VEDA MANDIR
GUJARATI SCHOOL BOLTON

GDPR NOTES & IMPLEMENTATION

VEDA MANDIR
GUJARATI SCHOOL BOLTON

GUJARATI SCHOOL
GDPR NOTES AND IMPLEMENTATION

Why GDPR?
Global communications has changed significantly in the last 50 years, and with the growth of internet technologies and computing, it was inevitable that data privacy laws would need redoing - especially considering the legislation it replaces in the UK is now 20 years old (Data Protection Act 1998).

Apart from legislative reasons, there are real problems that GDPR aims to solve. It has become clear over the past 10 years that personal data is a valuable commodity (just look at Google and Facebook among other companies), where products and services are free at the point of use, supported by advertising and other processes that use the data collected.

Over the past few years there have also been a string of huge data breaches that have shown companies are hoovering up massive amounts of personal data, which has led to questions such as:

- What processes do they have in place to keep the data secure?
- Are they handling the data correctly?
- Do they have permission to use the data in the ways they are using it?
- Do they even need to hold the data in order to perform the function we asked them to perform?

GDPR will strengthen and unify data protection for individuals within the EU, and will force all organisations processing personal data about EU citizens to abide by the new regulation.

What is personal data?
Personal data is defined as any information relating to an identifiable person who can be directly or indirectly identified from it. This is basic information such as name and email address, photos, and IDs.

This includes any electronically gathered and/or stored information, as well as paper-based storage.

There are also 'special categories' of personal data that schools are likely to handle, such as ethnicity and health information, which have additional rules around how the data should be stored and handled.

Controllers and Processors
GDPR applies to both controllers and processors, so all parties involved can be liable.

As a controller you are required to determine the purposes and means of processing personal data, and you have legal obligations to ensure your contracts with data processors are GDPR compliant.

As a processor you are responsible for processing personal data on behalf of a controller, you are required to maintain records of personal data and processing activities.

Controllers and Processors
You must have a good reason to collect and hold personal data, which needs to fall into one of the six lawful bases:

- The Data Subject has given explicit consent for the data to be collected and used for a particular purpose
- It is necessary to process the to fulfil a contract you have with the Data Subject
- It is necessary to process the data to comply with a legal obligation you have
- It is necessary to process the data to protect the vital interests of someone
- It is necessary to process the data to perform a task in the public interest
- It is necessary to process the data for the purposes of your legitimate interests

VEDA MANDIR
GUJARATI SCHOOL BOLTON

GUJARATI SCHOOL
GDPR NOTES AND IMPLEMENTATION

Each piece of personal data processed by the school must be attributed to one of these bases otherwise the processing is not lawful. Much of the personal data processed by a school (or other state funded educational establishment) will fall under the public task base. But you should always ensure that this is the case. For example, it's lawful to collect student address and telephone number under public task but it is not lawful to then share that with other third parties for a 'non-core' task without gaining appropriate consent.

Reasons for processing data

The new regulations are designed to prevent organisations from collecting massive amounts of personal data, when they don't necessarily need it for the purpose it was collected for, or that purpose has been served and there is no longer a need to keep it.

Part of preparing for the new regulations is going to be about auditing all the personal data you hold, and determining whether you actually need it. This process should also be documented, because we will all have personal data that we no longer need. Documenting what data there is, why you need it or how it has been discarded, is evidence that you have proper processes in place should a data breach occur.

This alone is not going to be a simple task, when you get down to stores of unstructured data, such as Word documents, spreadsheets, and email archives; determining whether they contain personal data, why it was created, and who's data it contains, then deciding what to do with that data is not going to be an easy task.

What is data breach?

The definition of a personal data breach is now more robust and clear than previous legislation; a personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Whether accidental or deliberate, anything that causes personal data to be lost, destroyed, corrupted, disclosed or unavailable, for whatever reason (for example, if it becomes encrypted by malware), can be considered a breach, and the ICO must be notified within 72 hours of the breach being discovered.

If the breach is significant enough to adversely affect the rights or freedoms of data subject(s), they must also be notified.

All this adds up to mean that you must have a plan in place for how data is to be protected,, how your systems should be monitored for data breaches, and for what happens if a breach occurs. Staff will need training on how to handle data and record how it is used.

Rights of the individual

GDPR is designed to give control over personal data back to the data subject, as and such it defines a number of individual rights over that data that organisations must adhere to, they are:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Individuals whose data you will be processing now have the right to be informed about the collection of any of their personal data, the reason you are collecting it, how it will be processed, who it will be shared with, and how long it will be held for.

VEDA MANDIR
GUJARATI SCHOOL BOLTON

GUJARATI SCHOOL
GDPR NOTES AND IMPLEMENTATION

They also have the right to request to see that data, for that data to be available for use by other services that the individual requires, for any incorrect information to be corrected, or for data be deleted (depending on the basis for the data being processed). They can also restrict usage of the data, and for personal data processed on the basis of their consent, the individual has the right to withdraw consent at any time.

The basis for processing the personal data of a child is also more complex, as parental consent may also be required.

Know the difference: personal and sensitive data

Personal data comprises any information that can help identify a person or their family. In school records, this would be their name, their address, their contact details, their disciplinary records, as well as their marks and progress reports. This sort of data remains "personal" even if an individual chooses to publicise it.

