UK GDPR - What do you need to know?

J A Walker, Solicitor

www.jawalker.co.uk
john@jawalker.co.uk
0333 772 9763

Introduction

Everyone in school needs to understand how UK GDPR affects them. Both as people who manage and process data about others, and also as individuals who have their data stored and used by school. This is a summary, but in school the Data Protection Policy and Privacy Notices have more detail.

What is the UK GDPR?

This is a European Directive that is now part of UK law with an updated Data Protection Act 2018 (DPA). Brexit will not change it.

What happened?

Data Protection changed across the UK from 25 May 2018. In schools there was already a wealth of good practice. Whilst some changes are necessary, it was about building on existing strengths. At the time there was a lot of hype and scaremongering, and whilst this disappeared overnight, UK GDPR obligations are here to stay.

There is a greater focus on individual obligations, responsibilities and rights. There is an expectation that schools are able to show what data they hold, why they hold it and how it is stored. People who work in schools need to understand what this means for them on a day to day basis.

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 the point of the UK GDPR?

The UK GDPR and new 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 UK 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, UK GDPR was never designed with schools in mind. The focus is on big business, international brands, banking and insurance sectors and government. The UK 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 UK GDPR and proposed provisions in the new Act.

What does it mean for us as an organisation?

In school we all need to be more aware of the data we hold and how we use and store it. We need to stay alert for situations that may give rise to a breach, for information that is inadvertently left out on desks, or up on walls.

Some policies will need reviewing. UK GDPR needs to be on the whole school agenda, awareness and good data protection processes need to embed as time goes by.

Schools must have a system of audit and monitoring to ensure continued compliance. Everyone will share that responsibility to a greater or lesser degree.

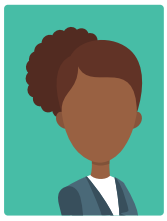
What is Data?

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. In schools a lot of the data we use daily falls into the sensitive category, the more vulnerable the child, the more sensitive the data.

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

Everyone one of us is a Data Subject. Anytime our name, date of birth, NI number or similar is used our data is being processed, and we have a legal right to make sure it is done lawfully and purposefully.

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

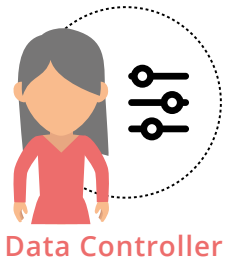
Schools must inform people about how they hold data, and also that individuals have a right to access it. This can be limited in some instances, for example where child protection is involved, or if there are legal or contractual exemptions. Schools need to tell people how they can do this and explain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

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. Retention policies are important in schools.

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.

Individuals employed by the Data Controller process data on behalf of the organisation.

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, possibly a governor, a contractor or temporary employee. It can also be another organisation such as the police or the LA. Of course, school staff and volunteers are all processing data too.

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

Processing Data

Schools must have a lawful reason to process the data.

This might be based on consent of the Data Subject. It might be that the school has a legal reason to process the data, safeguarding or paying tax are good examples.

Whilst 3rd parties process data on the instructions or as a result of the legal obligations of the Data Controller, school employees process data as part of their employment contract. Whatever the status of the individual or organisation, the obligations to care for and manage the data are the same.

In every school a process that maps data collection, use, sharing and storage is necessary. The Information Commissioner Office (ICO) expects all public authorities to do this.

Data Protection Officer (DPO)


Data Protection Officer

Every public authority, which includes schools, must have a DPO. The DPO's main function is to be independent and give advice about Data Protection compliance. If something goes wrong, the DPO helps to manage the process and to liaise with the Information Commissioner, and sometimes police and social care.

The DPO is there to ensure that the data controller is aware of, and fulfils, their legal responsibilities.

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

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. The ICO also issues guidance, that in reality must be followed.

Privacy by Design

New processes or software should be subject to assessments. This is to make sure that any new process takes account of how data is used and any risks that arise. This has an impact in classrooms and school offices – new attainment tracking or finance software for example. You may be required to provide input into this type of assessment.

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 UK 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.

In your school, you must know who to report the breach to. The sooner a breach is reported, the easier it is to fix it.

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. Data can also include opinions, not all of which may be flattering to the requester.

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.

What about information about me?

School staff have the same rights, and are subject to the same exceptions, as parents. You have a right to request the information.

Safeguarding and Child Protection

Keeping children and young people safe is the priority. UK GDPR and Data Protection is never an excuse to not share data with the police or social care. There are procedures to be followed, of course. At every training course I run I explain that I would always prefer to stand in front of the ICO and explain why I shared data, rather than a coroner or high court judge and explain why I did not.

Police requests, except in a genuine emergency, should be made on specific forms. Any such requests need to be referred to the data protection lead in school before information is shared. If it is an emergency, share the data but keep a record of why it was essential.

