SBS INSIGHT HUB

SHARD Business Services

INTRODUCTION TO DATA BREACHES - OVERVIEW

What is a data breach?

A data breach is a defined by the GDPR regulation as '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 transmitted, stored or otherwise processed' (Art.4[12]). Many data breaches are the result of human error, whether that be through honest mistakes or carelessness. Examples of breaches include:

- Accidentally sending an email containing personal data to the wrong recipient
- Losing a USB stick, documents, or a mobile device which contained personal information
- Intentionally or accidentally amending personal data without consent or permission
- Personal data being published on the school website without consent
- Throwing away personal data in the bin rather than shredding, for example, letters to parents
- Safeguarding information being shared with unauthorised people
- A virus or malware on the school system
- Accessing the system using somebody else's username and password
- A pupil having unauthorised access to a staff device/account
- Using 'to' or 'cc' where 'bcc' was required
- Posting pictures of pupils on social media without consent

It is essential that you know how to recognise data breaches, as we have an obligation to investigate data breaches and protect the personal data we hold. If you are in doubt about whether a data breach has occurred, ask for advice from your Data Protection Officer. Certain types of breaches need to be reported to the ICO within 72 hours, so it is better to be overly cautious.

Good practice to follow

- Implement a clear desk policy
- Locking your computer screen whenever you leave your device and setting screens to auto lock when periods of inactivity are detected
- If you're unsure about who is contacting you, check with somebody
- Backing up your systems and then testing you can retrieve your data
- Do not download attachments from senders that you do not know
- Make sure you shred all documents that contain personal data
- Ensuring you are aware of the organisation policies and procedures
- Avoid using portable media devices, such as USB drives unless fully encrypted
- Strong usernames and passwords that are changed regularly
- Keep work and personal emails separate – don't be tempted to mix the two
- Take care if taking personal identifiable data off site.
- Anonymise personal identifiable data wherever possible

DATA BREACHES

Responding to a data breach

Firstly, you need to know how to recognise a data breach and who to report it to. Remember, a data breach can be defined as any incident that has affected the confidentiality, availability, or the integrity of personal data, no matter how small.

You MUST report any suspected data breach to your school's Data Protection Officer.

Your DPO will then assess the risks and follow up on the incident. It is also good practice to inform of near misses and keep a record of both this and any breaches.
If you are reporting a breach, try to include the following information:

- What happened
- What data was involved
- How many people could be affected
- The likelihood/severity of those affected

Any breaches that are likely to involve 'risk to people's rights and freedoms', as outlined in Article 33, must be reported to the ICO. Again, the DPO will make this assessment based on the information available. It is important to remember that the faster a breach is reported, the better.

Legislation

'In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent explanation will be required. (Art.33[1])

'The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken' (Art.33[5])

REMEMBER: IF IN DOUBT, SPEAK TO YOUR ORGANISATION'S DPO FOR GUIDANCE ON WHETHER A BREACH HAS OCCURRED.