Data Protection – breach and non-compliance procedure

Breach management guidance

All staff, governors and trustees must be aware of what to do in the event of a DPA/UK GDPR breach. The 'Data Breach Flowchart' outlines the process.

Most breaches, aside from cyber-criminal attacks, occur as a result of human error. They are not malicious in origin and if quickly reported are often manageable.

Everyone needs to understand that if a breach occurs it must be swiftly reported so that risks to the data subjects are minimized and well managed.

What is a breach?

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

Examples of breaches are:

- information being posted to an incorrect address which results in an unintended recipient reading the information
- loss of mobile or portable device, unencrypted mobile phone, USB memory stick or similar
- sending an email containing personal data to the wrong person
- dropping or leaving documents containing personal data in a public place
- personal data being left unattended at a printer enabling unauthorised persons to read that information
- not securing documents containing personal data (at home or work) when left unattended
- anything that enables an unauthorised individual access to school buildings or computer systems
- discussing personal data with someone not entitled to it, either by phone or in person. How can you be sure they are entitled to that information?
- deliberately accessing, or attempting to access or use personal data beyond the requirements of an individual's job role e.g. for personal, commercial or political use. This action may constitute a criminal offence under the Computer Misuse Act as well as the Data Protection Act.
- opening a malicious email attachment or clicking on a link from an external or unfamiliar source, which leads to school's equipment (and subsequently its records) being subjected to a virus or malicious attack which results in unauthorised access to, loss, destruction or damage to personal data

What staff and governors should do?

Being open about the possible breach and explaining what has been lost or potentially accessed is an important element of working with the ICO and to mitigate the impact. Covering up a breach is never acceptable and may be a criminal, civil or disciplinary matter.

Report the breach to the data controller, Data Protection Compliance Manager and DPO as soon as possible, this is essential.

How is the breach managed?

The breach notification form will be completed and the breach registered on the Go-GDPR portal.

Advice will be sought from the Data Protection Officer as required. A plan to effectively manage the breach, who to inform and how to proceed will be put in place.

If the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach notification to those people will be done in a co-ordinated manner with support from the DPO.

Actions and changes to procedures, additional training or other measures may be required to be implemented and reviewed.

The breach report will be within 72 hours of becoming aware of the breach to the Information Commissioner if it is serious.

It may not be possible to investigate the breach fully within the 72-hour timeframe. Information about further investigations will be shared with the ICO with support from the DPO.

What happens to the people whose data has been breached?

For every breach the school will consider notification to the data subject or subjects as part of the process. If the breach is likely to be high risk they will be notified as soon as possible and kept informed of actions and outcomes.

The breach and process will be described in clear and plain language.

If the breach affects a high volume of data subjects and personal data records, the most effective form of notification will be used.

Advice may be taken from the ICO about how to manage communication with data subjects if appropriate.

Evidence Collection

It may be necessary to collect information about how an information security breach or unauthorised release of data occurred. This evidence gathering process may be used as an internal process (which can include disciplinary proceedings), it may be a source of information for the ICO, it could also be used within criminal or civil proceedings.

This process will be conducted by a suitable member of school staff, which may be the Data Management Compliance Officer or Data Protection Officer but will be determined depending on the nature of the breach.

Guidance may be required from external legal providers and police may be involved to determine the best way to secure evidence.

A record of what evidence has been gathered, stored and secured must be available as a separate log. Files and hardware must be securely stored, possibly in a designated offsite facility.

What happens next?

The impact of a serious breach will need to be assessed. It may be necessary to change some processes and procedures.

Additional training may be required. IT protocols may need to be reviewed.

The school will work with the Data Protection Officer to ensure that any changes are made to protect and secure information and to learn from any breaches.