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, and it is important to be aware that the ICO wants to see good practice and compliance. However, there is now also the option for individuals to seek compensation is new with the UKGDPR. Criminal offences for reckless or deliberate misuse of data are also part of the legal framework.

Mike Shaw, who heads up the criminal investigations team at the ICO, has said:

> ***"People expect that their personal information will be treated with respect and privacy. Unfortunately, there are those who abuse their position of trust and the ICO will take action against them for breaking data protection laws."***

Breaches can affect every single one of us. The message must be that from a personal point of view the UK GDPR is that everyone who interacts with data is potentially responsible.

What do Schools have to do? Where can I find this out?

Every school has to have a Data Protection Policy. This will be on the website and will explain in more detail obligations and how the school will meet these. Data Protection is also likely to be part of other policies, such as HR and staffing, CCTV, SEN and inclusion.

There will also be Privacy Notices that explain how data is stored and used. Privacy Notices can be used for different scenarios or groups of people, for example the pupil notice will be very different to the staff notice.

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). You need to know who this person is.

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 will 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.

It is important for all individuals to understand what is expected of them.

What impact does this have in the classroom?

The bottom line is to think about how you would feel if data and information about you and your family was accessed by an unauthorised person? Personal information needs to be cared for as though it was our own.

There are many instances where the school has no choice about how to manage or collect data. When it is mandatory, there can be option to opt out, or any need to seek consent. This covers a lot that happens in schools.

Pragmatism needs to be factored in too. The key function over every school is to provide an environment where children flourish, where good teaching and learning is paramount. There are a lot of myths about Data Protection. For example, it has been suggested that teachers can't call out a class register. That is ridiculous. It is a legal requirement to have a register. All the children in the class know each other, adults in the classroom are there with school authority.

What would be unacceptable would be if the register was returned to the school office, left on the reception desk and accessible to parents or school visitors.

Likewise, a stack of books for marking may have the child's name on the front, but it is unlikely they would contain any sensitive information. In the same way classroom displays with children's names next to them are not going to raise any data protection concerns.

But a specific learning plan for a child, or details of a child's health needs or SEN needs would be very sensitive. So such records need to be carefully looked after. They should not be left in a room that is not secure, or in a place where they can be accessed by unauthorised people. Locking information away safely is simple to do.

Any records that leave school, to go to meetings or are taken home to work on in an evening or at the weekend must be secured at all times. A locked cupboard or desk at home will suffice. Records

should never be left in the car or unattended. You are responsible for their security when they are in your possession.

When you leave the classroom or school office at night make sure anything sensitive is locked away.

How can it affect me?

For teachers

The Teacher Standards 2013 require 'Teachers must have proper and professional regard for the ethos, policies and practices of the school in which they teach, and maintain high standards...'

For everyone else

Contracts of employment, legal obligations around children protection and safeguarding require certain professional standards.

Also the Data Protection Act 2018 makes it a criminal offence if a person knowingly or recklessly obtains or discloses personal data without proper authority. Being reckless can include having an overheard conversation about a pupil or parent, leaving documents on a desk that are seen by someone else. It could mean losing an unencrypted memory stick with personal data on it, or even having a file of papers stolen from your car.

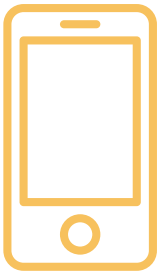
Criminal, civil and disciplinary action could follow, even where the loss is by mistake.

What about health needs?

If a pupil has health needs, for example a severe peanut allergy, notification should be given to the parent/carer that there will be a photo with the pupils name and allergy details in school at points where the risk occurs. - You do not need consent to share the information. So it may need to be in the form room, staff room and kitchen area. This should be explained parents and the pupils concerned (depending and age and capacity) to ensure that supply staff and others in the school can be aware of risks for individual pupils.

Balancing the child's health needs and data protection considerations are important but well- being is of critical importance, and data protection should never place an individual at risk of harm.

Can I use my own pc, laptop, smart phone or tablet?



Each School policy needs to set out if you can or cannot. If yo u access any sensitive or personal school information on your own device, then you need to be mindful of the UK GDPR obligations.

Encryption of mobile devices such as phones, tablets, USB sticks and laptops is essential. Your IT support should be in a position to advise about this in more detail. Encryption can be very simple to set up, for example an entry PIN code on a phone may be sufficient.

Understanding what encryption is and what is simply password protection is important. Just a password is not secure enough to comply with the DPA.

You also have to be aware of where your personal device stores data. If it is in the cloud you may be in breach of the DPA, lots of cloud storage is not hosted in the UK or Europe. If in doubt, check with your in school IT support.

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.

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 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 should not be used for school business, and that includes governors' emails too.

Overview

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.

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.

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

We need to build on our current good practice, to take advice as is required, and to keep putting the needs of pupils first.