

Barnsley Safeguarding Children Partnership and Integrated Front Door

Information Sharing Agreement

Barnsley Safeguarding Children Partnership

Westgate Plaza

Westgate

Barnsley S70 2DR

Contents

- 1 Introduction**
- 2 Purpose of the Agreement**
- 3 Scope of the Agreement**
- 4 Legal considerations for sharing**
 - 4a Consent
 - 4b Confidentiality
 - 4c Data Protection
 - 4d Children Acts 1989 and 2004
 - 4e Other legal powers
 - 4f Human Rights Act 1998
- 5 Processing information**
 - 5a Making a request for, or providing Information
 - 5b Information Quality and Relevance
 - 5c Access
 - 5d Secure storage and transfer of personal information
 - 5e Retention of records
 - 5f Reporting a security incident or breach
 - 5g Access to personal data
- 6 Complaints**
- 7 Approval of the BSCP Information Sharing Agreement**
- 8 Publication of this Agreement**
- 9 Agreement review and changes**
- 10 Further information**

Appendix 1. Legal powers and duties for data sharing

Appendix 2. Caldicott Principles

Appendix 3. Domestic Violence and Child Sex Offender Disclosure Schemes

Appendix 4. Flowchart

Appendix 5. Signatories' List

Introduction

Effective information sharing underpins integrated working and is a vital element of both early intervention and safeguarding. Case reviews and experience have repeatedly shown that keeping children safe from harm requires practitioners to record, analyse and understand the significance of the information they have about:

- A child's health and development and any exposure to possible harm.
- A parent who may need help or may not be able to care for a child adequately and safely.
- Those who may pose a risk of harm to a child.

It is vital that information is shared in an appropriate and timely fashion. Often, it is only when information from multiple sources has been shared and is then put together, does it become clear that a child has suffered, or is likely to suffer, significant harm. Practitioners should be proactive in sharing information as early as possible to help identify, assess and respond to risks or concerns about the safety and welfare of children. This includes when problems first emerge, or where a child is already known to local authority children's social care.

It is intended that agencies with the potential to be involved in safeguarding investigations will sign up to the use of this Barnsley Safeguarding Children Partnership Agreement. Its' purpose is to ensure compliance with the Data Protection Act 2018 and the UK General Data Protection Regulations (UK GDPR) and the Human Rights Act 1998 and provides procedural guidance in relation to multi-agency information sharing.

It allows participating agencies (the Parties) to share personal information in a timely and secure manner to decide on the appropriate pathway for service provision for children and young people, including referral to social care where appropriate. 'Children', in terms of the scope of this Agreement, and as established by the Children Act 1989, means children up to the age of eighteen.

This Agreement contains details of the standards agreed by the Parties involved in the sharing of personal data and personally identifiable information, to maintain integrity, confidentiality and compliance with the data protection principles, whilst ensuring that information is shared with those who 'need to know'.

Information shared under this Agreement should not be disclosed to any persons who are not Parties or if there is any doubt that the requirements of this Agreement might be breached.

2 Purpose of the Agreement

The purpose of sharing information is to ensure secure, confidential, proportionate and necessary information sharing, in relation to children and families, and that this is safeguarded, protected and their welfare is promoted. Strong, effective multi-agency arrangements are ones that are responsive to local circumstances and engage the right people. For the BSCP to be effective, it will engage relevant organisations and agencies that can work in a collaborative way to provide targeted support to children and families as appropriate. This approach requires flexibility to enable joint identification of, and response to, existing and emerging needs, and to agree priorities to improve outcomes for children.

The Agreement will be used to assist in ensuring that:

- Information is shared in a secure manner.
- Information is only shared with the specific relevant agencies concerned in order to perform their role.
- There are clear procedures to be followed with regard to information sharing.
- Each agency is responsible for what information is shared and they must satisfy the fair data processing conditions in the Data Protection legislation.
- Information will only be used for the reason(s) it has been obtained or for additional purposes where this is permitted under the Data Protection legislation.

