General Data Protection Regulation:

Preparation Guide for Schools

What is it?

The GDPR (or otherwise known as the EU General Data Protection Regulation 2016) is new legislation designed to protect and empower European citizens with regard to their data privacy. It enhances people's rights and places greater obligations on organisations.

Who does it apply to?

Schools and other organisations that handle personal data.

When do you need to comply by?

The legislation takes effect on the **25 May 2018,** so schools will need to be ready for this date. It will still apply to the UK when it leaves Europe, so don't delay!

Main areas affecting schools and what you need to do to prepare?

1. Consent *(Articles 7 and 8 of the GDPR)*

There are tighter rules around obtaining consent from adults and children. Most of what schools do, do not require consent, unless for example they photograph a school event and publish the images; take pupils on school trips; collect and use biometric information or send out direct marketing or fundraising information.

Under the new rules, schools will need to demonstrate that consent has been obtained freely, the individual is fully informed and they have *opted-in* to the specific activity. You cannot use pre-ticked consent boxes or assume consent has been given, just because they have not told you otherwise (ie consent cannot be inferred from silence).

Schools will be required to keep clear records of all consent they obtain, and they must inform individuals of their right to withdraw consent at the time and offer easy ways to do this.

When obtaining consent directly from children, schools will be required to adapt the wording according to the children's level of understanding. If schools offer on-line services to children, they will need parental consent for anyone under 16 years (this is likely to be lowered to 13 years when the UK Data Protection Bill is passed in 2019).

Firebird
Data Protection Consultancy Ltd

2. Citizens' Rights

People have new and enhanced rights. Here's a short overview about some of them.

- **Transparency and Information** (*Articles 12-14 of the GDPR)*

There are new requirements to publish more information in Privacy Notices - these include the contact details of your Data Protection Officer; the purpose and lawful basis for processing personal data; how long you keep the data for; who you share personal data with and so on.

- **Access to Personal Data** (*Article 15 of the GDPR)*

Otherwise known as a Subject Access Request- this enhanced right entitles pupils, parents/guardians and employees to receive a copy of the information the school holds on them for free and within one month. Under the current Data Protection Act you can charge £10.00 and you have 40 calendar days to respond, so schools should consider the resource implications of this new change.

- **Rectification and Erasure** *(Article 16 and 17 of the GDPR)*

Individuals are entitled to have inaccurate personal data rectified or incomplete information completed and have their personal data deleted in cases where the data is no longer needed or if the individual withdraws consent. This right does not require a school to delete data upon request, if the school is complying with a legal obligation in holding it, for example if the school is required under statute to collect and retain the data for a certain length of time.

- **Object to Direct Marketing** *(Article 21 of the GDPR)*

Individuals have the right not to receive direct marketing, which means that schools will have to gain explicit 'opt-in' consent before sending out marketing material. This will be relevant where schools target individuals for fundraising; advertise their school prospectus or send out advertising literature for other organisations.

3. Obligations for Schools *(Articles 24-32 of the GDPR)*

There are several new obligations for schools to fulfil under the GDPR. These include:

- **Data Protection policies and training**

You will need effective data protection policies, procedures and employee training.

- **Written contracts with suppliers**

Schools will be required to assess the suitability of all suppliers and contractors who process personal data on their behalf and issue them with written contracts stipulating what they can and cannot do with the data.

- **Record of processing activities**

Schools need to identify and record what categories of personal data they are processing; why; how long it is kept for; who it is shared with and a brief description of the security measures they have in place to keep it safe. This document must be provided to the Information Commissioner's Office or the public upon request.

- **Technical and organisational measures**

Proportionate and adequate technical security measures, policies and procedures will need to be implemented to ensure data protection compliance is built into everyday practices.

- **Data Protection impact assessments**

Data protection impact assessments will need to be carried out prior to any processing of personal data, which could result in high risks to the rights and freedoms of data subjects.

4. Data Breaches *(Articles 33 & 34 in the GDPR)*

There are new requirements to investigate and notify the Information Commissioner's Office (ICO) and data subjects about data breaches. Schools will need to notify the Information Commissioner's Office (the ICO) within 72hrs if they suffer a breach which is likely to result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage to data subjects, and carry out a full internal investigation as to how it happened and put mitigations in place to prevent it happening again in the future.

Schools will also be required to inform data subjects if their personal data has been put at high risk as soon as possible.

5. Data Protection Officers *(Articles 37-39 in the GDPR)*

All public authorities (maintained schools and academies) must appoint a Data Protection Officer (DPO). Independent schools that process 'special categories' (ie sensitive) personal data on a large scale, may also be required to appoint a DPO.

DPOs can be an existing employee or schools can appoint an external person to fulfil this role. The individual is required under the new law to have *"expertise in national and European data protection laws and practices and an in-depth understanding of the GDPR"* (Article 29 Data Protection Working Party Guidelines). The DPO must have the freedom to carry out the role independently and cannot have a conflict of interest.

6. Compensation and Fines *(Articles 82-83 of the GDPR)*

Data subjects have the right to receive compensation if they suffer damage as a result of a data breach and organisations can be fined up to £8million for a breach. It is therefore important that schools review how they handle personal data in order to avoid potential fines and compensation claims.

Preparation summary

1. Review how you seek, manage and record consent, ensuring that consent is freely given, the person is informed, and they have positively opted-in to the proposed activity. They must also be informed of their right to withdraw consent.

2. Plan how you will manage and respond when individuals exercise their rights. Ensure there is appropriate knowledge, resources and systems in place to react quickly. Update your privacy notices with the new information required and inform people of their rights in your policies and consent forms.

3. Carry out an audit to assess your compliance against the GDPR, particularly around your policies and procedures; contracts; risk assessments and technical and organisational security measures and improve your practices as required. This will help to mitigate against possible fines and compensation claims.

4. Carry out a data mapping audit to identify the personal data you process; the reasons why; the retention period; who you share it with and a brief description of the security measures you have in place. Record this in a Record of Processing Activity Inventory.

5. Create procedures for identifying, reporting, managing and investigating breaches and communicate these to staff.

6. Decide who will be your Data Protection Officer – an employee or external consultant, ensuring they have the appropriate knowledge and capability to perform the role and do not have a conflict of interest.

Firebird can support you

We offer a range of services to support organisations in their journey towards GDPR compliance. This includes expert advice, audits, training and the provision of an ***experienced*** and ***qualified*** (*to Masters Degree level)* external **Data Protection Officer**.

Bespoke packages are available to suit all budgets, whether you are looking for lite-support or the complete support and reassurance of having an independent, external Data Protection Officer.

Contact us for more information:

Email: info@firebirdltd.co.uk

Website: www.firebirdltd.co.uk

Firebird
Data Protection Consultancy Ltd