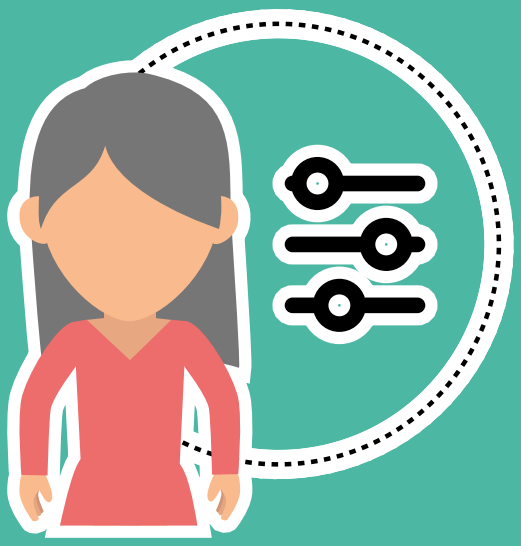
Data Protection Responsibilities of the Data Controller



PHP LAW LLP

www.phplaw.co.uk
info@phplaw.co.uk
0333 772 9763

Introduction

25 May 2018 saw the implementation of the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA). This was a reform of the previous Data Protection Act 1998. So much had changed that new legislation was required to provide more updated protections for individuals and a framework to manage technological developments.

School and Trusts are classed a public authorities and have additional obligations, principally to appoint a suitable Data Protection Officer. Everyone in the school community needs to understand their obligations, responsibilities and rights.

This is an overview of key issues and concepts for schools and academies. It looks at what needs to happen, and gives an overview of who is who in this very jargon heavy world.

Following the media furore about GDPR, everything suddenly died away. However, the legal obligations that GDPR and the DPA place on schools has not changed. The ICO hclear expectatiosn for accountability and compliance. Recenlty, there have been huge fines for some companies, for example British Airways. ICO officers are taking a more forensic approach to complaints. GDPR compliance is also forming part of internal audits.

GDPR is an essential and statutory part of school management. The Academies Handbook expects compliace with GDPR as part of good governance and data security. The DfE Governance handbook expects governors to assess and ensure compliance with the GDPR and DPA 2018.

Retaining compatibility with the EU is important for many UK businesses and organisations. Data centres that are in the EU, or EU suppliers need the certainty of the same rigorous standards.

A Data Protection Reform Bill is currently making its way through parliament. This will make some significant changes to obligations.

What is the point of the GDPR?

GDPR and the DPA exist to protect individuals' data. It is a series of safeguards for each of us. It is regulation designed to protect you, me and our families. In schools we handle data about children and adults every day. Some of that is very simple, a child's name on a book. Other information is far more sensitive, an EHCP for a child or an Occupational Health report for an adult for example.

Making sure that personal data is properly looked after is the whole point of the GDPR.

If it is shared without my permission or a legitimate purpose it could cause embarrassment, financial loss or have some other direct impact. If the data held is wrong or inaccurate it is important it is put right.

However, GDPR was never designed with schools in mind. The focus is on big business, international brands, banking and insurance sectors and government. The GDPR exists to protect individual rights in an increasingly digital world, and schools are caught up in this.

Who does it apply to?

Everyone, including schools. As Public Bodies schools have more obligations than some small businesses. It is mandatory to comply with the GDPR and proposed provisions in the Act.

Schools are good at data protection, it is simply part of day to day school life. However, GDPR requires some reviews to be in place, it is necessary to take stock of what data is held. Being clear about what is collected, why it is collected, how it is used, stored and disposed of is at the core of compliance.

Relations with those who process data on behalf of the controller should be GDPR compliant. New processes will need to be subject to a greater degree of scrutiny, a Data Privacy Impact Assessment. Doing this will assist in compliance with the key principles.

What are the 6 key principles of the **UK** GDPR?

1. **Lawfulness, transparency and fairness.**

   School's must have a legitimate reason to hold the data, and need to tell people what data school collects and how it is used.