I The information shared by virtue of this Agreement will be used:

- To identify those children and young people who require a necessary and proportionate intervention.
- To identify victims and potential victims who are likely to experience harm and exploitation and ensure that the Parties work together to deliver harm reduction interventions.
- To ensure that the needs of all children and young people are identified and signposted to relevant services for the delivery and co-ordination of harm reduction interventions, in accordance with the Children Act 1989 and Children Act 2004

II To formally record how the Parties to the Agreement will share information about children who have come to the attention of their organisation because they have not achieved at least one of the five outcomes as defined in the Children Act 2004.

III The Children Act 2004 defines a child's well-being as:

- Physical and mental health and emotional well-being (be healthy)
- Protection from harm and neglect (stay safe)
- Education, training and recreation (enjoy and achieve)
- The contribution made by them to society (make a positive contribution)
- Social and economic well-being (achieve economic well-being).

IV For the purposes of this Agreement the information that will be shared is Personal Data, which may also reveal Special Categories of Personal Data (as defined under the General Data Protection Regulation (Regulation (EU) 2016/679), and typically will be information found in a case file.

3 Scope of the Agreement

The Agreement covers the sharing of personal and special category data about children and young people to ensure effective systems are in place to protect children from abuse and to prevent impairment to children's health and development. Additionally BSCP will review the following:

- Notifiable incidents and non-notifiable serious safeguarding incidents
- Rapid and Child Practice reviews,
- Practice Learning Events
- Multiagency audits
- Child Death Overview Panel and processes

4 Legal considerations for sharing information

4a Consent

- I When sharing information consideration must be given to whether it is reasonable to gain the full consent of the Data Subject.
- II Consent is agreement freely given to an action based on knowledge and understanding of what is involved and its likely consequences. Consent can be expressed either verbally or in writing. Consent must also be informed so that, when someone agrees to information sharing, they understand how much is shared, why, with whom, and what may be the implications of not sharing. The Parties agree to notify data subjects and/or their parents or carers if relevant, that their data may be shared, in the form of a privacy notice. Where applicable explicit consent should always be obtained by the referring agency and this should be in writing where practicable.
- III The Parties understand that the Data Protection Act 2018 does not require them to notify the data subject of any sharing or ask for their consent, if in doing so it would prejudice the prevention or detection of crime, apprehend an offender or place the child, young person or someone else at increased risk of harm. When a decision has been made not to seek consent the rationale for doing so should be clearly recorded to ensure responses can be made to future challenge.
- IV When the consent of a Data Subject is refused or it is not reasonable to seek consent, consideration should be given to legal powers or whether the disclosure is in the public interest and this will be assessed on a case by case basis.
- V If consent is required and is refused, under this Agreement, if not disclosing information would prejudice the reasons listed in Section 2(I), the Parties may provide the information requested or may wish to proactively share. This would be decided on a case by case basis.

4b Confidentiality

- I **Confidential information** is information that is not normally in the public domain or readily available from another source. It should have a degree of sensitivity and value and be subject to a duty of confidence. A duty of confidence arises when one person provides information to another in circumstances where it is reasonable to expect that the information will be held in confidence.
- II **The common law duty of confidentiality** requires that unless there is a statutory requirement to use information that has been provided in confidence, it should only be used for that purpose that the subject has been informed and has consented to. The common law duty is not absolute and can be overridden if the disclosure is in the public interest (e.g. to protect others from harm).

4c Data Protection

- I The Data Protection Act 2018(DPA) applies if the information is personal data relating to an identifiable living individual and held on computer or as part of a 'relevant filing system'. To process or share information, the Data Controller must

ensure that the six principles as set out in section 35-40 of Data Protection 2018 are being met. Specific consideration must be given as to whether the information will be processed fairly and lawfully and for the specified purpose.

