Stanley St Andrew's Church of England Primary School

Data Protection Breach & Non-Compliance Procedure

At Stanley St Andrew's Church of England Primary School, we recognise the uniqueness of each person, young and old, all people are special and of worth in God's eyes.

All staff, governors and trustees must be aware of what to do in the event of a Data Protection Act (DPA)/UK General Data Protection Regulations (GDPR) breach. The 'Data Breach Flowchart' on page 4 outlines the process. The 'Data Breach Form' must be completed and updated as the process progresses.

Most breaches, aside from cybercriminal 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.

Examples of breaches are:

- Information being posted to an incorrect address which results in an unintended recipient reading that information.
- Loss of mobile or portable data device, unencrypted mobile phone, USB memory stick or similar.
- Sending an email with 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 to do?

Being open about the possible breach and explaining what has been lost or potentially accessed is an important element of working with the Information Commissioner's Office (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 Co-ordinator and Data Protection Officer (DPO) as soon as possible, this is essential.

The breach notification form will be completed, and the breach register updated.

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.

The breach report must be made within 72 hours of becoming aware of the breach however 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.

Procedure – Breach notification data controller to data subject

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 and discussed with the Data Controller with support from the Data Protection Co-ordinator and DPO.

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

A post breach action plan will be put into place and reviewed.

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 Co-ordinator 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, and the suggested format below can be used. Files and hardware must be securely stored, possibly in a designated offsite facility.

Date	Evidence Description	Secure storage location & confirmed date	School Officer

Review

This procedure was reviewed by the Data Protection Co-ordinator July 2022 and approved for use by the governing body at their meeting on 18 July 2022.

This procedure will be reviewed every three years in accordance with our schools' policy delegation schedule. All stakeholders will be notified of any changes to this procedure.

We will review this policy earlier than the scheduled review date should there be any change in guidance or legislation related to this policy or should we feel that an earlier review is necessary.

Breach Management Flowchart