GDPR

25th May 2018

This is when the General Data Protection Regulation 2016 (GDPR) and the Data Protection Act 2018 (DPA) came into force. If you handle personal data in your role as an officer or employee of the school, it is essential that you are aware of the requirements.

Although GDPR and the DPA broaden the requirements, particularly in relation to demonstrating accountability and transparency, many of the key principles are the same as those in the previous Data Protection Act 1998.

Throughout this guide, you will see this icon: 

It will highlight handy tips that must be taken seriously and actions put in place.

INDEX

Key Aspect 1 – Useful Definitions

Here are some key words (with definitions that will be used throughout this practical guide:

Data Subjects

A “data subject” under GDPR is an identified or identifiable natural person (i.e. a living individual not a corporate body or company).

Personal Data

This relates to a set of information that can identify a data subject or subjects. As well as obvious personal identifiers such as name and address, under GDPR this includes such things as genetic and biometric data.

Special Categories of Personal Data and Criminal Personal Data

“Special categories” of personal data relate to data which reveals an individual’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union activities, physical or mental health or sex life/orientation.

“Criminal personal data” relates to data about alleged criminal offences, criminal convictions and sentences.

Data Controller

This is the body which determines the purposes and means for which personal/special category/criminal data is processed. The School as a whole is a “data controller” for the purposes of GDPR and DPA.

Key Aspect 2 – The Six GDPR Principles

As a data controller, we must be accountable and keep records evidencing our compliance with the following GDPR principles. Such record keeping would include the logging of any new system onto our Information Asset Register.

1. Lawfulness, Fairness and Transparency

Personal data can only be processed if there is a lawful reason for doing so. It must be fair to the data subject and you must be fully transparent with the data subject as to why you are collecting their data and how it is going to be used and shared.

2. Purpose Limitation

Data should only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes, although further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes is permitted in certain circumstances.

3. Data Minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

4. Accuracy

Personal data must be accurate and, where necessary, kept up to date. Where personal data is inaccurate every reasonable step should be taken to enable its deletion (where appropriate) or correction without delay.

5. Storage Limitation

Personal data must be kept in a form that permits the identification of data subjects for no longer than is necessary. Such personal data can be stored for longer periods for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in certain circumstances and subject to the implementation of the appropriate technical and organisational measures.

6. Integrity and Confidentiality

Personal data must be processed in an appropriately secure manner: including protection against unauthorised or unlawful processing and against theft, accidental loss, destruction or damage, by the use of appropriate technical or organisational measures.

Key Aspect 3 – Rights of the Data Subject

One of the key factors of GDPR is that data subjects are granted certain rights and protections relating to their personal data. This includes:

Collecting their Data

When we collect data from our citizens, we must ***inform*** them about the reasons why we are collecting it and their rights. We also have a duty to ensure the data collection is ***limited*** to what is necessary in relation to its purpose and we don't use it for a ***different*** purpose without seeking legal advice beforehand.

Here are the five GDPR legal basis conditions which we rely on to lawfully process personal data:

1. **Legal obligation**: the processing is necessary to comply with a legal obligation. If your service is statutory, this is the basis for you;
2. **Public task**: the processing is necessary to perform a task in the public interest or in the exercise of official authority. This is where you are empowered by law but not obliged to provide a service (e.g. parks);
3. **Contract**: the processing is necessary as part of a stated or implied contract;
4. **Consent**: the individual has given clear consent for you to process their personal data for a specific purpose. This is the least favoured of your options because an individual is able to withdraw their consent at any time.
5. **Legitimate Interest**: either of the School or of a third party, which is not outweighed by the private interests of an individual.

So, if you collect personal data through an application form or survey, you must state on the form: why we are collecting this data and what we are going to do with it (Privacy Notice).

If you do not need to find out their date of birth for example when gathering the data on a form, you ***must not ask for it!***

If you use data for a different purpose (to your original purpose) then you will not be complying with GDPR; unless that other purpose is compatible with the original purpose.

Objecting to the use of their Data

The GDPR includes the “right to object”: meaning that the data subject can object to the processing of their personal data. If the objection is to direct marketing, the data subject does not need to give any reasons and staff must comply with the request.

When the data subject objects to other types of processing (i.e. not direct marketing) there are exemptions that apply. You will need to discuss this with your manager and take advice from him/her before proceeding.

