Information Sharing Guidance for Practitioners

Contents

This document replaces all other local information sharing guidance and must be read in conjunction with the Derby and Derbyshire Safeguarding Children Procedures				
Version	**Author/s**	**Signed off by**	**Date**	**Review Date**
1.	Based on Tri-x template, amended by DSCB Policy Officers	DSCB Policy and Procedures Group	May 2019	May 2021

1. Introduction

Effective information-sharing underpins integrated working and is a vital element of both early intervention and safeguarding. Research and experience have shown repeatedly that keeping children safe from harm requires practitioners and others to share information 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; and
- Those who may pose a risk of harm to a child.

Often, it is only when information from a number of sources has been shared and is then put together, that it becomes 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 (e.g. they are being supported as a child in need or have a child protection plan).

Practitioners should also be alert to sharing important information about any adults with whom that child has contact, which may impact on the child's safety or welfare.

Those providing services to adults and children, for example GP's, may be concerned about the need to balance their duties to protect children from harm and their general duty of care towards their patient or service user, e.g. a parent. Some practitioners and staff face the added dimension of being involved in caring for or supporting more than one family member - the abused child, siblings, and an alleged abuser. However, in English Law, where there are concerns that a child is, or may be, at risk of significant harm, the overriding consideration is to safeguard the child (The Children Act 1989).

2. The General Data Protection Regulations (GDPR) and the Data Protection Act (2018)

The General Data Protection Regulations (GDPR) and the Data Protection Act (2018) supersede the Data Protection Act (1998). Practitioners must have due regard to the relevant data protection principles which allow them to share personal information.

The GDPR and Data Protection Act (2018) place greater significance on the need for organisations to be transparent and accountable in relation to their use of data. All organisations handling personal data must ensure they have comprehensive and proportionate arrangements for collecting, storing, and sharing information in place. This also includes arrangements on informing service users about the information they will collect and how this may be shared.

The GDPR and Data Protection Act (2018) does not prevent, or limit, the sharing of information for the purposes of keeping children and young people safe.

To effectively share information:

- All practitioners should be confident of the processing conditions which allow them to store, and share, the information that they need to carry out their safeguarding role. Information which is relevant to safeguarding will often be data which is considered 'special category personal data' meaning it is sensitive and personal;

- Where practitioners need to share special category personal data, they should be aware that the Data Protection Act 2018 includes 'safeguarding of children and individuals at risk' as one of conditions that allows practitioners to share information with others without consent:

    - Information can be shared legally without consent, if a practitioner is unable to, cannot be reasonably expected to gain consent from the individual, or if to gain consent could place a child at risk;

    - Relevant personal information can also be shared lawfully if it is to keep a child or individual at risk safe from neglect or physical, emotional or mental harm, or if it is protecting their physical, mental, or emotional well-being.

Practitioners looking to share information without consent should consider which processing condition in the Data Protection Act (2018) is most appropriate in the particular circumstances of the case. This may be the safeguarding processing condition or another relevant provision.

3. Severn Golden Rules for Information Sharing

1. Remember that the General Data Protection Regulations, Data Protection Act (2018) and human rights laws 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 or your information governance lead if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible;

4. Where possible share 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 reason to do so, such as where safety may be at risk. You will need to base your judgment 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;

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

6. Necessary, proportionate, relevant, 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 people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely (Practitioners must always follow their organisation's policy on security for handling personal information);

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. Information on children and families can be held in many different ways, including in case records or electronically on a variety of IT systems which are accessible to different practitioners. Information may be shared face to face, over the telephone or via secure email. Whenever information is shared, a record of this should be made in the individual's record and the information should not be kept any longer than is necessary. In some rare circumstances, this may be indefinitely, but if this is the case, there should be a review process scheduled at regular intervals to ensure data is not retained where it is unnecessary to do so.

4. Confidentiality and consent

Information sharing: advice for practitioners providing safeguarding services includes a Myth-busting guide that states:

> *Wherever possible, you should seek consent and be open and honest with the individual from the outset as to why, what, how and with whom, their information will be shared. You should seek consent where an individual may not expect their information to be passed on. When you gain consent to share it must be explicit and freely given.*
>
> *There may be some circumstances where it is not appropriate to seek consent, either because the individual cannot give consent, it is not reasonable to obtain consent, or because to gain consent would put a child or young person's safety or well-being at risk. Where a decision to share information without consent is made, a record of what has been shared should be kept.*

5. National Guidance on Sharing Information

Working Together to Safeguard Children (2018) states that:

- *"… all organisations and agencies should have arrangements in place that set out clearly the processes and the principles for sharing information. The arrangement should cover how information will be shared within their own organisation/agency; and with others who may be involved in a child's life;*

