Data Protection Principles

The Data Protection Act 1988 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.

To comply with the act, schools must observe the eight 'data protection principles', ensuring that:

- Personal data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under this Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

In practice, it means that schools must:

- have legitimate grounds for collecting and using the personal data;
- not use the data in ways that have unjustified adverse effects on the individuals concerned;

- be transparent about how they intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- handle people's personal data only in ways they would reasonably expect; and
- make sure they do not do anything unlawful with the data

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.

The principles also extend to educational records – the names of staff and pupils, dates of birth, addresses, national insurance numbers, school marks, medical information, exam results, SEN assessments and staff development reviews.

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 head teacher 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.

You also need to differentiate between personal information that individuals would expect to be treated as private or confidential (whether or not legally classified as sensitive personal data) and personal information you can make freely available.
For example: the headteacher's identity is personal information but everyone would expect it to be publicly available. However, the head's home phone number would usually be regarded as private information.

What must schools and academies do?
Schools must notify the ICO (Information Commissioner's Office) that they are processing personal data.
Schools should ideally nominate an individual (typically, the School Business Manager) as the 'Data Controller'. If the principal role and responsibilities for information is not designated, the school will be the Data Controller (or rather the governing body or equivalent) as the appropriate 'body corporate'.

The school should have clear, practical policies and procedures on information governance for staff and governors to follow, and needs to monitor their operation. These should include:

- Data Protection Policy
- Staff Code of Conduct – the Essex HR model includes use and control of data
- Privacy notices for staff and parents/pupils
- Record Management Policy *(not mandatory, but good practice)*

Data protection legislation entitles an individual the right to request the personal information a school holds on their behalf – this is known as a ***Subject Access Request*** *(SAR)* and includes all and any information held by the school, not just that information held on central files or electronically, so it could also include correspondence or notes held by others in the school.

SARs must be responded to within 40 calendar days of receipt. The SAR should be made in writing by the individual making the request. The school may charge a fee for dealing with this request, typically £10. Parents can make SARs on behalf of their children if the children are deemed to be too young or they have consented to their parents doing so on their behalf.

Staff need to know and understand

- How to manage, keep and dispose of data
- The school's procedures in relation to pupil records, email, social media, taking photos in schools, mobile technology and the school website
- When they are allowed to share information with others and how to make sure it is kept secure when shared.

This briefing paper relates to the data protection principles – to develop the staff understanding of these issues, follow up with the additional 7-minute staff meetings:

- Information sharing
- Data management and Information security

Additional guidance and further reading

- EPHA website – dedicated page https://essexprimaryheads.co.uk/info-and-documents/data-protection/
- Data Protection Toolkit for Schools – DfE August 2018
- Data protection guide for schools – EPHA July 2017
- Information Commissioner's Office https://ico.org.uk/
- NAHT guide –data and its use in schools
- ICO Data Protection guide for schools
- ICO guide to taking photos in schools
- Information Management Toolkit for Schools 2019
- Information sharing advice for safeguarding practitioners July 2018
  Essex Schools Infolink
- https://schools-secure.essex.gov.uk/data/information-governance/Pages/DataProtectionAct1998.aspx