2. **Collect data for a specific purpose and use it for that purpose**

   So, data cannot be used for a purpose that it was not originally collected for, or where notice has not been given about how data may be used after collection.

3. **Limited collection**

   Data controllers should only collect the minimum amount of data needed for a particular task or reason. If there is a breach or a hack only limited information can be lost.

4. **Accuracy**

   Data collected should be accurate, and steps should be taken to check and confirm accuracy.

5. **Retention**

   There must be a policy that requires data to be stored for limited periods of time about individuals. You should not store data for longer than you need it, or for historical archive reasons.

6. **Security**

   Ensuring that physical, cloud and other electronic storage of data is secure is vitally important. Everyone has a responsibility for the data they hold and process. This also includes third party contractors.

What is Data?

Any information that relates to a living person that identifies them. This can be by name, address or phone number for example. It also relates to details about that person, which can include opinions.

Some data is considered to be more sensitive, and therefore more important to protect. This is information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and sexual orientation, genetic data, and biometric data where processed to uniquely identify a person.

Schools often collect sensitive data for DfE and LA requirements and of course pupil data may contain information about safeguarding, SEN or health needs. Information about other family members may also be on the school file.

Who is a 'Data Subject'?

Data Subject

Someone whose details we keep on file. Some details are more sensitive than others. The GDPR sets out which collection of details such as health conditions and ethnicity are more sensitive than names and phone numbers.

Essentially, the whole of Data Protection exists to make sure that information held about us is treated with proper care and respect.

Data Subjects' Rights

Schools must inform people about how they hold data, and also that individuals have a right to access it. This can be limited in some instances where child protection is involved, or if there are legal or contractual exemptions. Schools need to tell people how they can do this and explain the complaints policy.

If data is inaccurate, no longer needed or old and serves no purpose the data subject has a right to have the data amended or deleted.

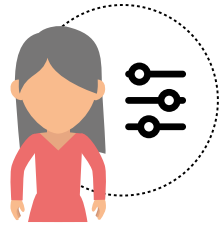
Children's data is particularly sensitive, and children have a right to ask for certain data to be deleted – this really is linked to social media accounts but has implications for schools.

If there are pending or potential legal proceedings data must be preserved.

Who is a 'Data Controller'?

The organisation that is ultimately responsible for the data collected about the data subject. It will be the governing body or academy trust. It can also be the head depending on the school structure.

The Data Controller must be satisfied that suitable policies and procedures are in place.



The Data Controller must ensure that:-

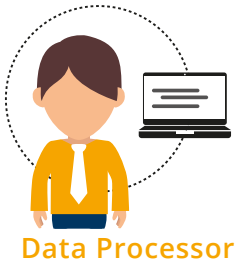
- Suitable Privacy Notices are in place
- The Data Protection Policy is fit for purpose
- In the event of a breach, suitable plans are in place to manage the breach and liaise with the Information Commissioner
- There is awareness of the changes across the school workforce, and that staff understand their personal responsibilities and liabilities
- The concept of 'Privacy by Design' or collecting only as much data is necessary for a task, is embedded in the school
- A suitable Data Protection Officer is appointed
- New processes are assessed using a Data Privacy Impact Assessment
- Everyone can understand how their data is held, and how to request amendments or erasure is necessary
- Enabling a Data Subject to complain is a simple procedure
- Data is processed and categorised using one of the lawful criteria for processing

Whilst the Data Controller can delegate actions to their employees, responsibility sits with the Data Controller. In maintained schools it is the governing body, in academies it is the trust. Compliance with Risk Management and Scrutiny obligations all require effective oversight of GDPR compliance and practive.

Article 5(2) states that

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Who is a 'Data Processor'?



This is a person or organisation that uses, collects, accesses or amends the data that the controller has collected or authorised to be collected on behalf of the data controller. It can be a third-party company, a contractor or temporary employee. It can also be another organisation such as the police or the LA. Of course, staff in schools are processing data.

Data controllers must make sure that data processors are as careful about the data as the controller themselves. The GDPR places additional obligations on organisations to make sure that Data Controllers require contractual agreements to ensure that this is the case.

