General Data Protection Regulation
2018
European Union
&
Data Protection Act
2018
UK

Personal Data
The GDPR Definition

- The GDPR applies to ‘personal data’ meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.
- This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.
- The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.
- Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.
- Legal directives that should underly our approach to everything we do with **Personal Data** and therefore the impact on our work in relation to:
    - Storage,
    - Use
    - Security
    - Permissions
    - Transfer and move
    - Retention
    - Display
    - Accessibility

Six Data Protection Principles'

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

Sensitive information has stronger legal protection

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences.

Data Subjects have Rights

Everyone has the right to find out what information the government and other organisations store about them, and these rights include:

- be informed about how your data is being used – typically through a privacy notice
- access personal data – a Subject Access request
- have incorrect data updated
- have data erased – if you don't plan on buying again from an online shop
- stop or restrict the processing of your data – you can store it but not do anything with it
- data portability - allowing you to get and reuse your data for different services
- object to how your data is processed in certain circumstances – unless you have an overriding legitimate reason to continue

You also have rights when an organisation is using your personal data for:

- automated decision-making processes (without human involvement)
- profiling, for example to predict your behaviour or interests – FB ads

Data controllers & data processors
Legal Obligations

- A Data Controller (DC) is the person or organisation who determines the purposes and means of processing personal data. – The school
- They are legally obliged to ensure that any data requested, collected and stored is done so whilst complying with the law and to respond correctly to any Subject Access Requests. Also to ensure that any Data Processor they use is complying as well.
- A Data Processor is responsible for processing personal data on behalf of a controller. - ParentPay
- They must follow the documented instructions of the ‘DC’ and ensure compliance with data protection regulations. – you should have a GDPR compliant data sharing agreement in place

Just because you can doesn’t mean you should

One of the first things we must consider is whether or not we need the information that we are requesting; what, why, when.

Scenario:

You are arranging a school trip to an outdoor activity centre. Before the details are finalised (date, price) you ask all parents who have expressed an interest to provide details of pre-existing injury and health conditions about which the school should be made aware of for the trip.

Asking yourself the what, why, when questions do you need the data at this point in time?

You do need to have a lawful basis for processing data.

Lawful bases for processing

1. The data subject gives **consent**
2. Necessary for **performance of a contract** with data subject or to enter into contract
3. Necessary to comply with a **legal obligation**
4. Necessary to protect the **vital interests** of a data subject or another person
5. Necessary for performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller – most of the data we have in schools, be it student or staff will come under public interest
6. necessary for the purposes of **legitimate interests –** Legitimate interests is the most flexible lawful basis, but you cannot assume it will always be appropriate for all of your processing. If you choose to rely on legitimate interests, you take on extra responsibility for ensuring people's rights and interests are fully considered and protected.

Whilst we can find a lawful base for processing data we must always ask ourselves two questions before doing so:

1) Do I need to process this data at all?
2) Is there a better way of achieving your objective

CONSENT

1. Be specific and granular - separate consent for separate things.
2. Avoid vague or blanket consent
3. ‘Explicit’ means a very clear and specific statement of consent
4. Keep consent requests separate from other Ts&Cs
5. Keep evidence of consent
6. Consent does not go off but it might degrade
7. Reconsider when students can consent for themselves
8. Don’t limit yourself to written only – if necessary you can get consent over the phone but it must be followed up with written confirmation
9. Consider your process for ensuring consents are followed
10. Check it all works!

The UK GDPR does not set a specific time limit for consent. Consent is likely to degrade over time, but how long it lasts will depend on the context. You need to consider the scope of the original consent and the individual’s expectations.

You need to keep your consents under review and refresh them if your purposes or activities evolve beyond what you originally specified. Consent will not be specific enough if details change – there is no such thing as ‘evolving’ consent.

Accountability and governance

You must have the following documentation available on your website as should any organisation that deals with data:

- Privacy Notice
- Data Protection Policy
- Retention and Deletion Policy

You must also have procedures for dealing with the following:

- Subject Access Requests (SARs) – these can be made in any form but must come from the data subject themselves, their parent or their legal representative; along with their consent
- Data Breaches – must be reported to the DPO as soon as you have become aware of one. The DPO must then report it to the ICO within 72 hours, even if it is with minimal data.
- Fines can now be up to 10 million Euros (or the equivalent in sterling) or 2% of your global income, depending on the severity of the breach.

Our biggest problems

- Filing things away straight after use
- Locking keys in cabinets in between uses
- Locking doors when leaving rooms/offices empty
- Sending email to the wrong person
- Computers
    - We should all have different passwords for logging in
    - Passwords must adhere to the school policy – do you know what it is or where to find it?
    - Lock your PC or laptop when you leave the room (CTRL+ALT+DEL)
    - Auto-lock for classroom computers should be set – is there a network setting for this?
    - **Passwords must not be shared with anyone.**

What do you need to do?

- You save a document containing data on a memory stick, which you then accidentally leave on the train.
- You send an email regarding a student or with data attached to the wrong person
- You've given personal information over the phone without confirming someone's identity.
- You've lost trip data paperwork before returning it to school to be shredded

All of these instances and anything similar must be reported to the senior lead on GDPR in your school and the DPO

You must report a data breach to either Sarah Manning or Faye Dennis as soon as you become aware of one