children'*) aged **pre-birth to 18** and their families or carers.

The agreement applies to all safeguarding partners[1] and agencies in West Sussex as listed in appendix one.

Caldicott Principle 7 acknowledges that the duty to share information can be as important as the duty of confidentiality. Information sharing is often necessary to promote the welfare of children and ensure they are safeguarded. *No practitioner should assume that someone else will pass on relevant information.*

Effective sharing of information between agencies is essential to support:

families and children to:

- Reduce the amount of time that they spend repeating their story to different agencies
- Receive early interventions that ensure that they receive the help, advice and support that they require in a timely way
- Improve outcomes by ensuring that all agencies are aware of relevant children and family circumstances

staff to:

- Reduce the time that they spend collecting basic information from families and carers
- Make fully informed decisions based on comprehensive information
- Understand it is acceptable to share personalised confidential data in the interests of getting the best possible outcomes for children and their families
- Understand that anonymised data can be shared freely

the organisation to:

- Ensure the safety of children and aim to reduce the need for child protection interventions
- Improve integrated working
- Reduce acute needs through earlier effective action

All staff working with children and families need to understand the delicate balance between preserving confidentiality and the imperative to share, when this will help children to achieve their full potential and ensure their safeguarding. No major enquiry has ever criticised staff for sharing information; rather, they have highlighted how failures to share have contributed to childcare tragedies.

Organisations involved in providing services to children have a responsibility to ensure that their use of personal information is lawful, and that the child and families Data Protection rights are respected. The partner agencies to this agreement are demonstrating that they are committed to fair and lawful information sharing in order to Safeguard and promote the well-being of children.

[1] Safeguarding Partners as described within Working Together guidance 2018

2. Categories of data covered by this agreement?

This agreement is intended to formalise:

- The organisational requirements to share information about children, their parents and carers by the signatories of this document.
- The sharing of information between practitioners about individual children and their families and carers.
- The categories of data which may be shared under this agreement are:
  names, contact data, family's relationships interactions and history, health data

3. Legal Framework

Each party must ensure compliance with the General Data Protection Regulation (GDPR) 2018 and the Data Protection Act 2018 (DPA).

The primary lawful basis under GDPR for the sharing of data under this agreement may be any of the following:

For personal data:

Article 6

(1)(c) 'Legal Obligation': the processing is necessary for you to comply with the law (not including contractual obligations).

(1)(e) ''Public Task'': the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law

For special category data:

Article 9

(2)(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

This means for these specific areas covered by Article 9, that, whilst families will be **informed** when personal data is being shared or processed, **their consent will not normally be required**.

The legal obligations to share information arise as a result of the statutory framework provided within Section 10 of the Children Act 2004, which places a duty on each local authority to make arrangements to promote co-operation between itself and relevant partner agencies to improve the well-being of children in its area.

In addition to this all partner agencies are subject to a variety of legal, statutory and other guidance which promotes the sharing of information including but not limited to:

The Children Act 1989
Education Act 2002
Education Act 1996
Learning and Skills Act 2000
Mental Capacity act 2005
Mental Capacity Act 2005 Code of Practice

Immigration and Asylum Act 1999
Local Government Act 2000
Criminal Justice Act 2003
Crime and Disorder Act 1998
Counter Terrorism and Security Act 2015
The Police and Justice Act 2006 and the Crime and Disorder Regulations 2009
Criminal Justice and Court Service Act 2000
National Health Service Act 1977
National Health Service Act 2006
The Adoption and Children Act 2002
Section 55 of the Borders, Citizenship and Immigration Act 2009

4. Golden rules for information sharing[2]

Each party will adhere to these rules for information sharing and if in doubt will seek guidance from their respective information governance team, Data Protection Officer or Caldicott Guardian.

1. **Remember that the General Data Protection Regulation (GDPR), Data Protection Act 2018 and human rights law are not barriers to justified information sharing**, but provide a framework to ensure that personal information about living individuals is shared appropriately.

2. **Be open and honest with the individual** (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

3. **Seek advice** from other practitioners if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.

4. **Where possible** share information with consent, and where possible, respect the wishes of those who do not consent to having their information shared. Under the GDPR and Data Protection Act 2018 you may share information without consent if, in your judgement, there is a lawful basis to do so, such as where children may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be clear of the basis upon which you are doing so. Where you do not have consent, be mindful that an individual might not expect information to be shared. Share with informed consent where appropriate.

5. **Consider safety and well-being:** Base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions.

6. **Necessary, proportionate, relevant, adequate, accurate, timely and secure**: Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.

