Data Protection Principles

The Data Protection Act 2018 and the General Data Projection Regulation (GDPR) are designed to protect the privacy of individuals. The provisions of the GDPR still apply, albeit as UK statute, even though we have now left the EU. They require that any personal information about an individual is processed securely and in accordance with a stated legal basis.

This includes both staff and pupils. How a school obtains, shares and uses information is critical, as personal data may be 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.

The **six principles of data protection in GDPR** are that data must be:

(1) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(2) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(3) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(5) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(6) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

In practice, this means that schools must:

- have legitimate grounds for collecting and using the a person's 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 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. Personal information can be defined as anything relating to an individual that identifies them. This applies to both physical and digital records. Processing amounts to collecting, using, disclosing, retaining or disposing of information.

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, financial records, SEN assessments and staff development reviews.

Special category 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.

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 special category 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.

Even this oversimplifies the sharing of data. For example: the fact that J in Year 2 has asthma might be well known because her mum tells everyone, but that doesn't mean the school should necessarily disclose it to all and sundry; however, disclosure of medical information with competent authorities might be necessary; e.g. if you need to call for an ambulance.

Consequently, you can't determine openness based only on the data type - it's the nature of the data and the circumstances together that determine if a processing activity is lawful.

What must schools and academies do?

- *Schools must notify the ICO (Information Commissioner's Office) (annually) that they are processing personal data.*
- *As the "data controller" schools must appoint a Data Protection Officer (DPO)*

The DPO's responsibilities include:

- ✓ Mediating contact between an organisation and the relevant supervisory authorities.
- ✓ Training all employees on applicable GDPR compliance requirements.
- ✓ Conducting regular assessments and audits to guarantee total GDPR compliance.

- ✓ Sustaining records of any company-wide data processing activities.
- ✓ Replying to data subjects to educate them on how their personal data is stored, secured, and used by the company.
- ✓ Outlining to staff, parents and pupils all data protection measures have been implemented.
- ✓ Responding to requests to share copies of personal data or erasing data as and when necessary.

Schools must have measures in place to prevent breaches of data through their internet, intranet, and email systems.

- ✓ Monitor all 'live' files to make sure they are updated and accurate.
- ✓ Send out a letter at the beginning of each school year urging parents and pupils to check that all of their personal details are correct. This is a great way to avoid emergencies; especially when emergency contact information is out of date.
- ✓ Amend all information that is inaccurate immediately.
- ✓ Destroy all personal data that is no longer needed or out-of-date. This could involve deleting computer files, shredding documents, or formatting hard drives securely so that all information is permanently erased and inaccessible.
- ✓ Adhere to the IRMS toolkit for schools 2019, which states the duration that certain types of personal information can be retained before they must be destroyed. Note that some stipulations are legally required while others are recommended for best practice.

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

Privacy Notices

When you collect information concerning a parent, child, or member of staff, you must offer transparency about how this information will be used. Your school has to explain precisely how you will process the personal information of all staff and pupils. Examples include how to arrange school trips, facilitate education, or store grades and exam results.

To ensure GDPR compliance, schools must display clear privacy notices. The purpose of a privacy notice is to present and summarise what information the school requires, why this information is being collected, and which third-parties are privy to such data. The individual whom the information relates to must give full consent to your school in order for you to store it. Primary and secondary schools have different data requirements. For this reason, every single school must have its own privacy policy covering the processing activities that are specific to their school.

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.

Schools must responds to Subject Access Requests to within 30 calendar days of receipt. The SAR should be made in writing by the individual making the request. 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
- GDPR https://gdpr-info.eu/
- 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
- IRMS 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
- https://cpdonline.co.uk/knowledge-base/business/data-protection-in-schools-all-you-need-to-know/#what-is-data-protection