- II Each Party to this Agreement is a Data Controller and exercise their role as such for the purposes of this Agreement.
- III The DPA provides Data Subjects with a right of access to records which are held about them.
- IV When a Party wants to share Personal Data or Special Categories of Personal Data with another Party, it must be able to satisfy the conditions in Schedule 9 of the Data Protection Act 2018. If 'sensitive' personal data is shared, the disclosing Party must also be able to satisfy the conditions as set out in Schedule 8 of the DPA 2018.
- V The rule of proportionality should be applied to ensure that a fair balance is achieved between the public interest and the rights of the data subject. All disclosures must be relevant and proportionate to the intended purpose of the disclosure.

4d Children Acts 1989 and 2004

- I This legislation provides statutory power to share information for the purposes of this Agreement.
- II The nature of the information held by individual parties that will be shared under this Agreement will often fall below a statutory threshold of S47 or even S17 of the Children Act 1989. If it does fall within these sections of the Children Act 1989, then these will provide the main legal gateway for sharing information.
- III **Section 10 and 11 of the Children Act 2004** place obligations upon the Police and Local Authorities to co-operate with other relevant partners in promoting the welfare of children and ensure that their functions are discharged having regard to the need to safeguard and promote the welfare of children. This legislation provides statutory power to share information for the purposes of this Agreement.

4e Other legal powers

There may be a requirement to share information under other legal requirements and these are set out in Appendix 1.

4f Human Rights Act 1998

The Parties to this Agreement must observe Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), which provides for the right to respect for private and family life. The Human Rights Act 1998 gives effect to these rights in UK law.

5 Processing information

5a Making a request for, or providing, information

- I The Parties to this Agreement will nominate a 'Single Point of Contact' (SPOC) for sharing information with each other. SPOC's will ensure that appropriate staff within

their organisation are made aware of the provisions of this Agreement and how to implement the procedures for sharing information with the other Parties, stated in this agreement.

- II The Parties agree to respond to all requests for information as quickly as possible and to supply information which they consider to be relevant and proportionate to the enquiry. A record should be made of all requests received and the details of the disclosure made and by whom. The Parties agree that, due to the sensitivity of the information contained within communications between the Parties, letters, emails and other correspondence must be kept secure and only accessible by persons within the organisation on a strict 'need to know' basis. Parties will record the decision and its rationale on case management systems and must ensure that the information recorded is neither irrelevant nor excessive, and that the decision record and rationale is recorded separately to the primary case file.
- III The Parties agree to treat in confidence information received from the other Parties.

5b Information quality and relevance

- I When sharing personal data, the Parties agree to share only the minimum information necessary to enable them to identify whether the child or young person identified is at risk of harm or is in need of additional services and support.
- II The Parties agree that they will check the information that they disclose to each other is accurate and up to date at the time of disclosure. They also agree that they will notify the requesting party of any new information that comes to light following disclosure where this could assist in decision making.

5c Access

Staff access to personal information must be on a 'need to know' basis and any specific additional restrictions agreed within agencies. Care should be taken to ensure that access to personal information is restricted on this basis. Restrictions need to be re-enforced by clear policies on confidentiality and by inclusion of appropriate confidentiality clauses in staff contracts. Staff must be aware of and comply with their own organisation's information governance policies, procedures and training

5d Secure storage and transfer of personal information

Steps should be taken by all partners to ensure that personal information is held and transmitted securely. Should any information be printed staff are required to store this securely when not in use. Each party should ensure that staff are aware of and comply with their organisations Confidentiality, Information Security and Governance policies.

- All Parties understand their responsibilities for keeping personal data secure.
- Information will be stored in secured premises and not in areas to which the public has access.
- All Parties confirm that they have adequate security measures on their electronic systems to which information from other Parties may be transferred. The status of all personal data shared is "OFFICIAL SENSITIVE".

5e Retention of Records

Partners should keep their own records in relation to each case in accordance with their own organisations policies on the retention of records. Any records which no longer need to be retained in accordance with agencies' own policies and procedures should be destroyed under secure conditions. Any records held jointly by the BSCP will be maintained in accordance with Barnsley MBC's retention policies as lead for Data Protection matters. Statutory reviews (Rapid Reviews / Child Practice Reviews) will be published on the BSCP website.