7. **Keep a record** of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

See Appendix 2 - for an information sharing flowchart which will provide you with further guidance.

[2] Information sharing advice for practitioners providing safeguarding services to children, young people, parents and carers HM Government July 2018

5. Personal Information and Special Category Data

Within health and social care, the term Personal Confidential Data (PCD) is often used. This describes personal information about identified or identifiable individuals, which should be kept private. 'Personal' includes the GDPR definition of personal data, but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' as defined by the GDPR. To elaborate, in line with the regulations:

- **Personal information** means any information relating to an identified or identifiable living individual.

- **Special category** data is broadly similar to the concept of sensitive personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual; the processing of data concerning health; the processing of data concerning an individual's sex life or sexual orientation.

6. Confidentiality

Personal information held by an agency is deemed to have been provided in confidence, and will not be shared unless there is a lawful basis to do so. The lawful basis bases are:

- Sharing is necessary to safeguard and promote the welfare of a child, or
- Necessity for the prevention and detection of crime.

In the absence of a more appropriate lawful basis for sharing no personal data will be shared without the data subject's written consent.

Agencies requesting disclosure of personal information from the partners will not seek to override procedures which each agency has in place to ensure that information is disclosed legally and appropriately.

7. Consent

It may be considered best practice to obtain consent in most cases when sharing information in multi-agency situations particularly when special category data is involved.

If consent is the lawful basis for sharing it should be obtained when beginning work with an individual or family, as part of the intervention. **The following are the requirements for consent:**

- Any consent must be distinguishable from the other matters, easy to understand and provided in an easily accessible form using clear and plain language otherwise you cannot rely on it.

- It is important to identify how much information you share and to provide written justification for your decision rather than a simple permission for generic processing and sharing with types of organisations. This means a consent form should contain a number of specific options.

- If another organisation/third party is relying on the consent you must name them in the consent form.

- Prior to giving consent, the data subject (or their appropriate representative) shall be informed that consent can be withdrawn at any time. It shall be as easy to withdraw as to give consent.

Certain circumstances override the need for consent, for example you do not need to seek consent from the child or their family, or inform them that the information will be shared, where there is a safeguarding concern. For example, if doing so would:

- Place a person (the individual, family member, yourself or a third party) at increased risk of harm.
- Lead to an unjustified delay in making enquiries about allegations of significant harm to a child, or adult.
- Prejudice the prevention, detection or prosecution of a serious crime. (If asked to share such information advice should be sought from a line manager, information governance team or Caldicott guardian).

8. What to do in the case of a breach of this agreement

Data security: Each organisation will have in place appropriate organisational and technical measures to ensure security of data and this will include that all staff (full/part time, members, temporary, students, volunteers, contractors) who have access to, or are likely to come into contact with, personal information sign a confidentiality agreement as part of their terms and conditions of employment.

Breaches reported by a member of the public will usually present as a complaint. Every agency must have their own complaints procedure, which should be adhered to should a member of the public report an incident.

Each agency will have in place a data security breach management process. Any inadvertent disclosure of information by an employee may constitute a data security breach and should be investigated in line with internal procedures.

Each agency shall notify any potential or actual losses of the Shared Personal Data, and any Data Security Breach, to the other party's Data Protection Officer (DPO) as soon as possible and in any event within 24 hours after becoming aware of the breach. The DPO shall work together to consider the action required in order to resolve the issue in accordance with the applicable Data Protection Legislation.

Each agency shall provide reasonable assistance as is necessary to the other to facilitate the handling by the other party of any Data Security Breach in an expeditious and compliant manner.

9. Management of the Information Sharing Agreement (ISA)

Proposed amendments to this ISA must be agreed with the leads of each statutory partner agency and a revised agreement produced and signed. This includes the inclusion or removal of any agency.