In schools employees and volunteers process data on behalf of the controller. Though they are not considered to be 'Data Processors'.

Processing data

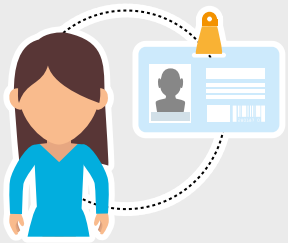
Schools must have a reason to process the data. The GDPR has 6 conditions for lawful processing, and processing must be within one of them to comply.

- School has the consent of the Data Subject
- It is necessary for the performance of a contract
- It is necessary to comply with a legal obligation
- It is required to protect the vital interests of the data subject, or another person
- It is necessary for the performance of a task carried out in the public interest or the exercise of official authority
- It is necessary for purposes of legitimate interests pursued by the controller or a third party (but not where the data subject's rights override the controller)

Sensitive Data

Processing sensitive data in schools requires careful consideration. Gaining consent is required, unless there is another legal basis to do so, for example safeguarding or protection of vital interests.

Data Protection Officer


Data Protection Officer

Every public authority, which includes schools, must have a Data Protection Officer.

The data protection officer shall have at least the following tasks:

- to inform and advise the controller or the processor and the employees who carry out processing of their obligations under the GDPR
- to monitor compliance with the GDPR and DPA
- to provide advice where requested about the data protection impact assessment and monitor its performance
- to cooperate with the supervisory authority and manage the breach procedure
- to advise about training and CPD for the GDPR
- should have expertise in national and European data protection laws and practices and an in depth understanding of the GDPR.
- to support the rights of Data Subjects

The Data Protection Officer's details should be on the school website, Privacy Notices and in the Data Protection Policy.

Privacy by Design

The idea of the GDPR is that data should be carefully managed and curated. New processes should be subject to assessments. These are to consider risk and how this can be managed as part of the procurement process. This has an impact in classrooms and school offices.

Information Commissioner Office (ICO)

In the UK it is the ICO who has responsibility for safeguarding and enforcing the DPA obligations. The ICO has the power to issues fines, publish decisions and seek undertakings.

Breaches

Breach preparation is key. Breaches happen as a result of human error. They are rarely deliberate (unless planned criminal activity) more likely to be as a result of forgetfulness or mistake. An email sent to the wrong person is the most frequent source of a breach.

The GDPR requires certain breaches to be notified to the ICO within 72 hours. In some cases 72 hours will not be long enough to complete the investigation. A key part of the response must be risk assessment of the data that has been lost and the planned remedial action to be taken as a consequence of the breach.

The Data Controller will need to have confidence that these can be handled, and reported back to the controller as necessary. Many breaches are internal action only, the more serious are reported to the ICO. Advice from the DPO is important to manage the process effectively.

Sanctions

New powers and sanctions apply – up to 20 million euros or 4% of global turnover in fines. Although no school has yet been given a financial penalty. It is now possible for individuals to seek compensation is new with the GDPR.

Criminal offences for reckless or deliberate breaches can affect every single one of us. The message must be that from a personal point of view the GDPR is that everyone who interacts with data is potentially culpable. Reckless loss of data can include leaving a file open for others to view it, it could be inadequate security measures. Reckless has a wide scope and the Data Controller has a responsibility to take measures, failure to do so could also be considered reckless.

Safeguarding

GDPR does not, at all, ever, prevent information sharing to protect children and/or vulnerable adults. Schools have statutory and other obligations to ensure that children are protected. Serious case reviews often point to the lack of good information sharing as a feature of child deaths.

Understanding that there is a process to be followed and mechanisms to ensure that data is shared appropriately need to be in place.

If in doubt the matter should be referred to the Designated Safeguarding Lead, the DPO and the local authority protection teams.

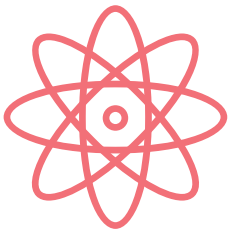
What is required?

