THE PRIMARY FIRST TRUST

Summary: The General Data Protection Regulation (GDPR)

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

THE PRIMARY FIRST TRUST

In Depth: The General Data Protection Regulation (GDPR)

45 minute video link: https://www.youtube.com/watch?v=UPIhtpkYpxs

The General Data Protection Regulation (GDPR) will apply from 25 May 2018 and will affect the way that schools process people's 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 involve the GDPR building on or strengthening the principles of the DPA. If you're compliant with the DPA now, you'll be compliant with much of the GDPR already.

> If you're compliant with the DPA now, you'll be compliant with much of the GDPR already

1. Tell key people the law is changing

Raise awareness of the GDPR by:

- Sharing a summary - which summarises the key points of the GDPR in just one page - with the relevant people
- Adding data protection to your risk register, if you have one, so it's formally recorded as a potential compliance issue

In schools

Your key people are those who have responsibility for managing or dealing with personal data.

Depending on how your school is organised, this will probably be senior leaders, IT technicians, data managers and potentially administrative staff. It will also include governors/trustees, who are likely to have overall responsibility for your compliance with data protection law.

Once you've worked out what you need to do:

- Assign responsibility for managing specific changes to relevant individuals
- Consider whether updated data protection training is necessary for any of your staff

2. Plan to appoint your data protection officer

Schools need to appoint a data protection officer (DPO). This person 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, and the DPO will be responsible for checking the system's compliance with the GDPR)

In schools

You could:

- Hire a full-time or part-time DPO
- Give the responsibility to a senior staff member if there are no conflicts of interest
- Outsource your DPO responsibilities to a third-party organisation
- Share a DPO across a group of schools (such as a multi-academy trust, federation, or a group of schools joining together purely for this purpose)

Bear in mind that there's currently no consensus about how schools should appoint their DPO. For this reason, you may wish to wait until closer to the May deadline to appoint your DPO, as more information may be available.

3. Carry out an information audit

Work out what personal data you hold, where it came from, and who you share it with. This will help you meet the GDPR requirements to:

- Maintain records of your processing activities
- Demonstrate how you comply with the data protection principles

Start by documenting where the riskiest and most sensitive data is. This is information which could cause detriment to an individual if the data was lost or seen by someone who shouldn't see it (for example, cause them distress, embarrassment or to suffer some form of discrimination).

- **In schools**
- The riskiest data is usually:
- Confidential information on staff and pupil records
- Safeguarding information
- Information that is taken away from the school premises, such as information on laptops, personal electronic devices or paper records that are transported from one place to another

Your governing board's working practices will need to be considered too. Think about:

- What documents governors have access to and whether these contain any personal data
- How governors get access to these documents
- Whether information is sent to personal email addresses
- Whether governors take information off the school site

Personal data may be stored in a wide range of places, including: your IT systems, laptops, personal devices, paper records, USB sticks or other portable storage devices, email accounts, and staff members' homes.

4. Identify your lawful basis for processing data

Under the GDPR, there are 6 'lawful bases' (or reasons) that a school can use to justify why it needs to process data.

In schools

You will most likely use **public task** as your lawful basis for most of your processing. This means that you need to process personal data to carry out your official functions in the public interest.

You might also use **consent** for processing data where it's not necessary for you to fulfil your function. It's recommended that consent is only used where none of the other bases apply, as the standard for getting consent is very high and consent can be withdrawn at any time.

We look at consent in more detail later in this article.

Look at the personal data you hold and identify which lawful basis/bases applies to how you process the data.

Then, document this and update your privacy notices to explain your lawful basis/bases.

Review your privacy notices

Model privacy notices

The Department for Education (DfE) has created a model privacy notice for pupils that is GDPR-compliant:

Data protection: privacy notice model documents, GOV.UK – DfE (Adobe pdf file)https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices

Our current model document will keep you compliant with data protection law until May.

Review your current privacy notices and put a plan in place for making any necessary changes in time for the GDPR.

Your privacy notices at the moment will probably say who you are, why you process information and what you do with it. By May 2018 you must have added information such as:

- Your legal basis for processing
- Notice of the individual's right to make a complaint to the ICO (as the 'supervisory authority')
- Notice of other rights in relation to access and correcting inaccurate data

You also need to make sure all your privacy notices are in clear and plain language – especially those that refer to children's data, so that a child can easily understand them.