All information obtained through this Information Sharing Agreement must be stored in each of the parties appropriate client case management system. No information should be stored by individuals in their own email systems. Once up to date information has been shared then there is a requirement for staff to update the appropriate client case management systems. This will avoid duplicate information storage across organisations and ensure the most up to date information is available within client case management systems and retention policies are applied.

5f Reporting a security incident or breach

- I Parties to the Agreement will have in place a mechanism for staff and the public to report information security incidents (for example, loss or theft of personal or confidential data held on computer equipment or paper) whether they are actual incidents or near misses. If personal data is lost or stolen and contains information which has been provided by another Party, the originating Party must be told and kept informed of the outcome of the investigation into the incident.
- II Any unauthorised release of information or breach of conditions in this Agreement will be dealt with through the internal disciplinary procedures of the individual Party to the Agreement.

5g Access to personal data

- I Individuals have a right to access personal data about them (subject to exemptions) under Chapter 3 of the Data Protection Act 2018 (Right of Access to Personal Data).
- II Any Party receiving a subject access request in relation to information originating from another Party should inform that Party that a request has been received.

6. Complaints

All complaints made in respect of disclosures made to or by the Parties will be brought to the attention of the SPOC. The complaint will be dealt with in accordance with the Party's own complaints procedure. Parties will keep each other informed of developments following a complaint received, where relevant and appropriate; and if necessary, brought to the attention of the BSCP.

7. Approval of the BSCP Information Sharing Agreement

The Information Sharing Agreement will be shared with all partners for approval and after any significant change, update or amendment. Partners are asked to:

- Share and implement the Agreement within each organisation.
- Support staff in the implementation of the Agreement through provision of training, advice and guidance
- Provide relevant information to facilitate monitoring and review.

All organisations that make up the multiagency Safeguarding Children Partnership will be invited as signatories to evidence acceptance of the Agreement. It will also be published on the BSCP website.

8 Publication of this Agreement

This Information Sharing Agreement may be published by each of the Parties in accordance with their obligations under the Freedom of Information Act 2000.

9 Agreement Review and Changes

The Parties to this Agreement will make sure that it is reviewed every three years and Earlier if required, to take account of any new legislation or official guidance.

10. Further Information. Links

[Working Together to Safeguard Children](#)

[Information Sharing: Advice for Practitioners Providing Safeguarding Services to Children, Young People, Parents and Carers \(includes The Seven Golden Rules for Information Sharing\)](#)

[The Information Commissioner's Office \(ICO\) website](#)

[Practice Guidance on Sharing Adult Safeguarding Information](#)

[GDPR \(General Data Protection Regulation\)](#)

[Data Protection Act](#)

[Barnsley Inter-Partnership Joint Working Protocol \(Link to follow\)](#)

[Barnsley Integrated Front Door Operational Guidance: Information Sharing](#)

Appendix 1

LEGAL POWERS AND DUTIES FOR DATA SHARING

Children Act 1989	<p>Section 17- Provision of services for children in need, their families and others.</p> <p>(i) It shall be the general duty of every local authority (in addition to the other duties imposed on them by this Part)-</p> <p>(a) to safeguard and promote the welfare of children within their area who are in need; and</p> <p>(b) so far as is consistent with that duty, to promote the upbringing of such children by their families, by providing a range of and level of services appropriate to those children's needs.</p> <p>Section 47 – Local Authority's duty to investigate</p> <p>(1) Where a local authority-</p> <p>(a) are informed that a child who lives, or is found, in their area-</p> <p>(i) is the subject of an emergency protection order; or</p> <p>(ii) is in police protection</p> <p>(b) have reasonable cause to suspect that a child who lives, or is found, in their area is suffering, or is likely to suffer, significant harm,</p> <p>the authority shall make or cause to be made, such enquiries as they consider necessary to enable them to decide whether they should take any action to safeguard or promote the child's welfare.</p>
Children Act 2004	<p>Section 10 – Co-operation to improve well-being</p> <p>(1) Each children's services authority in England must make arrangements to promote co-operation between—</p> <p>(a) the authority</p> <p>(b) each of the authority's relevant partners and</p> <p>(c) such other persons or bodies as the authority consider appropriate, being persons or bodies of any nature who exercise functions or are engaged in activities in relation to children in the authority's area.</p> <p>Section 11 – Arrangements to safeguard and promote welfare.</p> <p>(2) Each person and body to whom this section applies must make arrangements for ensuring that—</p> <p>(a) their functions are discharged having regard to the need to safeguard and promote the welfare of children; and</p> <p>(b) any services provided by another person pursuant to arrangements made by the person or body in the discharge of their functions are provided having regard to that need.</p>