A special category of data touches on more sensitive topics. Where schools are concerned, this includes students' biometric data (e.g. fingerprints, photos), religious beliefs (e.g. a student's opting out of religion class), health (e.g. allergies) or dietary requirements (which may hint at their religion or health). Data in this category may pose a risk to people and hence can only be processed under certain conditions. Schools likely won't be able to use it without parental consent.

Know the difference: data controllers and data processors

The GDPR highlights the importance of two roles, which can be either individuals or entities: a data controller determines the means and purposes of processing data, while a data processor handles the data on behalf of the controller. Each of these parties has different legal responsibilities.

The school will typically be the "controller", so it has to secure a clear contract with the "processor". A processor can take various forms: from a photographer to a shredding company, an online learning platform, or a piece of software. Any operation these entities perform on data counts as processing, even if it's automated: collecting it, storing it, retrieving it, destroying it, etc.

Good practises: monitor yourself

1. On what grounds are you processing data? There are six lawful bases for processing data under GDPR. Most relevant to schools is the lawful basis public task, which means they use the data to perform a task in the public interest. However, data collected for this purpose cannot be recycled for another purpose. For example, the school cannot share a parent's email address with a third party that promotes school events by claiming it is a "public task"; to share that data, they must seek another lawful basis, consent. Schools should also seek consent if they set up a student account on a cloud-hosting service.

2. What data is held where, and who has access to it? Schools should perform an audit on their data-processing practices. Once they have a full overview of the personal data at their disposal, they can consider the best way to protect it.

3. What security measures do you have in place? Data breaches aren't always the work of hackers and malicious software – they can also be the result of a laptop forgotten on a train, or a curious family member. For that reason, staff should only store personal data on school equipment, use strong passwords, and set their devices to auto-lock after five minutes. If personal data is downloaded to removable media, like a USB stick, it must be encrypted and password-protected, and kept away from other users. Staff should also undergo training on social engineering, phishing, cloud technologies, ransomware attacks and the like.

4. What do parents know? Schools should issue a privacy notice to parents via the prospectus, a newsletter, a report or a letter/email: in it, they should state the data they

VEDA MANDIR
GUJARATI SCHOOL BOLTON

GUJARATI SCHOOL
GDPR NOTES AND IMPLEMENTATION

collect, the reason they collect it, and the third parties that are privy to it. Keep in mind that, under GDPR, parents and students can request to see the data that is held about them free of charge.

What can schools do to comly with GDPR?

1. Create and maintain records

All records and students and parents that you create or currently have should be maintained. As part of the GDPR regulations any data you have on anyone (parents, students, teachers, staff and volunteers) should be correct. If not you most erase the data as soon as possible. If a parent, staff member, volunteer or student over the age of 16 requests to see the data you must be able to present all the data you have on them. This includes email data too.

2. Drafting data policies and procedures

All records and students and parents that you create or currently have should be maintained. As part of the GDPR regulations any data you have on anyone (parents, students, teachers, staff and volunteers) should be correct. If not you most erase the data as soon as possible. If a parent, staff member, volunteer or student over the age of 16 requests to see the data you must be able to present all the data you have on them. This includes email data too.

3. Providing training for employees

All records and students and parents that you create or Every member of staff needs to know about GDPR and what it means to comply by its rules and protection laws. They also need to know what the implications are if they don't comply and a complaint is launched against the school. The school could close down.

4. All the data must be kept safe

Any data on parents, students, staff and volunteers must be kept in a safe place in either a concealed place like a filling cabinet with a lock and key. You must nominate certain individual to only have access to this so that they can comply with GDPR rules. If data is digital and is kept on a computer, data must have sufficient security measures. These include passwords, pin numbers and verifications. All digital data must backed up onto a secure hard drive or onto a portal online storage area such as: Dropbox.

What can schools be doing now to become GDPR compliant?

- Ensure senior management team fully understand GDPR and its potential impact.
- Schools should document and review all of the personal data they hold; including data for pupils, staff, parents, suppliers and governors which should be organised and stored in an audit.
- Consider the personal data processed and ensure everyone understands how it is collected, where it came from, what it is used for and what risks are posed by its use.
- Schools should make sure that all staff are trained according to their roles and responsibilities. This should include general GDPR awareness training for all staff as well as more detailed training for staff with more responsibility (e.g. Head Teacher, Deputy Head Teacher, Data Protection Officer).
- Schools already have systems in place that verify individuals' ages and gather parental consent for data processing where required.
- An important area for schools is to identify ALL software being used within the school. Recent developments in apps for education have led to many teachers downloading apps and using these in their classrooms without the school knowing about this. Schools need to know what is being used, for what purpose and what personal data is involved so that they can ensure these apps are compliant with GDPR. Failure to do so could lead to breaches of GDPR, fines, enforcement action by the ICO and adverse publicity for the school concerned.

VEDA MANDIR
GUJARATI SCHOOL BOLTON

GUJARATI SCHOOL
GDPR NOTES AND IMPLEMENTATION

- As schools are classified as a public authority for the purposes of data protection and GDPR, they must assign a Data Protection Officer who is solely responsible for any data protection and compliance with the GDPR regulation. It is important to consider where this role will sit in line with the school's structure and governance arrangements.

VEDA MANDIR

GUJARATI SCHOOL BOLTON