The ICO explains the requirements for privacy notices under the GDPR in more detail, and summarises the information you must provide in a table:

Privacy notices under the EU GDPR, ICOhttps://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/

5. Review your data processing procedures

Your data processing procedures will need to cover the new requirements.

Check they cover the new rights for individuals

With respect to their personal data, individuals will have the right to:

- Be informed about how their data is used, typically through privacy notices
- Have access to their data, such as through subject access requests
- Have inaccurate or incomplete information about them corrected
- Have their data deleted where there is no compelling reason for its continued use
- Block or restrict processing of their data
- Obtain and reuse their data for their own reasons across different services ('data portability')
- Object to the processing of their data for particular purposes
- Not be subject to an automated decision made through the use of data, which has a legal or significant effect on the person

Some of these rights are new, and some are existing rights that have been strengthened by the GDPR. You can read more information about what each right means and when it applies, here:

Overview of the GDPR: individuals' rights, ICOhttps://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/

The rules around subject access requests are changing

Review how you respond to subject access requests

The new rules say you:

- Can't charge for complying with a request (in most cases)
- Have a month to comply (or 3 months where the requests are complex or numerous, in which case you must explain to the individual why the extension is necessary within a month)
- Can refuse or charge for requests that are clearly unfounded or excessive, particularly if they are repetitive or ask for further copies of the same information
- Can refuse a request, but within a month must tell the individual why, and that they have the right to complain to the ICO
- Must verify the identity of the person making the request using "reasonable means"

"Reasonable means" normally means you should seek 2 forms of ID. Also, follow up written requests with a phone call to confirm the request was made and to confirm the details of where the results should be sent to.

Schools should decide what is reasonable though. For example, seeking ID would probably be unnecessary if a staff member or governor makes a request.

If you're unfamiliar with subject access requests, we have more information in section 6 of our article on handling personal data.

Review how you manage consent

Check that you seek, record and manage consent in accordance with the rules. Your consent systems need to:

- Meet the GDPR requirements on being specific, granular, clear, prominent, opt-in, documented and easily withdrawn
- Record consent and ensure you have an effective audit trail

In schools

An example of where you may need to seek consent is for the use of a child's picture on the school website.

Many schools currently send a letter that says "if you don't respond, we will assume we can use your child's image", but this will not be allowed under the GDPR. If you obtained consent this way, you will have to ask parents again but following the new rules.

You will also need to seek consent when sending marketing or promotional material, for example, to prospective parents or to a group of alumni for fundraising purposes.

The ICO has more detailed guidance on consent, here:

Draft GDPR consent guidance, ICO https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

Check your processes adequately protect children's data

Your processes need to:

- Include systems to verify individuals' ages and gather parental or guardian consent for any data processing activities
- Be communicated in clear and plain language – especially any processes that refer to children's data, so that a child can easily understand them

In schools

This means:

- Verifying ages should be easy for schools as you will have children's dates of birth recorded
- If you need to seek parental consent for any processing of their child's data, you could incorporate this as a form in the admissions process, and refresh it at regular intervals throughout the child's schooling
- Privacy notices and requests for consent need to be in child-friendly language and accessible to a child, as already explained

Set out how you will respond to a data breach

Put procedures in place to:

- Detect, report and investigate personal data breaches
- Assess and report any breaches to the ICO within 72 hours where the individual is likely to suffer some form of damage, e.g. through identity theft or a breach of confidentiality
- Communicate a breach to individuals concerned, where appropriate

In schools

A data breach you need to report might involve:

- A non-anonymised dataset being published on the school website including the GCSE results of children eligible for the pupil premium
- Safeguarding information being made available to a lot of unauthorised people
- The theft of a school laptop containing non-encrypted personal data about pupils

When reporting a breach, you must set out the:

- Nature of the breach, including:

  - Categories and approximate number of people whose data has been breached
  - Categories and approximate number of data records concerned
- Name and contact details of the data protection officer or other person who can provide more information
- Likely consequences of the personal data breach
- Measures you have taken or propose to take to address the breach, including measures to mitigate its effects

Review your data protection policy

To check your processes cover the new rules, you could look through your data protection policy and ask yourself questions for each new requirement under the GDPR. For example, you might ask:

- If an individual asked for their data to be found/deleted/rectified/moved, do our systems allow us to do this?
- Do we have the staff, the time and the understanding of our data systems to comply with subject access requests within a month?
- How much is complying with subject access requests likely to cost?

6. Review your contracts with suppliers

Check and update relevant contracts

Check the data protection clauses in all existing contracts that will still be live when the GDPR comes into force. They need to reflect the GDPR requirements.

