Personal Data Breach Handling Procedure

2024-25

Approved by:	SELT
Date:	September 2024
Version:	1.1
Review Date:	September 2025

Table of Contents

Introduction

This document outlines our school's procedure for handling a personal data breach, in compliance with our obligations under The General Data Protection Regulation 2016 (the UK GDPR) and the Data Protection Act 2018. It supports our Data Protection Policy and Data Protection Training which should be read alongside this.

This procedure must be followed by our employees, temporary staff and contractors who handle the school's data.

Queries about this procedure should be addressed to the school's Data Protection Officer Email: dpo@firebirdltd.co.uk

Personal data

Personal data is broadly defined as any information which relates to an identified or identifiable living individual.

An individual could be identifiable in a number of ways, for example by a name, an identification number, location data, an online identifier or any factors relating to their physical, physiological, genetic, mental, economic, cultural or social identity.

Information is not personal data if it is anonymised data, which means the person cannot be identified from the data or other data in combination with that data. A generic work email address such as admin@school.sch.uk is also not considered to be personal data.

Personal data breach

A personal data breach is 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'

Breaches are categorised into three types:

1. **Confidentiality breaches** - *unauthorised or accidental disclosure or access to personal data*

2. **Integrity breaches** - *unauthorised or accidental alteration of personal data*

3. **Availability breaches** -*accidental or unauthorised loss of access or destruction of personal data*

Examples of personal data breaches

Here are some examples of personal data breaches (this is not exhaustive):

- Revealing personal email addresses to multiple recipients by not using the 'Bcc' field (eg parent email addresses)
- Emailing or posting sensitive or confidential information to the wrong recipient
- Not disposing of confidential or sensitive paperwork securely
- Loss or theft of media or equipment which has personal data stored on it eg a laptop, iPad, mobile phone or USB stick
- Altering, sharing or destroying personal data records without permission
- Using another person's login credentials to gain higher level access
- Sharing of login details or insufficient access controls to systems which result in unauthorised viewing, use, modification or sharing of personal data
- Hacking into a system containing personal data
- A social engineering incident whereby a person uses deception to manipulate individuals into divulging confidential or personal information eg a phishing email
- A service attack or ransomware attack resulting in loss of access to personal data
- Important personal data records are corrupted and cannot be restored from back ups
- Environmental incidents such as a fire or flood resulting in damage or destruction of personal data
- *An employee abusing their access privileges to look at someone else's file out of personal curiosity or gain

*Unauthorised access, use, sharing or procuring of data, may constitute a criminal offence under the Data Protection Act 2018 and/or the Computer Misuse Act 1990.

Reporting and recording breaches

If a personal data breach is suspected or has occurred, this must be reported immediately to the school's Headteacher (and / or the school's Data Protection Link Officer), who will notify the Data Protection Officer and the Plymouth CAST Chief Operating Officer immediately.

It is vital that all personal data breaches or suspected breaches are reported immediately upon identification, so swift action can be taken to address the incident and mitigate or limit the impact it may have on the people who are affected.

If an employee deliberately fails to report (or covers up) a breach, this could result in disciplinary action.

All personal data breaches (and 'near misses') shall be logged by the Chief Operating Officer on the Trust's Personal Data Breach Log.

Investigating the breach

Personal data breaches shall be investigated by the Headteacher (or other delegated role) within **24hrs** of the school becoming aware of the incident.

The Headteacher shall identify the following information:

- Date and time of the incident
- Date and time when the school became aware of the incident
- How the school discovered the incident
- How the incident occurred
- What personal data has been revealed or put at risk
- Who the data subjects are and how many are affected
- Whether the incident raises any safeguarding (or other) concerns
- Whether the incident is likely to cause a risk to an individual (eg damage, discrimination, detriment or distress)
- The actions taken to address the breach and prevent future occurrences
- Whether the employee who caused the breach (where relevant) had completed their data protection training.

This information shall be recorded on the Trust's Personal Data Breach Incident Report, where the following applies:

- Confidential or sensitive information has been sent to a member of the public
- The incident is likely to cause damage, discrimination, detriment or distress to anyone
- The incident is the subject of a complaint or media interest
- The incident has been reported to the Information Commissioner's Office
- The incident forms part of a disciplinary investigation
- It would be useful to record the incident using this form

This report shall be sent to the Data Protection Officer at dpo@firebirdltd.co.uk within **48hrs** of the school becoming aware of the incident, so the Data Protection Officer can assess whether the incident is required to be notified to the Information Commissioner's Office and to support the containment of the breach.

A Personal Data Breach Incident Report **does not** have to be completed where any of the following applies:

- The incident does not involve personal data
- An individual cannot be identified from the data
- Only low sensitive personal data was involved eg an email address or name only
- A personal data breach did not occur

The Data Protection Officer and Plymouth CAST Chief Operating Officer shall be informed of all personal data breaches and near misses (even if a report is not required to be completed) and all incidents shall be recorded on the Trust's Personal Data Breach Log.

Notifying the Information Commissioner's Office

The school has a legal duty to notify the Information Commissioner's Office (ICO) of serious personal data breaches, within **72hrs** of becoming aware of the incident. The Data Protection Officer shall determine whether the incident is required to be notified to the

Information Commissioner's Office during the early stages of the investigation and where required, shall report the breach within 72hrs using the ICO's online reporting form.

Notifying data subjects

The school has a legal duty to notify data subjects (ie the people whose personal data has been put at risk) of a breach, if the incident is likely to result in 'high risks' to data subjects, for example if it could lead to identity theft, psychological distress, humiliation, reputational damage or physical harm. In such cases, data subjects must be informed promptly and without undue delay.

The Data Protection Officer shall determine whether the breach is required to be notified to data subjects. If a data subject (or their parent where relevant) is to be informed, the communication shall be sent by the Headteacher (or other delegated role).

When informing a data subject of a personal data breach involving their personal data, the data subject shall be informed of the:

- nature of the incident
- likely consequences of the breach (unless this is obvious)
- actions taken so far to mitigate possible adverse effects
- name and contact details of the Data Protection Officer

Notifying the governing body

The Headteacher (or nominated role) shall notify the Chief Operating Officer of all personal data breaches without undue delay and keep them informed of the outcome following investigation. The Data Protection Officer shall include reference to the personal data breaches, within the Trust's Data Protection Compliance Reports.

Contacting unintended recipients

In the event where personal data has been sent to unintended recipients in error, the Headteacher (or other nominated individual) shall contact them to contain the incident.
The person who may have caused the breach shall not contact them directly, without approval from the Headteacher.

Learning from breaches

It is important the Trust learns from personal data breaches so it can prevent these from happening again. The Trust shall ensure that following every incident it will:

- Analyse what went wrong and the route cause
- Review how the incident was handled
- Improve the security measures in place (where required)
- Update or create new data handling guidance (where required)
- Decide whether additional staff training should be rolled out
- Ensure data security is regularly discussed and reviewed across the school

The Trust's employees and governors are required to support and contribute to this process, to help the Trust and its schools build and maintain secure data handling practices.

Resources

The Trust has template letters to assist in the containment of personal data breaches and when notifying recipients and data subjects. These are available on the Trust portal and shall be used accordingly.