

Explaining GDPR



What is GDPR?

The General Data Protection Regulation (GDPR) is a new EU law that will come into effect on 25 May 2018 to replace the current Data Protection Act (1998). It is the biggest overhaul of data protection legislation for over 25 years, and will introduce new requirements for how organisations process personal data.

It is focused on looking after the privacy and rights of the individual and based on the premise that consumers and data subjects should have knowledge of the lawful basis for processing their data, what data is being held about them, how it is held, how it will be used, why it will be used, how long it will be held for and whether or not this information will be exported elsewhere for use by another organisation.

What information does this relate to?

The data relates to any personal information that you could use to identify an individual directly or indirectly.

Identify who?

This includes any living person including pupils, parents, staff, governors, contractors, university students etc.

What are we doing?

As a school we will ensure that data we hold is accurate and kept up to date.

We will ensure that we only keep data for as long as is required. The length of time we keep documents can be found within our **Data Retention Policy**. We will ensure we inform the data subject of the length of time the information will be kept.

We will inform data subjects why we will use the data.

We will inform data subjects how we will use the data.

We will inform data subjects if their data will be used by a third party.

We will inform data subject what we will do with their data once we no longer require it.

We will identify the lawful basis for processing data (unless an exemption or derogation applies). This is within our **Privacy Policy**.

The lawful basis could fall into one of the following categories:

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

What can go wrong?

As an organisation we are responsible for the data we hold. Much of this data is sensitive so we need to ensure that we take care of this data.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

How can we reduce the risk of anything going wrong?

Ensure that we keep data safe on the schools site. This includes locking data away, locking computers, using passwords on documents etc.

Ensure data is being transported in a secure way when it is being removed off site.

Ensure that the intent with which any data is accessed and used is lawful, fair and transparent, and that it is for specified explicit and legitimate purposes.

Ensure that we protect the right of individuals. These include:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

We need to protect data to ensure it is only seen by people with the correct permission and keeping data that needs to be kept as per schools Retention Policy.

What if I think there may have been a personal data breach?

As a school we have a **Data Protection Breach Notification Form (DPNF)**. You should complete the DPNF with the school's Data Controllers.

They will then inform the Data Protection Officer (DPO). The DPO is responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements.

The DPO will inform the Information Commissioner's Office (ICO).

Contact Information - ICO Telephone Number: 0303 123 1113