- *... all practitioners should not assume that someone else will pass on information that they think may be critical to keeping a child safe. If a practitioner has concerns about a child's welfare and considers that they may be a child in need or that the child has suffered or is likely to suffer significant harm, then they should share the information with local authority children's social care and/or the police. All practitioners should be particularly alert to the importance of sharing information*

when a child moves from one local authority into another, due to the risk that knowledge pertinent to keeping a child safe could be lost;

- *... all practitioners should aim to gain consent to share information, but should be mindful of situations where to do so would place a child at increased risk of harm. Information may be shared without consent if a practitioner has reason to believe that there is good reason to do so, and that the sharing of information will enhance the safeguarding of a child in a timely manner. When decisions are made to share or withhold information, practitioners should record who has been given the information and why."*

In addition to the above Derby and Derbyshire Safeguarding Children Boards (DSCBs), on occasion may request information from an organisation in order to fulfil their statutory functions to co-ordinate and ensure the effectiveness of safeguarding. This includes information to support quality assurance processes such as multi-agency audit as well as learning reviews and serious case reviews.

The Derby and Derbyshire Safeguarding Partnership will replace the DSCBs in September 2019, may also require any person or organisation or agency to provide them with specified information to enable and assist the safeguarding partners to perform their functions to safeguard and promote the welfare of children in their area, including as related to local and national child safeguarding practice reviews.

Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers (2018) supports frontline practitioners working in child or adult service who have to make decisions about sharing personal information on a case-by-case basis. The guidance can be used to supplement local guidance and encourage good practice in information sharing."

For further information about local Information Sharing Agreements please see the DSCBs multi-agency safeguarding children procedures, document library.

The General Data Protection Regulation (GDPR) and Data Protection Act (2018) are based on existing best practice associated with the Data Protection Act (1998). They ensure personal information is obtained and processed fairly and lawfully; only disclosed in appropriate circumstances; is accurate, relevant and not held longer than necessary; and is kept securely.

They balance the rights of the information subject (the individual whom the information is about) with the need to share information about them.

The GDPR and the Data Protection Act (2018) introduce new elements and provide an opportunity for organisations to review their current data protection and privacy practices. The Data Protection Act 2018 sets out the lawful grounds for processing of special category personal data – including without consent if the circumstances justify it – where it is in the substantial public interest to safeguard children and individuals at risk.

Further details are set out in the SCHEDULE 8 Section 35(5) of the Data Protection Act (2018) which states:

1.4 (1) This condition is met if—

a. The processing is necessary for the purposes of:
    i. Protecting an individual from neglect or physical, mental or emotional harm; or
    ii. Protecting the physical, mental or emotional well-being of an individual.

b. The individual is:
    i. Aged under 18; or
    ii. Aged 18 or over and at risk.

Where there is a clear risk of significant harm to a child, or serious harm to adults the decision to share information is clear, as actions must be taken to respond to the disclosure. In other cases, for example, neglect, the indicators may be more subtle and appear over time. In these cases, decisions about what information to share, and when, may be more difficult to judge. Decisions in this area need to be made by, or with the advice of, people with suitable competence in Child Protection work such as named or designated practitioners or senior managers. The information shared should be proportionate.

Caldicott Guardian Principles:

A Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing.

The Seven Caldicott Principles

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

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

3. Use the minimum necessary personal confidential data;

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

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

6. Comply with the law;

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

The Guardian plays a key role in ensuring that the NHS, Local Authority Social Services Departments and partner organisations satisfy the highest practicable standards for handling patient/client identifiable information.

Section 115 of the Crime and Disorder Act (1998) establishes:

The power to disclose information is central to the Act's partnership approach. The Police have an important general power under common law to disclose information for the

prevention, detection and reduction of crime. However, some other public bodies that collect information may not previously have had power to disclose it to the Police and others. This section puts beyond doubt the power of any organisation to disclose information to Police authorities, local authorities, Probation Service, Health Authorities, or to persons acting on their behalf, so long as such disclosure is necessary or expedient for the purposes of crime prevention. These bodies also have the power to use this information.

Part 3 of the Data Protection Act (2018) covers the processing of personal data for 'law enforcement purposes'. It covers processing for the prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

The 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.

Members of the public can make an application for a disclosure, known as the 'right to ask'. Anybody can make an enquiry, but information will only be given to someone at risk or a person in a position to safeguard the victim. The scheme is for anyone in an intimate relationship regardless of gender.

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'.
If a potentially violent individual is identified as having convictions for violent offences, or information is held about their behaviour which reasonably leads the police and other agencies to believe they pose a risk of harm to their partner, a disclosure will be made.

Article 8 in the European Convention on Human Rights states that:

Everyone has the right to respect for their private and family life, home and correspondence:

There shall be no interference by a public authority with the exercise of this right except such as 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 rights and freedoms of others.

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. This scheme builds on existing, well established third-party disclosures that operate under the Multi-Agency Public Protection Arrangements (MAPPA).

Police will reveal 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.

The scheme is managed by the Police and information can only be accessed through direct application to them.