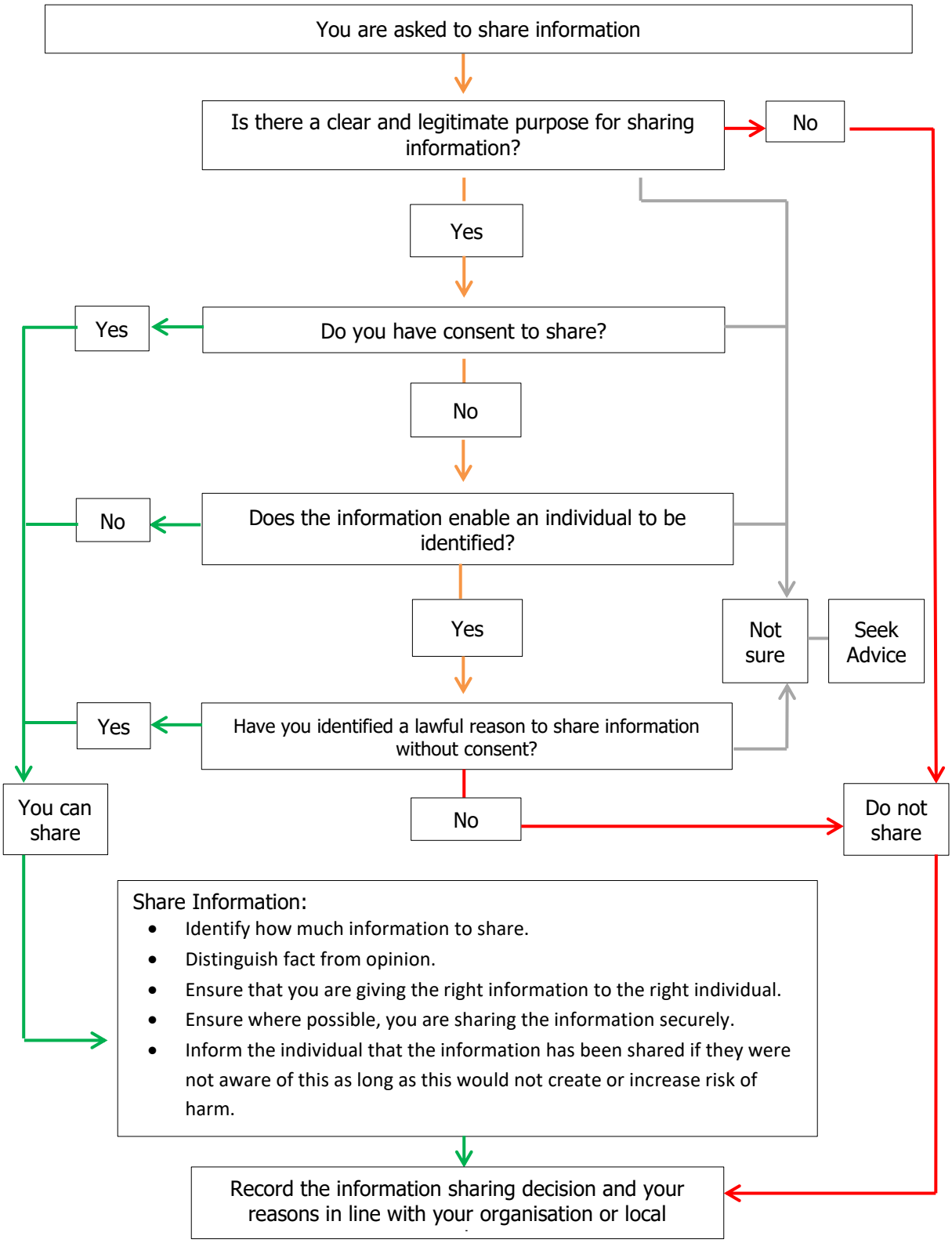
The agreement will be subject to formal review every two years and as a result of any changes to the law and policy in relation to the security and confidentiality of information.

Appendix 1.

Statutory Partner Agencies, relevant person and bodies

- Local Authority
- District Councils in local government areas which have them;
- The Chief Officer of Police;
- The Local Probation Trust (including appropriate representation by the Trust of Community Rehabilitation Companies);
- Youth Offending Service;
- NHS England Area Team;
- Clinical Commissioning Group;
- Independent Hospice Providers;
- NHS Trusts and NHS Foundations Trusts (including appropriate representation of hospitals, establishments, facilities and services situated in the local authority area Cafcass;
- The Local Authority must also take reasonable steps to representation from the following persons and bodies:
    - Voluntary sectors
    - Commissioned services (e.g. Change, Grow, Live or Barnardo's)
    - The Governing body of maintained schools
    - The proprietor of non-maintained special schools
    - The proprietor of a city technology college, a city college for the technology of the arts, or an academy;
    - The governing body of a further education institute, the main site of which is situated in the Authority's area;
    - Two lay members representing the local community:
- Partners implemented by Section 55 of the Borders, Citizenship and Immigration Act 2009

Appendix 2. - Flowchart of key questions for information sharing



If there are concerns that a child is in need, suffering or likely to suffer harm, then follow the relevant procedures without delay. Seek advice if unsure what to do at any stage and ensure that the outcome of the discussion is recorded.