The guidance from the ICO is clear. Understand and know your data. Mapping is a tedious, time consuming but vital task. Schools must ensure that they understand their data and how it is to be collected, used, stored and destroyed. Without that knowledge there cannot be good GDPR compliance.
Every school has to have a Data Protection Policy that reflects the GDPR requirements. This will be on the website and will explain in more detail obligations and how the school will meet these.
Every school should have a person who is designated to be responsible for data protection compliance, and to have a Data Protection Officer (who may be within school or outsourced).

IT security is a key element of data protection and an acceptable use policy, IT policy or similar is likely to be in place also. Compliance is likely to be mandatory and will include things such as not using a personal email address, only using encrypted mobile devices and the process for locking a computer if away from the desk.

The more information on the website, the better.

IT and Information Security



Many processes used on a daily basis in schools use IT. Whether this is emails, progress tracking, attendance management, cashless payments or many, many more examples.

Making sure that the IT systems, levels of access and protective measures are suitable is the responsibility of the Data Controller, but in practice will be delegated to operational leads to check and secure the outcomes.

Checking firewalls, server security and the location of and protection of back ups will be important elements of this strategy.

The Data Controller must be satisfied that effective IT security is in place, that it is well managed and up to date.

Encryption

The Information Commissioner has issued a number of notices and guidance about how important encryption is –

'Encrypting data whilst it is being stored (eg on a laptop, mobile, USB or back-up media, databases and file servers) provides effective protection against unauthorised or unlawful processing. It is especially effective to protect data against unauthorised access if the device storing the encrypted data is lost or stolen.' ICO

If a laptop that is encrypted is stolen, the chance of a data breach will be minimal, if a laptop with a password is stolen the likelihood of a data breach is very high.

Encryption can also be applied to tablets, ipads, smart phones and memory sticks.

The Data Controller must be satisfied about how mobile devices are protected. What is the school policy about personal devices? How does that fit with good GDPR?

Email

Email is not a secure form of messaging. It has been said that an email has as much security as a postcard.

Sending sensitive data by email must be done in a secure way. That might include password protected word, excel or pdf documents. It might include getting parental consent to use email for more sensitive correspondence, or finding an alternative by sending an email with a securely controlled attachment.

Personal emails **must** not be used for school business, and that includes governors and trustees emails too. A Subject Access Request can be applied to personal accounts in some cases.

Staff, Parent's and Pupils Rights to view Data

Unless there is a reason to refuse that is linked to legal confidentiality, safeguarding the child or another person, a contractual or regulatory reason the basic position is that all data should be disclosed on request.

A 'Subject Access Request' (SAR) process should be in place. It should be clear and if any parents want information about their child, or themselves, that is more than the usual round of parent's evening

and reports, then they should be directed to the process on the website. Any request made to you should be directed to the in school person responsible for dealing with a SAR.

Each request must be considered on a case by case basis.

The school must have a process to manage the request and the timeline to comply. The Data Controller is obliged to comply with the timeline, and be satisfied that those acting on its behalf have a clear understanding of what needs to be done.

Subject Access Requests have increased over the last 12 months. Some have been easy to manage, some have involved hundreds and thousands of emails. One has been in excess of 100,000 emails. The resources to manage the scale of these requests can be very significant. Having a process to destroy emails, unless they are required, is very important.

Overview

All schools have sensitive data, and it is used in classrooms and in the office. When an individual uses, accesses, collects or edits that data they are responsible for ensuring the security of the data. Getting consent to use the data is a very important factor, but schools can share data with other professionals to safeguard children and help detect crime. Every time we are asked to share data we need to know what is the lawful basis for doing so, and if in doubt check, with a line manager or with a lawyer.

Keeping data safe is an obligation on the school and the individual. Schools must make sure they have suitable processes, effective policies and the right support for staff. Staff must make sure they understand their obligations and need to comply.

If there is ever a breach, then working together will be the best way to put it right, learn the lessons and move forward.

As the Data Controller, governing boards and trustees have a direct legal obligation to ensure that suitable polices, procedures and measures are in place.