Data Protection Breach & Non Compliance Procedure

All staff (including visitors, volunteers and contractors) and governors must be aware of what to do in the event of a Data Protection Act/GDPR breach. The Data Breach Management Flowchart (see Appendix 1) outlines the process.

The Data Breach Form must be completed and updated as the process progresses.

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. Examples of breaches are:

- Information being posted to an incorrect address with results in an unintended recipient reading that information.
- Loss of mobile or portable data devices, such as an 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 and honest 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 as soon as possible to the Data Protection Compliance Manager (Headteacher) 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 risk the rights and the 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. 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. The Chair of Governors will also be informed at this stage.

Investigation

In most cases, the next stage is for the Data Protection Compliance Manager or the DPO to fully investigate the breach. The Data Protection Compliance Manager or the DPO should ascertain whose data was involved in the breach, the potential effect on the Data Subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data
- Its sensitivity
- What protection was in place (e.g. encryption)
- What has happened to the data
- Whether the data could be put to any illegal or inappropriate use
- How many people are affected
- What type of people have been affected (pupils, staff members, suppliers, etc.) and whether there are wider consequences to the breach.

A clear record should be made of the breach in the school's log.

Procedure – Breach Notification: Data Controller (Governing Board) 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 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 Compliance Manager and the Data Protection Officer.

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.

The Data Protection Compliance Manager, with support from the DPO if necessary, will review both the causes of the breach and the effectiveness of the response to it. This should be reported to the governing board for further discussion. Action plans should be made to address any identified systematic problems or if risk assessments indicate possible recurrence of the breach. If the breach warrants a disciplinary investigation, the Data Protection Compliance Manager will liaise with HR support for advice and guidance.

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 or it could also be used within criminal or civil proceedings.

This process will be conducted by the Data Protection Compliance Manager or the DPO; this 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 the evidence that 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.

Date	Evidence Description	Secure storage location & confirmed date	School Officer

Appendix 1

Data Breach Management Flowchart