To demonstrate that you are complying with the GDPR first principle of processing personal data, (that it is processed lawfully, fairly and in a transparent manner), you must maintain a record of any request made under the right to object to processing and notify your manager of your actions.

Review existing processes to ensure that where you undertake marketing communications with citizens by email, you include an ‘unsubscribe’ option to allow them to object to the use of their information.

Accessing their Data

Our citizens are able to access their data via a “Subject Access Request”. These requests must be handled without delay and within one month of receipt.

We must provide this information free of charge from 25th May 2018 and it is imperative that requests are taken seriously and handled efficiently.

The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing.

We are able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, you must inform the individual within one month of the receipt of the request and

explain why the extension is necessary.

At all times, we must ensure that the data we have collected from our citizens now or in the past is accurate and up-to-date. Staff must take reasonable steps to ensure that where data is inaccurate, it is ***rectified*** without delay.

Just imagine your personal data being sent to the wrong address by your bank because the wrong house number was on their ICT system. How would you feel if your neighbour had opened the letter and read certain personal details about you?

Everyone is busy but staff are sometimes more concerned with completing their tasks than ensuring the data of our citizens is secure. This must change under GDPR or you are putting the School at risk of fines and reputational damage.

Citizens have the right to contact the Information Commissioner to report where we have failed to keep their data accurate or their data has been breached. This could result in compensation to the citizen on top of a fine from the Information Commissioner.

Storing Data

Citizens have the right to ensure that their data is not kept by us for longer than is necessary.

Staff must ensure ***we do not hold data*** any longer than required. Remember all data that we hold is open to Subject Access and Freedom of Information requests.

If your role consists of processing data, you are accountable for protecting this data from unauthorised or unlawful processing and against accidental loss, theft, destruction or damage.

Staff are responsible for ensuring that all ICT devices are encrypted in case the device storing the data is lost or stolen.

Sharing Data

When sharing data you must ensure a Data Sharing Agreement or a Data Processing Agreement is in place and contact should be made with the Legal Section when embarking on this.

Deleting Data

Under certain conditions, citizens can now request the erasure of their personal data. These are the conditions, one of which must be met:

- the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
- where the legal basis for processing is consent, the data subject withdraws his or her consent for us to use it; or
- the personal data has passed the retention period defined in the corporate records retention schedule.

If any of our citizens' personal data has been made public via a third party then we must take reasonable steps to inform the data processors who are processing the personal data on our behalf that the data subject has requested that they want their data deleted.

The right to be forgotten only applies where the above conditions are met and there are further exemptions where we can refuse to comply with a request:

- If it conflicts with the "right of freedom and expression".
- An overriding need to adhere to legal compliance.
- Reasons of public interest in the area of public health.
- Scientific, historical research or public interest archiving purposes.
- If the data is required for supporting legal claims.

Key Aspect 4 – Privacy Notice

Being transparent and providing accessible information to our citizens about how you will use their data is a key element of the GDPR. We must inform the data subjects at the first point of contact what to expect when we collect their personal data.

As part of our journey to GDPR compliance, we have written a new bilingual overarching corporate Privacy Statement, which sits on our website.

Inserting a Privacy Notice

When collecting personal data from the public (typically this is achieved through an online or a paper form), you have to provide more specific information than is contained in the overarching corporate Privacy Statement.

You must ensure there is a short Privacy Notice with the data collection document which explains your use of the data, who you share it with and what is the legal basis for you processing the data.

Advice on Privacy Notices can be obtained from your Data Protection Officer.

As mentioned in Key Aspect 3 of this guide, there are five main legal basis for the School to be able to capture and process personal data, and all data collection forms must make clear what the legal basis for processing is, if we want to be compliant with GDPR.

Key Aspect 5 – Providing Consent

We have already mentioned that consent is one of the legal basis for processing and if we can avoid relying on consent then we should do so. Here is why:

An indication of consent must be unambiguous and involve a clear affirmative action by the data subject.

If you are collecting special category personal data, the bar is set even higher. In that case you will need explicit consent, such as a written signed statement from the data subject.

Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service.

Consent involves presenting the data subject with a clear statement regarding the personal data to be collected; and an explicit action agreeing with this statement (such as ticking a box saying 'I agree').

The form should say, "I consent" (or similar) for consent to be considered valid. ***Silence or pre-ticked boxes*** on webpages are banned under GDPR as they do not establish explicit consent.

Withdrawing Consent

The GDPR gives a specific right to withdraw consent. Where we are collecting data which is legally based on consent, we need to tell people about their right to withdraw, and offer them easy ways to withdraw consent at any time.

