Data Protection & Privacy Notices

DATA PROTECTION IN PRACTICE

Staff Consulted (Date)	Governors Review (Date)	Comments	Next Review Due (Date)
	Sept 2018		Sept 2018
	Summer 2019		Summer 2019
	Summer 2020		Summer 2022
	Summer 2022		Summer 2024

Data Protection in Practice

January 2018

sbm services
school business management

Data Protection in Practice

Every school has access to, uses and stores a lot of information, or data, about individuals; pupils, staff and parents. Taking good care of that data is vital. Everyone has a responsibility to ensure that data is properly care for.

Data that is accessed by people who have no right to it, either by mistake, human error or deliberately, is a data breach. The consequences for the school as an entity, and for individuals themselves can be severe. The General Data Protection Regulations (GDPR) that some into force in May 2018 increase the sanctions available - and include criminal as well as civil and financial penalties.

This is an overview for school staff. A more detailed account is available as part of the Data Protection Policy and other guides.

What is Data?

Data is 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 as part of DfE and LA requirements and pupil data may contain information about safeguarding, SEN or health needs. Information about other family members may also be on the school file.

Data Protection Principles

The GDPR has 6 basic principles about data in organisations:

1. **Lawful, fair and transparent:** You have to have a lawful reason to collect the data. People have a right to know how the data will be used, and it should not be in a way they do not expect.
2. **Limited for its purpose:** Data can only be used for the reason it was collected in the first place. Privacy Notices tell people how it will be used.
3. **Adequate and necessary:** It is only permissible to collect data that is necessary to perform a function. You should not collect or access and process data simply because it is there.
4. **Accurate:** It is important to have a process to check if the information on file is still accurate.
5. **Not kept longer than needed:** Data should not be kept for longer than is needed, a clear retention policy needs to be in place and applied.
6. **Integrity and confidentiality:** Data should be kept secure; this applies to hard copy and digital information. Keeping data secure in the classroom and anytime it is in use in outside school meetings is critical. When you have data in your possession, you are responsible for that data.

Using Data, being a Processor

Everyone in the school will be a data processor. It is a term for someone who accesses, changes or uses data about another person, child or adult. In schools there are legitimate reasons to use data. This can be for staff reasons; you have to access data to pay people at the end of the month. It can also be about pupils.

What happens if there is a breach?

The school Data Protection Officer (DPO) needs to be notified ASAP. It may be necessary to tell the Information Commissioner, and the person(s) affected by the breach. The DPO will determine this.

What happens next depends on the seriousness of the breach. There are potential disciplinary, criminal and civil sanctions that can be applied. The sooner a breach is reported, the sooner it can be dealt with.

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. Every school should have a 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.

What impact does this have on 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 your own.

However, pragmatism needs to be factored in too. And 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 incorrect as it is a legal requirement to have a register. All the children in the class know each other and 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 be personal data.

But a specific learning plan for a child, or details of a child's health needs or SEN needs would be very sensitive. Therefore 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.

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). 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 at night make sure anything sensitive is locked away.

How can it affect me?

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 in their own attendance and punctuality.'

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 peanut allergy, consent should be sought from the parent to have a photo with the pupil's name and allergy in school at points where the risk occurs. So it may need to be in the form room, staff room and kitchen area. This should be done with consent of the parents 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 tops DPA.

Can I use my own pc or laptop?

School policy needs to set out if you can or cannot.

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 is encryption 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 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 (e.g. 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. 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 governor emails too.

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.

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.

Conclusion

All schools have sensitive data, and it is used in classrooms and in the office. When an individual uses, access, 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.