You will have to include certain information in contracts with suppliers (such as insurers, payroll and school club providers) where the school passes data to them, and they receive and store it.

These contracts must set out:

- The subject matter, duration, nature and purpose of the data processing
- The type of personal data being processed
- The categories of the data subjects
- The obligations and the rights of the data controller (your school)
- That the data processer (the supplier) processes data only on the documented instructions of the school
- That the people who process the data are committed to confidentiality
- That the supplier takes measures to ensure secure processing

- That the supplier will not engage another processor without prior written authorisation of the school, and that if the supplier does engage another processor, it will also be bound by the same data protection conditions as are in the contract
- That the supplier helps the school comply with requirements regarding the data rights of individuals (e.g. to access, delete or rectify data), secure processing, reporting and communicating data breaches, and conducting impact assessments where relevant
- That the supplier deletes or returns the personal data to the school at the end of the provision of services
- That the supplier makes information available to the school to demonstrate its compliance with the obligations in this contract, and allows the school or a third party instructed by the school to conduct audits and inspections

Contracts with suppliers will need to include certain information

You can add this information as a schedule to the contract, rather than having to amend the whole document.

The GDPR, The Official Journal of the EU, see article 28, paragraph 3 (Adobe pdf file)http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Carry out due diligence on suppliers

Carry out some data protection due diligence on any existing suppliers which hold personal data.

Ask suppliers:

- What action they are taking to prepare for GDPR
- What technical and organisational security measures they have in place to protect data
- What policies and procedures they have in place
- How secure their systems are
- Whether they have any information management accreditation

You could send a letter or questionnaire including these questions to all your suppliers.

THE PRIMARY FIRST TRUST

Role of the DPO

Who to appoint:

To find your DPO, you could:

- Hire a full-time or part-time DPO
- Give the responsibility to a senior staff member
- Outsource your DPO responsibilities to a third-party organisation
- Share a DPO across a group of schools (such as a multi-academy trust, federation, or a group of schools joining together purely for this purpose)

Whoever you appoint, they must:

- Have an expert understanding of data protection law
- Report directly to the highest management level of the school, which would usually be the board of governors or trustees
- Be in a senior role, if they're a member of staff

Ensure the DPO has enough time and resources

When giving the responsibility to an existing staff member, ensure they have enough time to carry out their data protection tasks.

The European Commission guidelines (see page 14) say you should determine:

- A set percentage of time for the DPO function
- The time needed to carry out DPO tasks
- The level of priority for the DPO's different tasks and responsibilities

You should also ensure the DPO has sufficient resources and training, as explained in the final section of this article.

Appointing an existing senior staff member

If you give the responsibility to an existing staff member on a part-time basis, they must have:

- Professional duties which are compatible with the demands of the DPO role
- No conflicts of interest with the rest of their job

Regarding conflicts of interest, the European Commission's guidelines say:

The DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data.

Due to the specific organisational structure in each organisation, this has to be considered case by case.

Conflicting positions within the organisation may include senior management positions but also other roles lower down in the organisational structure.

So, for example, it is unlikely that the head of IT could be the DPO as they are responsible for implementing the IT system, and the DPO will be responsible for checking the system's compliance with the GDPR.

It's for you to decide what would count as a conflict of interest, based on your school's specific systems and structures.

Guidelines on DPOs, Data Protection Working Party, European Commission (Adobe pdf file)http://ec.europa.eu/newsroom/document.cfm?doc_id=44100

Hiring a DPO to work across a group of schools

As explained above, you can have a single DPO for multiple schools if this works for your school structure and size.

The DPO could be one person with the official title and oversight. Some school-level duties could be delegated to either the school business manager or the principal at each school.

Bear in mind that the DPO must remain easily accessible for each school and be able to act as a contact point on data protection issues.