We need to review our existing consent mechanisms to check they meet the GDPR standard. If they do, there is no need to obtain fresh consent.

It is important for staff to maintain appropriate records in order to evidence consent has been given.

Key Aspect 6 – Information Asset Register (IAR)

Maintain a Register

One of the requirements of GDPR is to maintain a record of all the processing activities that take place within the School. For this, we need to identify:

- what personal data we process;
- what is the lawful basis for processing;
- how we store and keep the data secure;
- who has access to it;
- who we share the data with and what sharing arrangements are in place;
- how long we keep it for.

Please liaise with the Data Protection Officer for access to the IAR and how to complete.

Providing an Overview

The record will provide an overview of all data processing activities within the School, and therefore enable us to demonstrate to the Information Commissioner what personal data is being processed, by whom and why.

Your Responsibility

If you collect and hold personal data electronically within your service then you must identify the system on the record. You must keep this information up-to-date.

NOTE: If you have not identified your system on the record and a data breach happens within your area, the ICO will hand out far more significant fines.

Key Aspect 7 – Data Protection Impact Assessments

Assessing the Risk

Data Protection Impact Assessments (DPIA) are a method that we must introduce under GDPR for ***assessing the risk*** associated with the processing activity we undertake of personal data.

Whenever a new system is being designed or introduced, or an existing system is being changed via a project, staff must undertake a DPIA to determine the risk to individuals' privacy associated with the processing.

A DPIA will:

- Help the project have a clear data protection focus;
- Allow appropriate organisational and technological measures to safeguard information to be built into any new operation;
- Challenge the designer to develop a way of working that will promote data protection principles;
- Give practical solutions to enable a data subject to exercise their rights

Just like the equalities impact assessments already undertaken within the School, if you are not sure a full DPIA is needed, you carry out a simple screening exercise which will guide your decision.

Data protection should not be a secondary function or consideration when designing a new processing activity. It is vital therefore, that staff, project leads and managers do not leave data protection principles and citizens' rights under GDPR to be considered at a later stage of the planning and design process.

Under GDPR, failure to carry out a DPIA where one is necessary can lead to enforcement activity and a fine from the Information Commissioner.

Key Aspect 8 – Data Breaches

The School has an existing process in place to detect, report and investigate a personal data breach. The Data Security Breach Panel are responsible for investigating and reporting all data breaches within the School.

However, GDPR bring in a new breach notification timeframe under which we will have to notify the Information Commissioner of serious breaches within 72 hours of discovery of the breach. A failure to report a breach within the timeframe could itself result in a fine, as well as a fine for the breach itself. The fine could be up to **£17,000,000**.

These fines can be significant sums which, with the reputational loss that comes with the associated press coverage, may impact severely on the work of the School.

Impact of a Data Breach

The first 24 hours are critical! A data breach can potentially have a range of significant adverse effects on the rights and freedoms of data subjects. The breach may cause them physical, material or non-material damage. They may as a result of the breach be at risk of domestic violence or of credit card fraud.

When a breach is identified you must report it as soon as you become aware of it in line with the School's Policy:

Staff must respond quickly and efficiently to lower the impact of the breach.

Key Actions

When a data breach occurs, here are the ***key actions*** to undertake:

- if there is a high risk to the data subject from the breach (e.g. identity theft, fraud or domestic violence), they need to be told straight away so they can take actions to protect themselves;
- Containment is key. If we can retrieve the data from the unauthorised recipient, go and get it straightaway;

- When retrieving the data from them, confirm that no copies of the data has been made or shared;

- Ask if they have read the whole document or just parts of it and if they know the person who should have initially received this information;

- Report the breach to the DPO.

Key Aspect 9 – Data Protection Officer (DPO)

GDPR introduces a requirement to appoint or designate a Data Protection Officer (DPO) with formal responsibility for data protection compliance in the School. The School's DPO is the head teacher who works in the School to ensure compliance with the legislation.

The tasks of the DPO include:

- Informing and advising its employees of their data protection obligations;
- Monitoring compliance of policies and procedures. This includes monitoring responsibilities and training of staff involved in data processing;
- Ensuring the IAR is an active register that identifies all systems that hold personal data;
- Advising on the necessity of data protection impact assessments (DPIAs), the manner of their implementation and outcomes;
- Serve as the contact point for all data protection issues, including managing risks and data breach reports.