



The General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a piece of EU-wide legislation which will determine how people's personal data is processed and kept safe, and the legal rights individuals have in relation to their own data.

'Personal data' means information that can identify a living individual.

The regulation will apply to all schools from **25 May 2018**, and will apply even after the UK leaves the EU.

Main principles

The GDPR sets out the following **key principles** for processing personal data.

- **Data must be:** processed lawfully, fairly and transparently; collected for specific, explicit and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected

There are also **stronger rights for individuals** regarding their own data.

- **The individual's rights include:** to be informed about how their data is used, to have access to their data, to rectify incorrect information, to have their data erased, to restrict how their data is used, to move their data from one organisation to another, and to object to their data being used at all

New requirements

The GDPR is similar to the Data Protection Act (DPA) 1998 (which schools already comply with), but strengthens many of the DPA's principles. The main changes are:

- Schools must appoint a data protection officer, who will advise on compliance with the GDPR and other relevant data protection law
- Privacy notices must be in clear and plain language and include some extra information – the school's 'legal basis' for processing, the individual's rights in relation to their own data
- Schools will only have a month to comply with subject access requests, and in most cases can't charge
- Where the school needs an individual's consent to process data, this consent must be freely given, specific, informed and unambiguous
- There are new, special protections for children's data
- The Information Commissioner's Office must be notified within 72 hours of a data breach
- Organisations will have to demonstrate how they comply with the new law

- Schools will need to carry out a data protection impact assessment when considering using data in new ways, or implementing new technology to monitor pupils
- There will be higher fines for data breaches – up to 20 million euros

What we are doing

We are committed to ensuring we are fully compliant with the legislation and that we do the right thing for our students, staff, governors, trustees and the third parties with whom we work.

We know that complete GDPR compliance can only be achieved through a collaborative and transparent approach.

We have been working on the following:

- Identification of a Data protection officer. Miss Michelle Jefferies will fulfil this role alongside her existing position, with support from Harvey Monk and Richard Pycroft.
- Undertaking an audit of all data we hold and compiling a data register
- Reviewing data protection policies, retention policies, privacy notices and processes
- Seeking further assurance about the use of our data from third parties with whom we share data

Like many schools and companies, we have been waiting for guidance to be issued by the ICO and EU's Article 29 Working Party. We recognise we can't wait until all guidance has been released to implement our GDPR program, so have been pragmatically progressing with our plan. We continue to review guidance as it becomes available and will adjust our implementation if appropriate.

GDPR Roll Out

In the next few weeks, we will start to roll out new GDPR privacy notices.

We will publish a new GDPR/Data Protection Policy

We will roll out new consent notices

We will review all contracts (including employment contracts) to ensure they are compliant with the new legislation

We will ensure that data processing complies with GDPR

We will keep you informed of the new requirements and we welcome your views and suggestions for improvements in our data management handling. If you have any queries regarding GDPR or any suggestions for improvement please contact either Michelle Jefferies at JefferiesM@harpergreen.net or Harvey Monk at HMonk@rbhs.co.uk,