GDPR Guidance: Employee Briefing

A summary of the key points of the General Data Protection Regulations (2016)

1. **What is Data Protection Law?:** GDPR comes into force on the 25th May 2018 and will be part of the Data Protection Act 2018 (more)
2. **What is personal data?:** Information that on its own (or with other available data) can identify an individual (more)
3. **What is 'Sensitive' Personal Data?**: Some categories of personal data are considered particularly sensitive and require additional protections (more)
4. **Data Protection Principles:** The 7 rules that the School must follow in order to comply with the law (more)
5. **Enforcing the Law:** The UK regulator is the ICO. The public can complain about the School to this body. The ICO can investigate and has a range of powers including the ability to fine (more)
6. **Information Governance Framework:** The School must identify key roles and responsibilities to make sure we comply with the law (more)
7. **Data Protection Officer role:** A statutory role the School must have access to which helps us to maintain our compliance (more)
8. **Personal responsibilities**: All staff who have access to personal data have a role to play in maintaining the School's compliance (more)
9. **Privacy Notices**: Parents/ Guardians need to have easy access to details of what we do with their personal data (more)
10. **Rights**: We must provide for parents/ guardians exercising their improved rights (more)
11. **Requests for information**: We must have procedures in place for dealing with requests for personal data so that we can fulfil them within legal deadlines (more)
12. **Information Sharing**: We must only share data with other bodies where the laws allows us to, or with an individual's consent (more)
13. **Privacy by Design & Default**: We must understand the risks of how we manage personal data, undertaking statutory risk assessments where necessary (more)
14. **Breach Management**: Where we have incidents of data being lost, stolen, given to the wrong person or deleted when it shouldn't have been, staff must report it to the School and it must be investigated. Decisions need to be made about reporting to the ICO within 72 hours. (more)
15. **Further Information**: Link to the ICO website (more)

Data Protection

The Data Protection Acts 1998 & 2018 control how personal information is used by the School. Everyone responsible for handling and using this data has to follow strict rules called 'data protection principles'. The law only applies to information that *identifies a living individual*.

GDPR is EU law that will be part of the Data Protection Act 2018. The UK Act won't change GDPR; only make decisions that the EU has allowed individual countries to make (Return to top)

What is Personal Data?

GDPR applies to 'personal data'; meaning any information relating to an identifiable living person who can be directly or indirectly identified by it.

This definition provides for a wide range of personal identifiers to constitute personal data, including:

name, identification number, location data or an online identifier.

This reflects changes in technology and the ways in which organisations collect and hold information about people. (Return to top)

What are the special categories of data?

The law says there are certain types of personal data that have a higher sensitivity, and where an organisation holds this data, there is a higher risk to a person's rights as a result. Therefore, this data must have a higher level of security. This is data about an individual's:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs, or
- Trade union membership, and the processing of
- Genetic data,
- Biometric data,
- Mental or physical health
- Sex life or sexual orientation.

(Return to top)

Principles

The School is required by law to ensure that personal data is used fairly and lawfully, and GDPR holds a set of principles which describe how such data should be handled:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary
- Ensures appropriate security
- Demonstrate compliance with the principles

(Return to top)

Enforcing the Law

Data Protection legislation is regulated in the UK by the Information Commissioner's Office (ICO). The ICO are the UK's independent authority set up to uphold information rights in the public interest; promoting openness by public bodies and data privacy for individuals

The ICO provides Codes of Practice, advice and guidance to organisations to enable their compliance with legislation and they have the power to take enforcement action when things go wrong. These powers include:

- *Information Notices* – requiring that organisations tell the ICO about their practices
- *Decision Notices* – published written judgements on the outcome of an investigation
- *Enforcement Notices* – legal orders requiring organisations to make specific improvements
- *Monitoring* – Making sure an organisation improves over time
- *Consensual or compulsory audits* – Investigations into practices through onsite audits
- *Monetary Penalties* – Fines of up to €20,000,000

(Return to top)

Framework

In order to manage personal information lawfully and fairly it is essential that the School identifies roles and responsibilities to support this

All staff have responsibilities to ensure they know who to go to for advice on Data Protection issues

Compliance with legislation must be documented and evidenced on a continual basis in order to comply with Data Protection Principle 7. (Return to top)

Data Protection Officer

The new Data Protection Act 2018 requires the School to appoint a Data Protection Officer (DPO). This is a statutory post, and key tasks include:

- Ensure awareness and training is in place for employees and regularly completed/reviewed
- First point of contact for Data Subjects in relation to queries on how their data is handled
- First point of contact with the ICO for regulatory matters
- Approves Information Sharing Agreements
- Approves Privacy Impact Assessments
- Ensures adequate reporting to senior leaders on compliance with information management

The role of DPO can be carried out in conjunction with another role, provided there is no conflict of interest; shared with other organisations, or contracted-out. (Return to top)

Responsibilities

- All employees hold a personal responsibility for ensuring that personal information is used fairly and lawfully
- The School's information policies are there to help staff understand what they can and can't do when using personal data. It is critical that these policies are clearly communicated and readily available. All staff have a responsibility to abide by the information policies developed by the school.
- Any high volume and frequent sharing of personal information outside of the School must be documented and approved by the Data Protection Officer.
- Employees also have a key role in ensuring the security of personal data. If an employee becomes aware of a security incident (or a near miss), they must report all such incidents immediately to the designated staff member so that they can be investigated and managed. The purpose of reporting incidents is not to apportion blame, but to identify areas of risk and target training in order to improve.
- All staff must ensure that they understand who to go to for advice and guidance for Data Protection issues. (Return to top)

Privacy Notices & Consent

The law requires the School to process personal information fairly and lawfully and in a transparent manner

Fairly – if an individual does not have a clear understanding of how we are using their information, or how to exercise their rights, then it cannot be considered 'fair'. The School must make available at the point of collection a privacy notice explaining to individuals:

- Why their data is used
- How it is secured
- How long it is kept
- Who we will share it with
- How to exercise their rights
- How to contact the Data Protection Officer
- The legal basis for the processing of their information

Lawfully – there must be a clear and documented legal basis for an organisation to process personal information about an individual. There are a number of legal permissions we can use, including:

- Consent (e.g. Parent/ Guardian permission)
- Required by law (e.g. The Education Acts)
- Entering into a contract (e.g. Your contract of employment)
- Vital interests (in order to protect health in emergencies)
- Public tasks in the public interest (e.g. holding CCTV or visitor data for security)

(Return to top)

The Rights

GDPR provides a number of rights in relation to how personal information is used to ensure that processing is fair. These rights include:

- Right to be informed
- Right of Access
- Right to Rectification
- Right to Erasure
- Right to Restriction
- Data Portability
- Right to Object
- Rights related to Automated Decision Making & Profiling

Any staff member receiving a request to exercise these rights, which may be in writing or verbally, should immediately make the Data Protection Lead aware of the request to ensure it is handled within the legal timescales (a calendar month).
(Return to top)

Requests

GDPR provides a right of Access to information, known as Subject Access Requests. Individuals can request access to personal data about them held by the School; including parents/ guardians accessing data about their children. We must therefore ensure we only provide personal data to individuals who have a legal right to it. This involves checks of ID, and potentially removing certain information from the records disclosed.

(Return to top)

Sharing

Any sharing of personal data outside the School should be documented. Remember, unless the law requires us to share, we cannot do so without the individual's consent. In circumstances where the law does require us to share (and we therefore do not need to seek consent), we must still ensure that our privacy notice advises individuals of the circumstances where we may share their data.

Any sharing of sensitive data must be documented in a relevant system, detailing:

- The date of sharing
- The information shared
- Who you shared the information with
- Your rationale for deciding to share the information

If the sharing is intended to be regular it must be supported either by a contract or an information sharing protocol to ensure the correct security arrangements are in place.

(Return to top)

Privacy by Design

A key mechanism for assessing risk is the Data Protection Impact Assessment (DPIA). The DPIA will document what you want to do, the data you wish to use, the legal basis, how the data will be secured and managed and how individuals can exercise their rights in relation to the processing. If there is a risk to people's rights from our activities, the law says we must conduct a DPIA, and our DPO must approve it (Return to top)

Breach Management

Under GDPR there is a legal requirement to notify the ICO of any serious breaches involving personal data within **72 hours**

It is therefore important that you understand your responsibilities including how to identify a breach, who to report incidents to, and ensuring all staff are trained on how to use technology securely and effectively in line with their role

When a serious breach occurs we will be required to consider notification to the affected individuals. If we take the decision not to inform them, the ICO may overrule that decision if they feel it is in the best interests of the individuals

Failure to notify a serious breach to the ICO could result in up to a €10,000,000 fine – in addition to any other fine imposed for the breach itself. (Return to top)

Further Information

There are a number of resources available for more information about GDPR.

A recommended 'plain English' resource is the ICO website.

(Return to top)