General Data Protection Regulation (GDPR)

Schools' Action Plan

www.eani.org.uk/thinkdata

#eaThinkData

"GDPR is an evolution in data protection, not a total revolution. GDPR is building on foundations already in place for the last 20 years."

Steve Wood – Deputy Commissioner for Policy, ICO

Last Updated 11 June 2018

Background and Context

The General Data Protection Regulation (GDPR) impacts all organisations, including public authorities and schools. The new GDPR legislation replaces the existing 1998 Data Protection Act.

Under the current Data Protection Act, each school is a Data Controller. This has not changed. Each school will continue to be a Data Controller and, as such, is still responsible for ensuring that all practices relating to the handling of personal data in the school meet the requirements of GDPR. The Board of Governors is responsible for ensuring compliance with GDPR.

The EA Think Data website (www.eani.org.uk/thinkdata) is a useful online resource containing templates and guidance documents designed to help schools prepare for GDPR. Here you will also find our GDPR introductory video produced in partnership with the Information Commissioner's Office (ICO). This provides a very useful overview of GDPR for school principals, governors and staff.

This GDPR Guide for Schools provides a summary of the key actions your school should take to prepare for GDPR.

If you need advice or guidance, you can contact EA as outlined below.

EA GDPR HELPDESK

Email: thinkdata@eani.org.uk

Telephone: 028 8241 1300

Website: www.eani.org.uk/thinkdata

Get Ready for GDPR

1: Awareness

You must tell staff and volunteers in your school about GDPR. They must understand what personal information is and how to handle it safely.

You must keep a record of GDPR awareness and training sessions delivered in your school.

EA has developed a presentation that Principals can use to raise awareness of GDPR among school staff and volunteers. The ICO has also published a pack of useful posters and leaflets that can be used in school.

Online GDPR training is also available. There are two training places available per school - one for the Principal and one for another school representative. Register for online training at www.eani.org.uk/about-us/think-data/registration/

2: Register with the ICO

You must register your school with the ICO. The average cost of registration is £40 per school. It only takes five minutes to complete the online registration form on the ICO website. Make sure you register before 25 May 2018 at www.ico.org.uk/for-organisations/register/

3. Information Asset Register (IAR)

Each school must create an Information Asset Register (IAR). This is a spreadsheet that sets out a clear record of personal information held by the school, why it is held, how it is stored, for how long it is kept, how it is used and who it is shared with.

An IAR template and guidance notes are available to download at www.eani.org.uk/about-us/think-data/templates-and-guides/

The IAR template has already been populated with information that is collected via C2k. You simply need to review and update the template for your school and add any information your school collects through other means.

In completing your IAR, you will find it useful to refer to the Department of Education's Retention & Disposal Schedule for schools which is availbale at https://www.education-ni.gov.uk/publications/disposal-records-schedule. This Schedule tells you how long you must retain information for and when you must dispose of it.

4: Privacy Notice

A Privacy Notice is a statement that tells people why you are collecting their personal information and how it will be used.

You must have a Privacy Notice written and published by 25 May. EA has prepared sample Privacy Notices for schools which schools can adopt:

- Privacy Notice for Parents/Pupils/Families/Legal Guardian
- Privacy Notice for School Teaching Staff
- Privacy Notice for School Non Teaching Staff

These sample Privacy Notices will are available at www.eani.org.uk/about-us/think-data/templates-and-guides/

You must read these documents carefully and customise them to suit your school.

You can publish your Privacy Notices in different ways, for example: on your school website, notice boards or in newsletters. We recommend publishing the Privacy Notice on the school website.

You must tell people how to access your Privacy Notice. It is important that you review all of the forms used to collect personal data and include how to access your Privacy Notice. For example, this will apply to parental permission forms.

5: Data Protection Policy

Your school must have a Data Protection Policy.

EA has developed a sample Data Protection Policy which can be adopted by schools. This is available at www.eani.org.uk/about-us/think-data/templates-and-guides/

You must read this document carefully and customise it to suit your school.

6. Individuals' Rights

Under GDPR, people have certain rights relating to personal information. The ICO lists these Rights and further information at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

Your school must have documented procedures to ensure you can deal with requests in relation to these rights e.g providing access to or deleting personal information. EA is developing sample procedures in relation to rights. These will be available on the EA Think Data website shortly.

7: Subject Access Requests (SAR)

A Subject Access Request (SAR) is a request from someone to get a copy of personal information held about them. Usually you would have 40 days to respond. Under GDPR this is one month. EA is working on the basis of 28 days.

Your SAR procedure must enable you to respond within this new shorter timeframe.

EA has developed a sample SAR procedure for schools. This includes guidance, and template forms and letters that can be used to hely you manage requests for information and communicate with individuals requesting information.

This procedure has been emailed to schools for use as an internal school document.

8: Consent

You must review how you seek, record and manage consent for handling and processing personal information. You will need to read the ICO's detailed guidance on consent at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/.

EA has developed guidance for schools including template pro-formas for seeking consent. These are now available on the EA Think Data website at www.eani.org.uk/thinkdata

9: Children's Data

GDPR will bring in new special protection for children's personal data.

The ICO has published a number of guidance notes on children's data and its handling.
This is available at: https://ico.org.uk/for-organisations/guide-to-the-general-dataprotection-regulation-gdpr/applications/children/

10: Data Breaches

You must have a procedure in place to detect, assess and, where necessary, report data breaches. For example, what do you do if a laptop or phone is lost or stolen? Under GDPR, any data breach that is significant enough to be reported must be reported to the ICO within 72 hours.

EA has developed a sample Data Breach Management Procedure which incudes useful templates that can be used by schools when managing data breaches.

This procedure has been emailed to schools for use as an internal school document.

11: Data Protection by Design and Privacy Impact Assessment (PIA)

After the 25 May, if you are developing a new process or purchasing a new product/service, you must carry out a Privacy Impact Assessment (PIA) at the very start of the process and before you make changes to howe you do things.

This means thinking about the implications might be for personal data before you make any change or decision. This is known as 'Privacy by Design.'

A sample PIA template and guidance notes will be available on the EA Think Data website shortly.

12: Data Protection Officer (DPO)

Your school is already a Data Controller. Your Board of Governors ensures your school is compliant with current data protection legislation. and the Principal is responsible for day-to-day operational matters relating to data management and protection.

Under GDPR, there is a new requirement for your school to have a named Data Protection Officer (DPO). This person must have specific experience and expert knowledge of data protection law and its practical application. **EA is prepared to act as DPO for your school.**

Schools have been provided with a detailed agreement setting out the terms of this arrangement. This agreement must be signed by the Chair of the Board of Governors and returned to EA.

Under this arrangement, the Principal is still the key point of contact for all of your school's data protection issues and has operational responsibility for day-to-day management of all data protection matters. The Board of Governors will still be responsible for ensuring compliance with all data protection legislation including GDPR.

If you are appointing EA as your DPO, you should include the following contact details on your GDPR documentation:

DPO: Education Authority
Email: dpo@eani.org.uk
Tel: 028 8241 1300