Crime and Disorder Act 1998	<p>Section 17 – duty of each authority to exercise its functions with due regards to the likely effect of the exercise of those functions, and the need to do all that it reasonably can, to prevent crime and disorder in its area.</p> <p>Section 115 – any person who apart from this section would not have power to disclose information to a relevant authority or to a person acting on behalf of such an authority, shall have the power to do so in any case where the disclosure is necessary or expedient for the purposes of this act.</p>
Criminal Justice Act 2003	<p>Section 325 – the authority for each area must establish arrangements for the purpose of assessing and managing the risks posed in that area by relevant sexual or violent offenders and other persons who have committed offences who are considered by the authority to be persons who may cause serious harm to the public.</p> <p>Section 325 – interpretation of who is a relevant sexual offender.</p>
Education Act 2002	<p>Section 175 – a local education authority shall make arrangements for ensuring that the functions conferred on them in their capacity as a local education authority are exercised with a view to safeguarding and promoting the welfare of children.</p>
Local Government Act 1972	<p>Section 111(1) – a local authority shall have the power to do anything which is calculated to facilitate, or is conducive to or incidental to, the discharge of any of their statutory functions.</p>
Local Government Act 2000	<p>Section 2(1) – a local authority shall have the power to do anything which they consider is likely to achieve the promotion or improvement of the social well-being of their area.</p>
Human Rights Act 1998	<p>Article 8 Right to respect for private and family life</p> <p>1 Everyone has the right to respect for his private and family life, his home and his correspondence.</p> <p>2 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.</p>

Appendix 2

CALDICOTT PRINCIPLES

The Caldicott Report set out a number of general principles that health and social care organisations should use when reviewing its use of client information and these are set out below (Revised September 2013)

Principle 1. Justify the purpose(s) for using confidential information

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

Principle 2. Don't use personal confidential data unless it is necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3. Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

Principle 4. Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Principle 5. Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6. Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

Principle 7. The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Appendix 3

- **Domestic Violence Disclosure scheme**

The Domestic Violence Disclosure Scheme (DVDS) gives members of the public a formal mechanism to make enquires about an individual who they are in a relationship with, or who is in a relationship with someone they know, where there is a concern that the individual may be violent towards their partner. This scheme adds a further dimension to the information sharing about children where there are concerns that domestic violence and abuse is impacting on the care and welfare of children within the family.

Partner agencies can also request disclosure is made of an offender's past history where it is believed someone is at risk of harm. This is known as 'right to know'.

