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. Good data protection practices ensure that an organisation and the individuals within it can be trusted to collect, store and use our personal data fairly, safely and lawfully.

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 and all those who process others' personal data have to follow strict rules.

These rules are set primarily by:

- the UK General Data Protection Regulation (UK GDPR)
- the Data Protection Act 2018 (DPA)

The UK GDPR sets out 7 key principles that should guide you in processing personal data. Those principles are:

- lawfulness, fairness and transparency
- purpose limitation
- data minimisation
- accuracy
- storage limitation
- integrity and confidentiality (security)
- accountability

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 identified or identifiable living individual.

In a school, examples of personal data include:

- identity details (for example, a name, title or role)
- contact details (for example, an address or a telephone number)
- information about pupil behaviour and attendance
- assessment and exam results
- staff recruitment information
- staff contracts
- staff development reviews
- staff and pupil references

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.

Special category data is personal data that's considered more sensitive and given greater protection in law. Special category data includes:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade-union membership
- genetic information
- biometric information (for example, a fingerprint)
- health matters (for example, medical information)
- sexual matters or sexual orientation

In a school, it would be best practice to also treat as special category data any personal data about:

- a safeguarding matter
- pupils in receipt of pupil premium
- pupils with special educational needs and disability (SEND)
- children in need (CIN)
- children looked after by a local authority (CLA)

Criminal offence data is personal data that's treated in a similarly sensitive way to special category data. It records criminal convictions and offences or related security measures. Criminal offence data includes:

- the alleged committing of an offence
- the legal proceedings for an offence that was committed or alleged to have been committed, including sentencing

Schools process criminal offence data in storing the outcome of a Disclosure and Barring Service (DBS) check on their employees, non-employed staff and volunteers. As this data relates to criminal convictions, collecting and retaining it means the school is processing criminal offence data. This applies even though the check has not revealed any conviction.

Managing data

Schools collect, store and use personal data about a variety of individuals. In this context, those individuals are known as data subjects.
A school's data subjects include:

- pupils and former pupils
- parents and carers
- employees and non-employed staff
- governors and trustees
- local-authority personnel
- volunteers, visitors and applicants

Schools hold personal data in several forms. These are collectively known as its data assets.
Data assets comprise:

- data items – single pieces of information
- data item groups – data items about the same process
- data sets – collections of related data that can be manipulated as a unit by a computer
- systems – administrative software
- system groups – the larger systems housing administrative software

A data breach is a security incident that results in personal data a school holds being:

- lost or stolen
- destroyed without consent
- changed without consent
- accessed by someone without permission

Data breaches can be deliberate or accidental. A breach is about more than just losing personal data.

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 February 2023 https://www.gov.uk/guidance/data-protection-in-schools/what-data-protection-means-for-schools
- 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