Information Sharing

The Data Protection Act 2018 is designed to protect the privacy of individuals. It requires that any personal information about an individual is processed securely and confidentially.

This includes both staff and pupils. How a school obtains, shares and uses information is critical, as personal data is sensitive and private. Everyone, adults and children alike, has the right to know how the information about them is used. The Data Protection Act requires schools to strike the right balance in processing personal information so that an individual's privacy is protected. Applying the principles to all information held by schools will typically achieve this balance and help them to comply with the legislation.

Personal data is information that relates to an identifiable living individual that is processed as data. Processing amounts to collecting, using, disclosing, retaining or disposing of information. The data protection principles apply to all information held electronically or in structured paper files.

Sensitive personal data is information that relates to race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical and mental health, sexuality and criminal offences. Sensitive personal data is given greater legal protection as individuals would expect certain information to be treated as private or confidential – for example, a headteacher or member of staff may have a school e-mail account that is made publicly available on the school's website whereas their home e-mail account is private and confidential and should only be available to those to whom consent had been granted.

Sharing information is an intrinsic part of any frontline practitioner's job 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. 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. At the other end of the spectrum it could be the difference between life and death. 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.

Fears about sharing information cannot be allowed to stand in the way of the need to safeguard and promote the welfare of children at risk of abuse or neglect. No practitioner should assume that someone else will pass on information which may be critical to keeping a child safe.

Sharing Personal Information

There are occasions where sharing personal data with local authorities, other schools, different departments or social services cannot be avoided. It may be that without sharing the data, actions cannot be completed. For example, you may need to pass on details about a child showing signs of harm to social services, or another school may need to know which pupils will be present at their sports day event.

You must consider all the legal implications and ensure that you have the ability to share the specified data. For example, what is the intention behind sharing? Who requires the data, which data is needed and what will it be used for?
Consent must be given by the individual before their personal information can be shared, unless there are reasons to believe that there may be a risk of significant harm.
This applies whether you are sharing data between people or online, such as photographs on the school's Facebook page.

Data should only be transferred to other countries if they have suitable or equivalent security measures. All European Union countries have equivalent data protection rules, so it's safe to transfer to them if necessary. However, explicit consent should be acquired from the individual if personal data needs to be processed outside of the UK. If the school cannot establish a safe system of data protection with a country outside the EU, they should not even consider sharing personal data.

The seven golden rules to sharing information

1. Remember that the Data Protection Act 1998 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. Share with informed consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, there is good reason 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 certain of the basis upon which you are doing so. Where you 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.

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.

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 confidential?

- Yes – see next question
- No – you can share but should consider how

Do you have consent?

- Yes – you can share but should consider how
- No – see next question

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 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.

Is consent always needed to share personal information?

You do not necessarily need the consent of the information subject to share their personal information. Wherever possible, you should seek consent or be open and honest with the individual (and/or their family, where appropriate) 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 and they have a genuine choice about this.

Consent in relation to personal information does not need to be explicit – it can be implied where to do so would be reasonable, i.e. a referral to a provider or another service. More stringent rules apply to sensitive personal information, when, if consent is necessary then it should be explicit. But even without consent, or explicit consent, 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.

Also, 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.

Before responding to a subject access request for information, you need to consider whether the child is mature enough to understand their rights. If they are, then your response to the request should go to the child, not their parent.

Additional guidance and further reading

- EPHA website – dedicated page https://essexprimaryheads.co.uk/info-and-documents/data-protection/
- Information Management Toolkit for Schools 2019
- Information sharing advice for safeguarding practitioners March 2015
- Data protection guide for schools – EPHA July 2017
- Information Commissioner's Office https://ico.org.uk/
- Essex Schools Infolink https://schools-secure.essex.gov.uk/data/information-governance/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, follow up with the additional 7-minute staff meetings:

- Data Protection principles
- Data management and Information security