Outsourcing to a third party

You can also outsource your DPO to a third-party organisation. This might be:

- An independent consultant
- A 'service contract' with a data protection consultancy, for example
- Someone from your local authority, if it offers this service

If you choose to have a service contract with, for example, a data protection consultancy, the European Commission recommends that there is:

- Clear allocation of tasks within your provider's team
- A single individual as a lead contact who is ‘in charge’ for each client
- A service contract setting out the above terms

Responsibilities of the DPO

DPOs will:

- Advise the school and its employees of their obligations under relevant data protection law, including the GDPR
- Monitor compliance with data protection law, by:
    - Collecting information to identify data processing activities

- Analysing and checking the compliance of data processing activities
- Informing, advising and issuing recommendations to the school

- Ensure the school's policies are followed within the school, by:
  - Assigning responsibilities to staff members
  - Raising awareness of data protection law, including the GDPR, across the school
  - Training staff
  - Conducting internal audits

DPOs will advise schools of their obligations under data protection law

- Advise on and assist the school with carrying out data protection impact assessments, if necessary
- Act as a contact point for the ICO (as the 'supervisory authority'), involving:
  - Helping the ICO to access documents and information
  - Seeking advice on data protection issues
- Act as a contact point for individuals whose data is processed (staff, pupils and parents, for example)
- Take a risk-based approach to data protection, involving:
  - Prioritising the higher-risk areas of data protection and focusing on these the most
  - Using their common sense to advise the school on whether it should conduct an audit, provide training in certain areas, and determine what the DPO should spend the most time doing

The DPO may also be assigned additional tasks – for example, maintaining a record of the school's processing operations.

The GDPR, see section 4 'Data protection officer', Official Journal of the European Union (Adobe pdf file)http://bit.ly/2DMRwZZ

The DPO is not ultimately responsible for GDPR compliance

The European Commission's guidance on the DPO role, linked to earlier in this article, explains on page 17:

Monitoring of compliance does not mean that it is the DPO who is personally responsible where there is an instance of non-compliance.

The GDPR makes it clear that it is the controller, not the DPO, who is required to 'implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this regulation' (Article 24(1)).

Necessary qualities and experience

The European Commission says the necessary skills and expertise for a DPO include:

- Expertise in data protection laws and practices, including the GDPR
- Understanding of the processing carried out by the school
- Understanding of information technologies and data security
- Knowledge of the school sector, and the school itself
- The ability to promote a data protection culture within the school

The level of expert knowledge a DPO needs is not strictly defined. It depends on the sensitivity, complexity and amount of data you process.

> The level of knowledge a DPO needs depends on the sensitivity, complexity and amount of data you process

The professional qualities needed are similarly undefined, as the European Commission says they should be determined:

... according to the data processing operations carried out and the protection required for the personal data being processed.

In a nutshell, the more complex or sensitive your data processing is, the more expertise and knowledge your DPO will need.

WP243 annex – FAQs, see page 4, European Commission (Adobe pdf file)http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_annex_en_40856.pdf

Your obligations regarding the DPO

Your school must ensure that your DPO:

- Operates independently and autonomously
- Is not dismissed or penalised for performing their task
- Is provided with necessary resources to meet their GDPR obligations and maintain their expert knowledge
- Is involved in all issues which relate to the protection of personal data

You must also publish the contact details of your DPO, and communicate them to the ICO.

'Necessary resources'

'Necessary resources' would be:

- Active support from governors/trustees
- Sufficient time to fulfil their duties

- A suitable budget, help from staff, and the use of premises, facilities and equipment
- That the purpose of the DPO is communicated to all staff in the school
- Access to, and support from services such as HR, legal, IT and security
- Continuous training
- A team of staff to support the DPO (depending on the size and structure of the school)

This is explained on page 14 of the European Commission guidance.

Training

To train somebody for the DPO role at this stage, you should make sure they're familiar with:

- The GDPR
- The Data Protection Bill that is currently being debated in Parliament, which will determine how some of the GDPR provisions will be implemented in the UK
- The Data Protection Act 1998
- The GDPR guidance from the ICO
- Any guidance from the Department for Education

Commercial providers are offering GDPR training for data protection officers.

GDPR practitioner certificate, Act Now Traininghttp://www.actnow.org.uk/dpp

Certified DPO (GDPR compliance), Firebrand Traininghttp://www.firebrandtraining.co.uk/courses/data-protection/certified-data-protection-officer-certification

Certified EU GDPR practitioner training course, IT Governancehttps://www.itgovernance.co.uk/shop/product/certified-eu-general-data-protection-regulation-practitioner-gdpr-training-course

Responsibilities and risks - a guide for data protection officers, MBL Seminarshttp://www.mblseminars.com/Outline/Responsibilities-_-Risks---A-Guide-for-Data-Protection-Officers/8833/

Practitioner certificate in data protection, PDP Traininghttp://www.pdptraining.com/practitioner-certificate-in-data-protection

Some organisations are also developing DPO courses especially for schools – for example:

GDPR certified practitioner course, 9inehttp://www.9ine.uk.com/gdpr-certified-practitioner-course