GDPR – A commitment to Compliance (May 2018)

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 **key principles** that all personal data must be processed in line with.

- **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
- Higher fines for data breaches – up to 20 million euros

Our commitment to demonstrate our compliance to GDPR – we are:

- Documenting our processing activity, including ensuring we have a lawful basis for processing
- Auditing this processing and identifying and creating an action plan to mitigate any risks to personal data
- Documenting the compliance of third-party providers and reviewing contracts to ensure compliance
- Ensuring that we have processes and procedures in place to ensure the rights of data subjects
- Reviewing the technical and organisational measures in place to protect data
- Training all staff on GDPR and our data handling procedures including governance staff

We have also appointed a Data Protection Officer for the Trust.

With the schools processing large amounts of data the Trust takes its responsibility as guardians of this data very seriously. The opportunities GDPR provides to make improvements in how we handle data has been fully embraced by the schools and Trust.

GDPR is a long-term project and we are committed to developing a privacy programme that becomes a cornerstone of our approach to data in the school. Whilst there will be changes, we are committed to ensuring that there is no negative impact on teaching and learning and the welfare of students and staff.