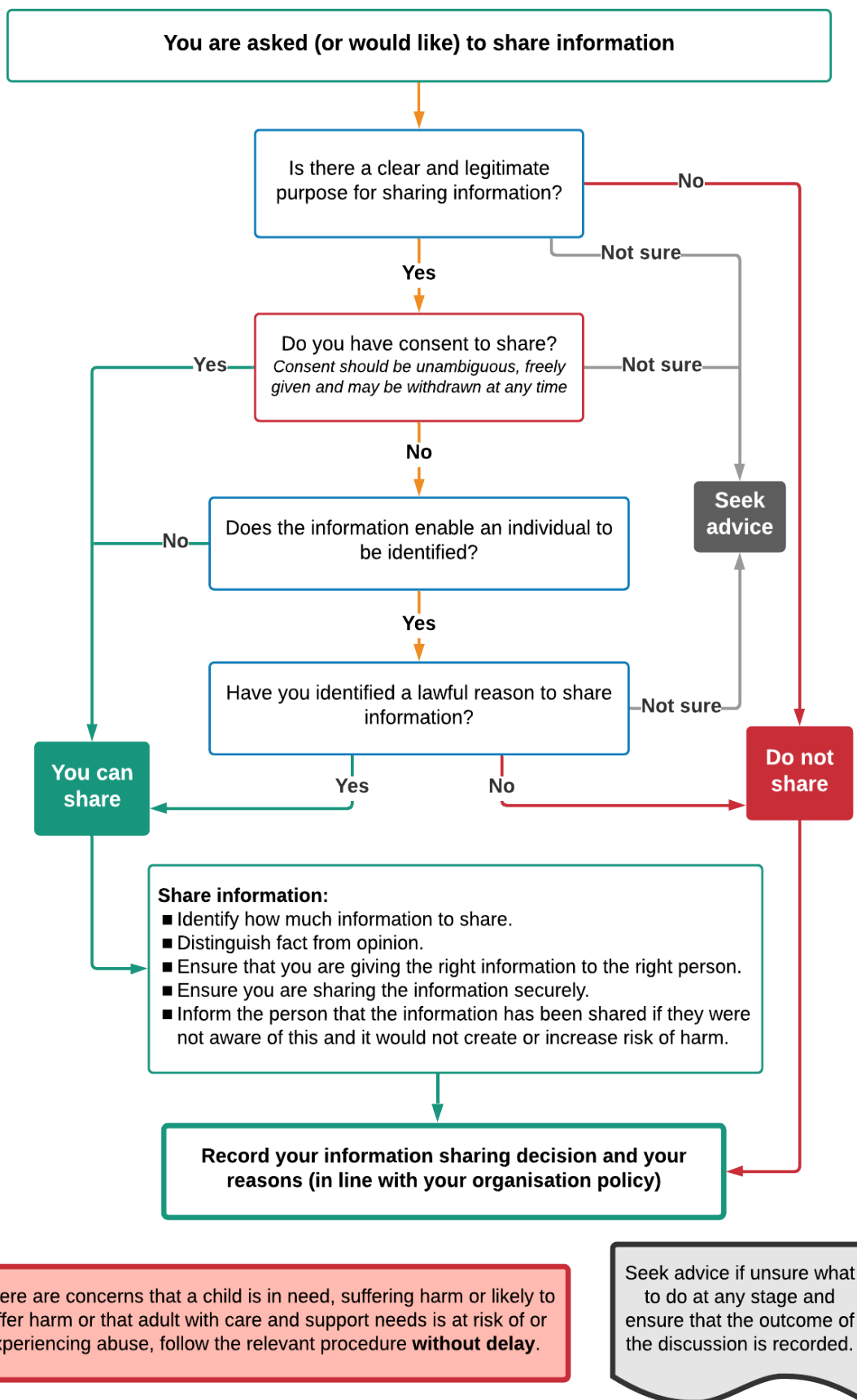
See: [Domestic Violence Disclosure Scheme: Guidance](#).

- **Child Sex Offender Disclosure Scheme**


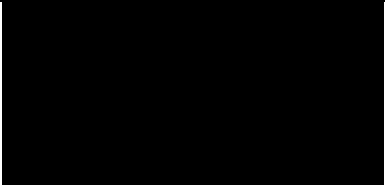
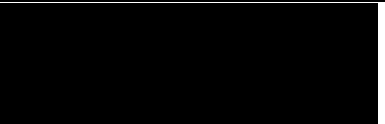
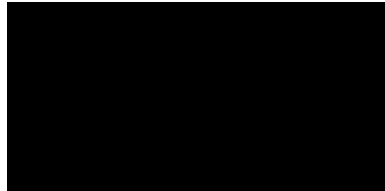
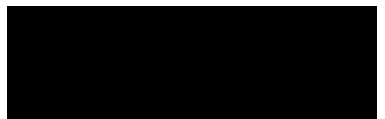

The Child Sex Offender Review (CSOR) Disclosure Scheme is designed to provide members of the public with a formal mechanism to ask for disclosure about people they are concerned about, who have unsupervised access to children and may therefore pose a risk. Police will provide details confidentially to the person most able to protect the child (usually parents, carers or guardians) if they think it is in the child's interests.

