GDPR – Jargon Buster

Queen Katharine Academy

Term	Definition
	The General Data Protection Regulation (GDPR) only applies to organisations' use of personal data. This is any information relating to an identified, or identifiable, person.
Personal Data	This may include such information as a person's • Name • Contact Details • Identification Number • Online identifier such as username It may also include anything relating to physical and mental health, genetics, finances, or their physiological, cultural, or social identity.
Personal Sensitive data	Personal data which is more sensitive and so needs more protection. It includes information about a person's: • Racial origin • Political opinions • Religious and philosophical beliefs • Trade Union Membership • Genetic information • Biometrics (such as fingerprints, iris and retina patterns, where used for identification purposes) • Health – physical and mental • Sex life or sexual orientation
Processing	Anything done to personal data such as, collecting, recording, organising, structuring, storing, adapting, altering, retrieving,using, disseminating, erasing or destroying. Processing can be manual or automated.
Data Subject	The person whose data is held or processed (e.g. all your pupils and staff will be data subjects)
Data Controller	A person or organisation that decides how and why your personal data is processed (e.g. your school)
Data Processor	An external person who is not employed by your school who processes data on your school's behalf (e.g. your payroll provider, an external careers advice or your parental communications provider).
Data Protection	A person in your school or an external Data Protection Adviser who takes responsibility for monitoring data protection compliance.
Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
	There are 6 'lawful bases' (or reasons) that you can use to justify why you need to process person data. You only need to meet one of them. You can process data as long as

Lawful Basis

- It helps you fulfil a contract with the person - e.g. to fulfil your obligations to staff under an employment contract.
- You need to do it to comply the law - e.g. the law requires schools to pass certain information to the Department for Education.
- It will protect someone's 'vital interests' - e.g. to save as someone's life.
- It helps you to carry out your official functions or a task in the public interest - e.g. schools must process most of their data in order to function as a school.
- You have the express consent of the person - e.g. they have said they want to receive fundraising communications from your school's alumni network.
- You have legitimate interests in the data - e.g. if you are a private sector organisation with a genuine and legitimate reason for using someone's data, unless it's outweighed by harm to the person's rights (schools are unlikely to use this one)

Breaches

Personal data breaches can include the following examples

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.
- **Data left in insecure location** - could be a bag on a train or even as simple as a file left on a desk in a public area.
- **Data posted/faxed to incorrect recipient** - check and double check what you're sending and who it's going to.
- **Data sent by email to incorrect recipient** – inappropriate use of 'Reply to All' can easily result in a breach.
- **Failure to redact data** – Failing to obliterate personal details of another when sharing information.
- **Failure to use bcc when sending email** – If sending to multiple recipients, do they need to be aware of each other? Believe it or not more common than you'd think.
- **Insecure disposal of hardware** – what are you doing with your old computers or laptops etc?
- **Insecure disposal of paperwork** – incorrect use of the shredding bags or failing to use a shredding bag for personal data.
- **Loss/theft of only copy of encrypted data** – What is on **your** pen drive or external hard drive?
- **Loss/theft of paperwork** – Do you need to take it off site? If you do make sure it is secure.
- **Loss/theft of unencrypted device** – Watch for a change of policy coming soon requiring that all school owned equipment is encrypted or clearly identified not to contain any personal data.
- **Verbal disclosure** – Who are you talking to? Make sure it is the correct person.