Making sense of the GDPR Jargon for schools

Everyone wants to do the right thing in protecting personal data in schools. However, you must understand the language relating to data protection and privacy, and this can be quite baffling. Where possible misunderstandings can take place, you will inevitably find myths cropping up – we'll be dispelling a load of myths in a series of blogs over the coming weeks so keep an eye on our website.

Here's our attempt to turn the GDPR, data protection and privacy terminology into everyday language that every member of staff in schools will understand.

The GDPR – the General Data Protection Regulation

An acronym used regularly today for the new data protection laws which needed to change because the old ones were out of date in today's digital world.

ICO

The Information Commissions Office – sometimes referred to as the UK Supervisory Authority, which is the organisation that oversees data protection in England, Wales and Northern Ireland and, to a limited extent, in Scotland.

Personal data

Any piece of information that can identify a person, directly or indirectly. In particular, where it can be referenced to things like names, location, online IDs, or to specific things such as physical, physiological, genetic, mental, economic, cultural or social identity of someone. You will often see this in referent to the term Natural Person.

Sensitive personal data

As above but this is called Special Category personal data and needs to be looked after very carefully; it refers to very specific groups of personal data which could be particularly harmful to individuals if in the wrongs hands, not available when needed or not correct.

contact@gdpr.school **www.gdpr.school** **0203 256 2018**

Biometric and Genetic Data

Details about an individual which identifies them uniquely, such as finger prints or DNA.

Data processing

A collective term when you collect, use, share or store data. The GDPR focuses specifically, but not completely, on digital data such as used in computers, phones and tablets, and on websites.

Data Controller

This is the person or organisation that an individual has allowed, or is obliged, to hold their personal details. The Data Controller decides what, why, how, where and when personal data is processed. A school is most often the Data Controller, but it CANNOT process any data unless there is a lawful basis to do so. Find out more about your school's obligations as a Data Controller.

Data Processor

This is a person or organisation that the Data Controller has asked to 'do something' with the data they control. They must only 'do' what is allowed in the data sharing agreement. They would be seriously breaking the law if they used this data for any other purpose. In a number of cases, the Data Controller and the Data Proccessor is the same person or organisation. If a school collects and uses the data, without it by shared or processed with anyone else, then they are both Data Controller and Data Proccessor.

Data Sharing Agreement

You must have one of these with any person or organisation you share data with. It will clearly say what can and can't be done with the shared data. It will ask for reassurances on issues such as storage security, how long the data is kept and how is the data disposed of. There are good examples of data sharing agreements on the web and the ICO has formal guidance on their website.

Privacy notice

This is your notice to the world about the way you handle information you have access to. Every school must have one already and it's important that all staff know what it says and means. It should also be in clear language so it can be easily understood by parents and children, where relevant.

Lawful basis for processing

Also referred to as legal basis for processing No person or organisation can process data unless there is a legal reason for doing so. There are six main categories for lawful processing. You must find a lawful basis that fits the reason you are processing data. If you can't, and you still process personal data, then you are breaking the law. Take a look at what GDPR in Schools think you should consider when identifying your legal basis for processing data.

Encrypted Data

This is when the data is jumbled up. You need a 'key' to unjumble it otherwise it looks like rubbish. Personal data that leaves a safe and secure environment, for example, it goes out of school or is sent in an email, must be encrypted.

Data Breach

This is a breach of security, a breach of availability or data that is not correct when it should be; where accidentally or unlawfully personal data has been destroyed or misused. This might lead to physical or mental harm to an individual.

Profiling

The use of existing information about someone to predict how they might behave in the future. If you shop online, you'll see it all the time when the website suggests things you should buy as you have bought them before or they compliment a purchase. Profiling is used in education to predict students' end of key stage or examination performance.

Data Protection Impact Assessment (DPIA)

Also sometimes referred to as part of a PIA or Privacy Impact Assessment. It sounds very grand, but is just formalising and structuring considerations you probably already do. When you start or review a project or process, you consider all the things that can go wrong regarding aspects of personal data. You then think about how you would put it right or if it's worth the risk doing nothing. A DPIA is written evidence that you have been through this thought process. Schools are already used to Risk Assessments for safeguarding and H&S, so this is part of what schools need to consider.

Privacy by Design

This means you consider data protection and privacy from every angle in everything you do or plan.

Privacy Impact Assessment (PIA)

A tool used to identify and reduce the privacy risks.

Data Erasure/Right to be Forgotten

An individual can ask the Data Controller to remove and stop processing their personal data. If the Data Controller can justify it needs to process this data, then the request can be refused.

Data Portability

The ability to take data from one Data Controller and transferring it to another. A good example of this is changing banks or energy suppliers. In schools, data is regularly ported when students change establishments. Some data may not be portable due to it only being usable in a particular system but every effort should be made to make it available.

Data Protection Officer (DPO)

An expert on data protection who works independently to oversee that data protection policies and issues are correctly managed. Learn more about who can be your DPO.

Pseudonymisation

Sounds complicated, but it really isn't! It's used a lot in education where data is analysed and presented in reports or for examples, but the links to identify individuals are removed.

Subject Access Right

Also known as the Right to Access or SAR. If you hold data on anyone, they have the right to ask you for a report which says what, where, how and with whom you share that data.

Natural Person

A legal term used to be specific about individual human beings rather than a Legal Person, which may be a private or public organisation. Staff, learners, their parents and others whose data is processed by schools will generally be a Natural Person.