Briefing note on the

General Data Protection Regulation (GDPR)

It is very important to be data protection complaint, and with the new General Data Protection Regulation (GDPR) coming into force in May 2018, schools should consider its impact in advance.

What is GDPR?

The GDPR is a comprehensive regulation produced by the European Commission, and covers all aspects of data protection. Despite Brexit, the Government has confirmed that the GDPR will apply from 25 May 2018, replacing the Data Protection Act 1998 (the DPA).

What impact will the GDPR have on schools?

The risks of non-compliance are significantly greater under the GDPR than under the DPA. For example, maximum fines will increase from £500,000 under the DPA to the higher of €20 million and 4% of turnover for certain breaches under the GDPR.

Despite still some uncertainty as to how the GDPR will apply in practice, there are clear changes in the law that schools should be aware of. Taking on board these changes and ensuring GDPR compliance in advance can only be a good thing.

- Insurance – the GDPR is far more favourable than the DPA for individuals bringing claims that their data rights have been infringed, so schools should **check that they are insured for data protection related claims**.
- Data Protection Officer – it is likely that schools will be required under the GDPR to have a Data Protection Officer. Even if a school isn't legally required to have one **it is advisable to have a Data Protection Officer** as it is harder to demonstrate compliance if there is not one individual with overall responsibility.
- Record keeping – the GDPR imposes **extensive requirements around record keeping and being able to show a paper trail of compliance**. These records must contain, for example, information about the purposes of processing and a description of the categories of data subject and categories of personal data.
- Policies and procedures – the GDPR makes explicit reference to having **data protection policies** (although in practice this is already a requirement under the DPA). Schools should therefore ensure that they have policies in place which provide practical guidance to staff, particularly around information security.
- Information security – under the current law schools are required to take **appropriate technical and organisational measures to keep personal data safe**. The GDPR expands on these obligations, for example by referencing specific measures such as encryption, pseudonymisation and privacy by design.
- Reporting – the GDPR creates a **new obligation to report data breaches to the Information Commissioner's Office** (the ICO) where the breach represents a 'high risk'.
- Data processor – a data processor is anyone who handles personal data on behalf of a school (e.g. cloud storage provider). **Schools will need to check that their data processors are GDPR complaint**. The DPA already requires that there is a written contract in place between the two parties, but the GDPR mandates additional requirements around the wording which must be included in the contract.

- Privacy impact assessments (PIAs) – if a school plans to handle personal data in a way that represents a 'high risk' to individuals then the GDPR will require the school to carry out what is known as a **privacy impact assessment**. The requirement to carry out a PIA is subject to further implementation but is likely that activities such as introducing a new IT system, monitoring staff and pupil emails or browsing habits will trigger an obligation to carry out a PIA.
- Marketing communications – the GDPR will introduce a more restrictive definition of consent for fundraising communications. One of the consequences of this is that so called 'implied consent' is unlikely to be data protection compliant (if it ever was**). Schools should check any forms used to capture marketing and fundraising consent to ensure that they are GDPR complaint.**
- Privacy notices – individuals have a right to be given certain information about how a school handles their data, which is usually provided in a document known as a privacy notice. The **GDPR will require additional information to be included in privacy notices**. For example, individuals must be told about their right to complain to the ICO. The GDPR also requires privacy notices to be transparent and written in clear and plain language, especially if addresses to children.
- Subject access requests (SARs) – the GDPR preserves an individual's right to request a copy of the data held about them (a SAR) with some changes. In most cases, a school will have just one month to respond to a SAR, rather than the 40 day time period under the DPA. **Schools should therefore consider what measures it needs to put in place so as to ensure that SARs will be dealt with in accordance with the shorter statutory timeframe**.
- New rights such as the right to be forgotten – various new rights will be introduced by the GDPR. The right to be forgotten, for example, requires the school to delete personal data in certain circumstances. **Schools should ensure that there are processes in place to allow these rights to be exercised**.

What should governors do next?

- **Book and attend relevant training sessions.**
- **Appoint a Data Protection LINK Governor.**
- **Start audit of all relevant policies and documents and create an action plan.**

In addition, Governors should be aware of the support available which they can buy into to support their understanding of their current level of compliance:

- **Awareness briefings**
- **Training**
- **On site audits including an action plan**
- **Consultancy**
- **Helpdesk for DPA/GDPR**
- **Helpdesk for statutory requests for information, i.e. FOI, EIR and SAR**
- **E-Learning package to meet the annual refresher requirement once compliance is achieved, with minimum impact for schools**

Sources of information:

Preparing for the General Data Protection Regulation (12 steps to take now)

Overview of the General Data Protection Regulation (GDPR)