What Governors need to know about GDPR

What Governors need know and do

Clive Haines and Rebecca Walker

achieving for children

Aims of the training

- To ensure you have the appropriate information and knowledge about GDPR – **WHAT IS IT**
- To ensure that you have the tools to hold the school/academy to account for GDPR - **YOUR ROLE**
- Introduce a check list to support the Governors' role in GDPR

General Data Protection Regulations

- The **General Data Protection Regulation (GDPR)** will apply from 25 May 2018 and will affect the way that schools process personal data. Its overall aim is to make sure that people's sensitive data is kept safe and secure.

- **It's similar to the Data Protection Act (DPA) 1998 in many ways – most of the differences are where the GDPR builds on or strengthens the principles of the DPA.**

Who does GDPR apply to:

Everyone:

- Staff
- Parents
- Partners
- Public

All personal data held by the school and its partners will be covered by GDPR

What are the principles

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 purposes.

  We must limit to what is necessary for the purposes for which it's being used (accurate)

  Data needs to be held securely and only retained for as long as is necessary for the reasons it was collected

What are the principles

Main principles

- 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 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

New Requirements

- 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
- 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

First Step for Schools

Information Audit – What should schools be looking at as part of this audit?

- What information is held?
- Where does it come from – data subject or third party?
- What is done with it?
- Who is it shared with?
- How long does it have to be kept for?
- How/where is it stored?
- Identify where Information Sharing Agreements are in place and where they need to be put in place
- **Identify where Privacy Notices are required**

What is a Privacy Notice?

- Identities and provides contact details of the data controller and the data protection officer – **Who to contact**
- Purpose of the processing and the legal basis for the processing of data – **Why are we collecting the data?**
- Data subjects' rights
- Retention/disposal requirements – **How long we keep the data**
- Right to complain to ICO – **What to do if concerned**
- Details of overseas transfers – **How the data will be shared**

What is a Privacy Impact Assessment?

Mandatory requirement:

Do at the start of a project whether new or change to existing systems

- Map information flows – **the journey of data**
- Identify privacy risks – **who will see the data**
- Identify who needs to be consulted
- Identify corporate compliance risks – **Policy**
- Identify owners of privacy risks/solutions
- Integrate the PIA outcomes back into the project – **review and reflect**

GDPR and Sharing of Information

- Sharing must only happen when there is a legitimate & lawful purpose.
- Formal sharing agreements must form part of contract documentation when sharing is a routine operation.
- One-off sharing **must not happen** until a disclosure template is completed and signed by relevant designated officers.

Templates are available from the Data Team
dpa@rbwm.gov.uk

GDPR – Website Compliancy

Schools must:

- Replace any Data Protection Act 1998 references.
- Correct out-of-date contact information.
- Publish Privacy Notices.
- Check links work!

Does your school need to review their website prior to 25th May?

Data Protection Breach reporting

Mandatory requirement to report to the ICO within 72 hours

Threshold – significant detrimental effect on individuals e.g. results in:

- Discrimination
- Reputational damage
- Financial loss
- Breach of confidence

Reporting of a breach to the ICO is a judgement call for the Data Protection Officer

Please ensure your school's data policy is updated to reflect

Data Protection Breach reporting

Schools need to appoint a data protection officer (DPO) by May 2018, who must:

- Have an understanding of data protection law
- Report directly to the highest management level of the school
- Be a senior member of staff
- Not have any conflicts of interest between their existing role and the DPO role (so, for example, the head of IT should not be the DPO as they are responsible for implementing the IT system)

Has your school appointed a DPO?

GDPR – Governors' Role

Knowing what you know now regarding GDPR, what is the governing board's responsibility, and the strategic role governors will play regarding GDPR?

GDPR – Governors' Role – Appoint DPO

It's important you get this right

- Governors should not be involved in the operational side of recruiting or appointing the DPO, but should provide the necessary challenge and scrutiny of the appointment.
- The headteacher should come to the governing board with a proposal for how the school will appoint its DPO.
- Your role is to discuss, approve or challenge the plans.

Note: there is currently no consensus on how schools will most likely appoint their DPO. For this reason, bear in mind that your SLT may not appoint a DPO until closer to the May deadline. (Or SLA to the role of DPO)

GDPR – Governors' Role – Appoint DPO

If the headteacher proposes using a data protection consultancy rather than appointing a staff member in-house, you could ask questions like:

- Why do you think this is the best option?
- Does this represent value for money?
- Do we not have the expertise in-house, or the capacity to up-skill someone?

GDPR – Governors' Role – Appoint DPO

If the headteacher proposes giving the role to an existing staff member, you might ask questions like:

Why this staff member?

- Why are you sure they're the best person for the job?
- How are you going to make sure they can balance all of their responsibilities?
- Is the necessary training in place for them?
- Does their contract allow them to remain available and accessible all year round, to respond to subject access requests and deal with any issues?

Designate a data protection CHAMPION

Although data protection is a collective responsibility, you could designate someone on the board as a data protection champion. Whether you choose to do this will depend on the size of your board and governors' existing responsibilities.

Can this person:

- Keep up to date with data protection changes
- Meet with the DPO or other relevant members of staff before relevant governing board meetings, to monitor compliance and request any specific information
- Add data protection to meeting agendas when necessary, to make sure it is recognised as an important issue

OR could this be included in Health and Safety

Plan how you will monitor GDPR compliance

Possible actions to monitor GDPR compliance from May onwards:

- Add a standing agenda item to full governing board meetings to scrutinise the risk register, which will include the data protection section
- Designate a data protection champion who can liaise with the relevant school leaders before each meeting
- Make sure you're receiving reports from the DPO (**a requirement under the GDPR**)
- Request a 6-monthly update from the DPO on how the GDPR is working in practice more widely – it's new legislation, so keep tabs on the sector to see if more information is released or there are lessons to be learnt from other schools

Plan how you will monitor GDPR compliance

- Ask the relevant committee/champion to present to the full governing board on the effectiveness of your data protection procedures and IT controls
- **Incorporate questions about data protection into your school visits:**
  - Ask staff what training they receive on data protection, if they know what counts as a data breach, what procedures they should follow to keep personal information safe, and if they understand how data protection fits in with **safeguarding**
  - Ask pupils how they learn about keeping information safe and how they learn about the internet

Final Note:

The Data Protection Bill

- The GDPR is just one part of the data protection framework – the UK government is currently debating the Data Protection Bill in Parliament. The bill should become law in 2018, replacing the Data Protection Act 1998.

- It will set out the UK's policy on aspects of the GDPR which are left up to member states to decide, and cover areas of data processing not covered by the GDPR.

- **More updates due**

Toolkit:

GDPR – Privacy Notice Guidance

This checklist is designed to help school leaders produce a privacy notice, which is a statutory requirement. It also suggests what you could include in a broader data protection policy. It is based on guidance from the Information Commissioner's Office (ICO).

What to include	Tips	
Privacy notice (statutory requirement)		
Policy introduction	You should explain that the school is a data controller and, as such, is registered with the ICO and complies with the principles of the Data Protection Act 1998.	
Fair processing	You should set out the types of information you hold about pupils, staff and other groups, what you do with it and why you need it. You should also set out the other organisations you share information with. You may wish to make it clear that access to the information is only available to those who need it.	
Storage and disposal of information	You should explain how confidential information will be kept secure while it is being stored or used by the school, and when it is being shared with others. You should also explain how the school will ensure that personal data is	