Information Sharing

Sharing information is an intrinsic part of every frontline practitioner's role when working with children and young people. The decisions about how much information to share, with whom and when, can have a profound impact on individuals' lives. Appropriate sharing of information relies on everyone having a clear understanding of what the benefits and risks associated with doing so are, supported by robust procedures to ensure that sharing is always:

- **Justifiable:** what is the policy framework within which sharing is taking place?
- **Proportionate:** how do you ensure you do not under or over-share?
- **Controlled:** what systems do you have in place to ensure that actions and decisions are recorded and risks managed?

For example, it could ensure that an individual receives the right services at the right time and prevent a need from becoming more acute and difficult to meet. In extreme cases, it could be the difference between life and death. Being overprotective can be as dangerous as over-sharing; poor or non-existent information sharing is a factor repeatedly flagged up as an issue in Serious Case Reviews carried out following the death of, or serious injury to, a child.

The seven golden rules to sharing information

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, 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 the agreement of the information owner, 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 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 the agreement of the information owner, or if the legal basis for sharing has not been clearly explained to the data subject, be mindful, 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.

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.

The Data Protection Act 2018

Sharing personal data brings with it additional legal requirements, including significant regulator penalties or legal action if school systems, policies and procedures are defective. The Data Protection Act 2018 ('DPA') is designed to protect the privacy of individuals' personal data by requiring data controllers and processors to handle it in accordance with a set of data protection principles.

The terms 'controller' and 'processor' describe the responsibilities in a relationship between two people or organisations that are processing personal data. A controller determines the purposes and means of the processing, and a processor is responsible for processing personal data on behalf of a controller. In education settings, a school will be a data controller, and any third party that provides it with a service that requires it to handle personal data (for example, a contractor providing IT services) would be its data processor.

The Data Protection Principles require schools that intend to process personal data to determine in advance:

- What the purpose of the processing is;
- On what legal basis the processing will take place (there are six);
- What personal data will be processed, and particularly is any special category data is involved;
- Who the personal data will be shared with to facilitate the intended purpose of the processing, including with which data processors;
- How long the personal data will be retained; and
- What security measures might need to put in place over and above the norm.

All of these details must be recorded in a document kept by the school called the **Record of Processing Activity** (ROPA). The data subjects affected (i.e. the people whose personal data is being processed) must be informed via a Privacy Notice (PN). These must be freely accessible to affected data subjects, including staff, pupils and governors.

Appropriate sharing of personal data

With all of the above elements in place, answering most questions about whether or not it is appropriate to share personal data should be straightforward. The ROPA should record with whom and in what circumstances personal data will be shared.

Where the ROPA is silent or unclear you need to determine whether sharing the personal data would be appropriate; ask yourself:

- Is it in the interests of the data subject that the personal data be shared, does it benefit them or potentially cause them harm?

- Does the mechanism through which sharing is taking place create a security breach risk that would potentially harm the data subject?
- Can the proposed specific act of sharing be reasonably interpreted within the original intended purpose, as stated in the PN?

Example 1: You need to pass on details of a child showing signs of harm to social services. Sharing personal data with social services will be a routine activity of any school. This processing activity should therefore be captured in generic form in the school ROPA, under which any sharing of specific case details will be captured.

Example 2: You are holding a sports day with another school and they have asked for the names of the children taking part, and details of any pre-existing medical conditions to satisfy their health and safety rules.
Other entries in your ROPA are likely to cover this sharing, but if not:

- Sharing is clearly in the interests of the children and staff concerned;
- The sharing is reasonable and proportionate;
- There is a clear legal basis for the sharing as carrying out a suitable risk assessment is a statutory requirement.

However: as health information is special category data, you may want to ensure that the action is recorded in your ROPA, and update your PNs if necessary; AND

- Ask how the information is to be communicated securely? What does your Security Policy say? E.g. if the data is to be emailed appropriate digital protection must be applied, e.g. via data encryption (or at least password protected) document.
- If in any doubt, check with your Data Protection Officer.