This scheme builds on existing, third-party disclosures that operate under the [Multi-Agency Public Protection Arrangements \(MAPPA\)](#).








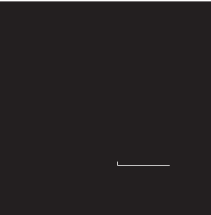
Guidance: Information Sharing Flowchart


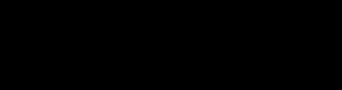
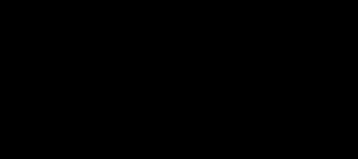

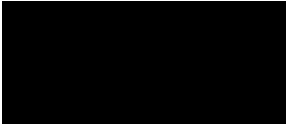
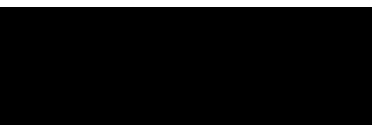
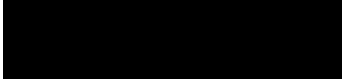



Appendix 5**Signatories to the Agreement**

ORGANISATION	PRINTED NAME & DESIGNATION (ROLE)	SIGNATURE & DATE
Academies Enterprise Trust (AET)		 Date: 15.06.2023
Barnardo's		 Date: 09.06.2023
Barnsley College		 Date: 02.05.2023
Barnsley CVS		 Date: 04.05.2023
Barnsley Hospital NHS Foundation Trust		 Date: 05.04.2023
Barnsley Metropolitan Borough Council		 Date: 04.05.23

Barnsley Sexual Abuse and Rape Crisis Service (BSARCs)			Date: 09.06.2023
Berneslai Homes			Date: 20.03.2023
Cafcass			Date: 14.06.2023
Compass Be			Date: 15.06.2023
Every Child Matters Academy Trust (ECM)			Date: 14 th June 2023
Federation CC (Academy Trust)			Date: 15.05.2023
Greenacre School			Date: 17.05.2023
Hallam Schools Partnership Academy Trust (HSPAT)			Date: 14.06.2023

HCAT		 Date: 05.05.2023
Healthwatch		 Date: 25.04.2023
Heather Garth Primary		 Date: 11.06.2023
Humankind		 Date: 16.05.2023
Independent Domestic Abuse Services (IDAS)		 Date: 18.05.2023
NHS South Yorkshire Integrated Care Board		 Date:03.05.2023
Oakwell Rise Primary Academy		 Date: 29.03.2023
Outwood Grange Academies Trust		 Date: 10.05.2023

Penistone Grammar School		 Date: 20.03.2023
Pioneer Academies Community Trust		 Date: 12.05.2023
Probation Service		 Date: 04.05.2023
South West Yorkshire Partnership NHS Foundation Trust (SWYFT)		 Date: 16.06.2023
South Yorkshire Fire and Rescue		 Date: 30.05.2023
South Yorkshire Police		 Date: 30/05/2023
Spectrum Community Health C.I.C.		 Date: 23.02.2023
United Learning (Academy Trust)		 Date: 12.06.2023

Upperwood Primary Academy (Standalone Academy)		 Date: 07/06/2023
Wellspring Academy Trust		 Date: 23.05.2023
Worsbrough Common Primary School		 Date: 29.03.2023

Version control

Version	Date	History	Author
1.0	27/09/2017	Original agreement	Julie Govan
1.1	16/05/2018	Inclusion of GDPR, additional membership	Lisa Loach
1.2	23/02/2023	Update and review	Annette Carey Strategic Safeguarding Partnership Manager
1.3	03/08/2023	Additional membership	BSCP
1.4	12/08/2024	Review	Rebecca Oates Project Officer, BSCP