Information Sharing

Information sharing is essential for effective safeguarding & promoting the welfare of children and young people. In many serious case reviews, it is a key factor when opportunities are missed to keep children safe.

Practitioners are responsible for sharing appropriate information & cannot assume someone else will do it.

Sharing information between practitioners, agencies, the child or young person and their families, is essential to:

- Multi-agency working
- Co-ordinating offers of early help
- Reducing the risk of harm
- Assisting with public protection

Governing bodies should ensure their setting:

- Has a policy that reflects the procedures & practice of the local authority & Sheffield Children Safeguarding Partnership (SCSP)
- Supplies information to the SCSP, e.g. your safeguarding team details, via Schoolpoint 365; & the SCSP Safeguarding Annual Audit
- Understands local assessment protocols & the SCSP's Thresholds of Need Guidance
- Attends, supports, and contributes to child protection conferences and plans
- Allows access for children's social care to consider whether to conduct a section 17 or a section 47 assessment
- Informs pupils/students and their families, through a leaflet, website, or prospectus, about how they store & use all their information

The GDPR and Data Protection Act 2018:

- Place greater significance on organisations being transparent and accountable for their data use
- Require organisations to have comprehensive and proportionate arrangements for collecting, storing, and sharing information
- **Do not prevent, or limit, information sharing to keep children and young people safe.**

To effectively share information:

- Be confident about your processing conditions: safeguarding data is often 'special category personal data' i.e., sensitive & personal
- The Data Protection Act 2018 includes 'safeguarding of children and individuals at risk' as a condition that allows practitioners to share information without consent
- Information can be shared:
  - Legally without consent if a practitioner is unable to or cannot be reasonably expected to gain consent; or if to gain consent could place a child at risk
  - Lawfully if to keep a child or individual at risk safe from neglect or physical, emotional, or mental harm, or to protect their physical, mental, or emotional well-being.

The General Data Protection Regulation 2018 reflects the progress of digital technology and the use of social media platforms.

Myth busting:

- **The GDPR & Data Protection Act 2018 are barriers to sharing information:** no, they provide a framework to share appropriately, balancing the rights of the information subject & the need to share their information
- **Consent is always needed to share personal information:** no, e.g. where gaining consent would put a child or young person's safety or well-being at risk. Where possible seek consent & be open & honest about why, what, how and with whom information will be shared. Consent must be explicit and freely given. When sharing with or without consent (see below) or choosing not to share, record the reasons why
- **Personal information collected by one organisation cannot be disclosed to another:** if children are in need or at risk of significant harm, it is unlikely there will be a legal barrier to sharing their personal information; consider which processing condition in the Data Protection Act 2018 is most appropriate for use.
- **The common law duty of confidence & Human Rights Act 1998 prevent personal information sharing:** no, practitioners need to balance this against the effect on individuals at risk if they do not share; sharing with consent is not a breach, without consent requires grounds e.g. the subject/public interest, court order etc.
- **IT Systems are a barrier to effective information sharing:** no, IT systems can be useful in supporting information sharing; however professional judgment is the most essential aspect of multi-agency work, which could be put at risk if organisations rely too heavily on IT systems.

Information Sharing

Seven golden rules:

1. **GDPR, the 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, 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 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 still share information without consent if, in your judgement, there is a lawful basis to do so, such as where safety 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
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 (see principles)
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 sharing: advice for practitioners providing safeguarding services, DfE 2018

Principles:

Use your judgement & organisational procedures to decide what information to share and when and consult your manager if in doubt.

Always consider whether sharing information is needed to safeguard & protect a child.

Necessary and proportionate:

- How much information do you need to release?
- Impact on the subject & third parties
- Share proportionately to need and level of risk

Relevant:

- Only relevant information should be shared
- Only share with those who need it
- Allows others to make informed decisions

Adequate:

- Information should be adequate for its purpose & the right quality to ensure that it can be understood and relied upon

Accurate:

- Accurate & up to date information, clearly distinguishing between fact and opinion
- If historical then this should be explained

Timely:

- Share in a timely fashion to reduce missed opportunities to offer support and protection
- In emergencies you might not seek consent if it causes delays & places a child at increased risk

Secure:

- Share appropriately and securely
- Always follow your organisation's policy on security for handling **any** personal information

Record:

Record all decisions & the procedure followed and whether you decided to share. If shared:

- what you shared, why & who you shared with
- who you discussed your decision with, and if not shared, the reasons why not?

Always review retained information regularly and do not keep longer than necessary.

Useful web links/resources:

- Information sharing advice for safeguarding practitioners, DfE 2018
- Data Protection Toolkit for Schools, DfE 2018