Where the risk of harm is potentially high, or where special category data is involved, you must consult your Data Protection Officer before sharing data. The law defines special category data as:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

This does not include personal data about criminal allegations, proceedings or convictions, as separate rules apply.

The Best Interests of the Child

Fears about sharing information cannot be allowed to stand in the way of the need to safeguard and promote the welfare of children, particularly if they are at risk of abuse or neglect, or of school staff. No practitioner should assume that someone else will pass on

information which may be critical to keeping a child or staff member safe. The concept of the best interests of the child comes from Article 3 of the United Nations Convention on the Rights of the Child (UNCRC):

> *"In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration."*

It is important to note that children below the age of 13 years are unable to provide informed consent. Where this is relied on as a legal basis for processing, consent can only be provided by a parent or legal guardian.

Is consent always needed to share personal information?

Consent, when relied upon to create a legal basis for processing, must always be explicit and informed (one of the major changes in the 2018 law). It is still possible to share personal information if it is necessary in order to carry out your role, or to protect the vital interests of the individual where, for example, consent cannot be given. You do not necessarily need the consent of the information subject to share their personal information because this ability should be captured within the school's record of processing.

For example, if it is unsafe or inappropriate to do so, i.e. where there are concerns that a child is suffering, or is likely to suffer significant harm, you would not need to seek consent. A record of what has been shared should be kept.

When and why are we legally required to gain consent from the parents and (where possible) the child?

- Non-statutory Services - *need consent*
- Section 17 – Child in need of additional support -*need consent*
- Section 47 – Child at risk of significant harm – *no consent required although best practice*

When may seeking consent place a child at risk of significant harm?

- Suspected sexual abuse
- Suspected fabricated/induced illness
- Forced marriage/honour based abuse
- Some cases of Domestic Abuse

Student Subject Access Requests

A student, or someone acting on their behalf, has the right to make a request to see any personal data their school holds about them and why. All pupils have a right to see their own personal information. It must be provided should they ask.

Parents are only entitled to access the personal information held about their child if the child is unable to act on their own behalf, or if the child has given consent to their parent. Even if the child is young, the personal data being held is still their personal data. It doesn't belong to anyone else, including their parents or guardian.

When and how to share information

When asked to share information, you should consider the following questions to help you decide if and when to share. If the decision is taken to share, you should consider how best to effectively share the information.

When

Is there a clear and legitimate purpose for sharing information?
- Yes – see next question
- No – do not share

Does the information enable an individual to be identified?
- Yes – see next question
- No – you can share but should consider how

Is the information personal or confidential?
- Yes – see next question
- No – you can share but should consider how

Is there another reason to share information such as to fulfil a public function or to protect the vital interests of the information subject?
- Yes – you can share but should consider how
- No – do not share

How
- Identify how much information to share
- Distinguish fact from opinion
- Ensure that you are giving the right information to the right individual
- Ensure where possible that you are sharing the information securely
- Inform the individual that the information has been shared if they were not aware of this, as long as this would not create or increase risk of harm

All information sharing decisions and reasons must be recorded in line with your organisation or local procedures. **If at any stage you are unsure about how or when to share information, you should seek advice from your Data Protection Officer and ensure that the outcome of the discussion is recorded.** If there are concerns that a child is suffering or likely to suffer harm, then follow the relevant procedures without delay.

Additional guidance and further reading

- EPHA website – dedicated page https://essexprimaryheads.co.uk/info-anddocuments/data-protection/
- Information Management Toolkit for Schools 2019
- Information sharing advice for safeguarding practitioners March 2015
- ROPA model template for schools (EPHA website)
- Data protection guide for schools – Information Commissioner's Office https://ico.org.uk/
- Essex Schools Infolink https://schools-secure.essex.gov.uk/data/informationgovernance/Pages/DataProtectionAct1998.aspx
- Whole Essex Information Sharing Framework https://weisf.essex.gov.uk/

This briefing paper relates to **information sharing**– to develop your understanding of data protection issues further, follow up with the additional 7-minute staff meetings:
Data Protection Principles, Records Management and Data Security and the Introduction to GDPR.