If a disclosure is made, the information must be kept confidential and only used to keep the child in question safe. Legal action may be taken if confidentiality is breached. A disclosure is delivered in person (as opposed to in writing) with the following warning:

If the person is unwilling to sign the undertaking, the police must consider:

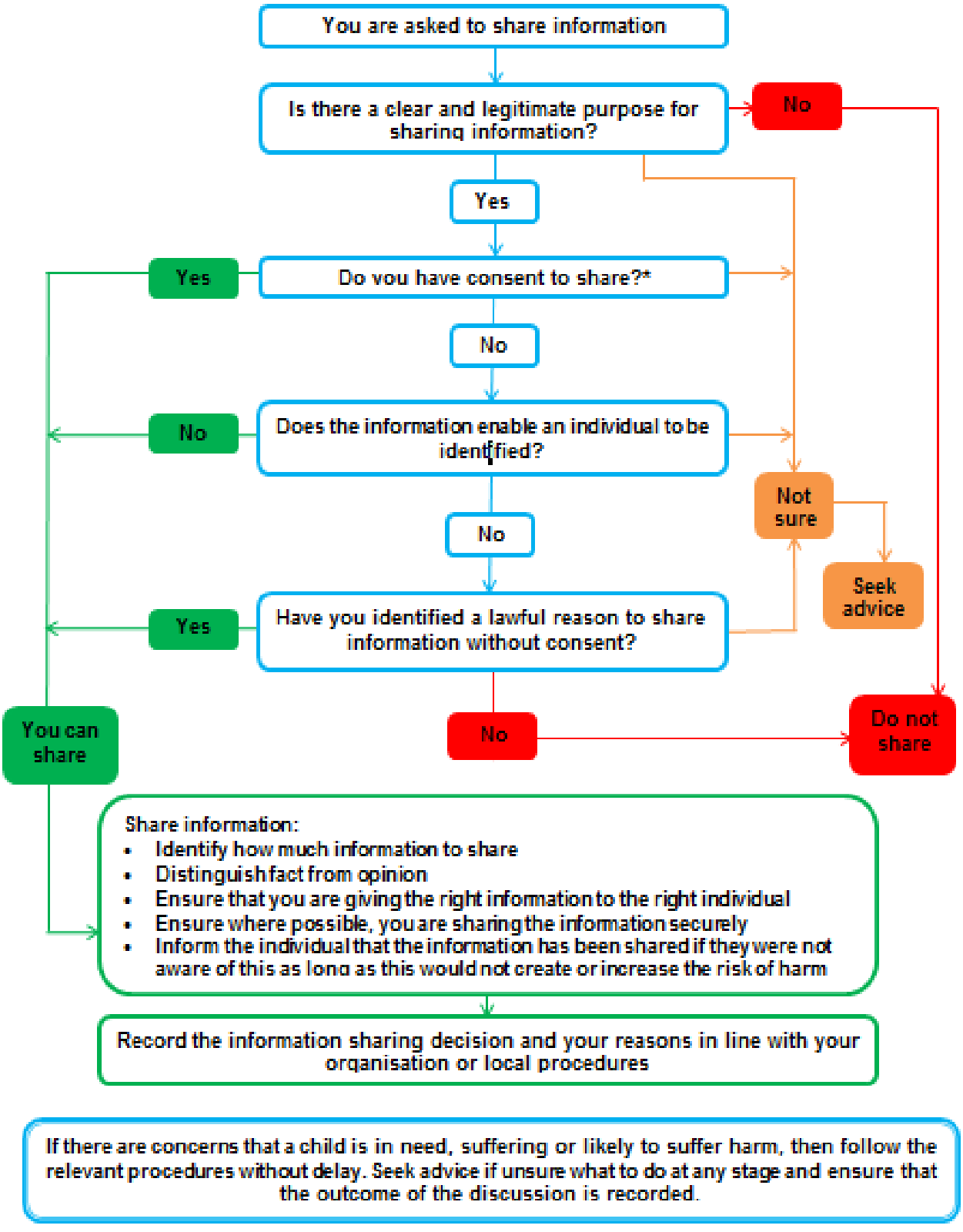
- 'That the information must only be used for the purpose for which it has been shared i.e. in order to safeguard children;
- The person to whom the disclosure is made will be asked to sign an undertaking that they agree that the information is confidential and they will not disclose this information further;
- A warning should be given that legal proceedings could result if this confidentiality is breached. This should be explained to the person and they must sign the undertaking' (Home Office, 2011, p16).

If the person is unwilling to sign the undertaking, the police must consider whether the disclosure should still take place.

Further Information

- Information sharing: advice for practitioners providing safeguarding services
- The Information Commissioner's Office (ICO)
- Practice guidance on sharing adult safeguarding information

Appendix 1. Flowchart of when and how to share information



*Consent must be unambiguous, freely given and may be withdrawn at any time

Taken from Information sharing; advice for practitioners providing safeguarding services to children, young people, parents and carers (2018) Page 12