Personal Data Security Breach Handling Procedure

2022-23

Approved by:	Plymouth CAST Board
Date:	July 2022
Version: 1.0	Version 1.1
Review Date:	July 2023

This document outlines our Trust's procedure for handling a personal data security 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 Trust's data.

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

Table of Contents

Personal data	3
Personal data security breach	3
Examples of personal data security breaches	4
Reporting and recording breaches	4
Investigating the breach	5
Notifying the Information Commissioner's Office	5
Notifying data subjects	5
Notifying the governing body	6
Learning from breaches	6

Personal data

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

Examples of data not considered to be personal data include:

- anonymised data
- an email address such as info@company.com

Personal data security breach

A personal data security 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 security breaches

Personal data breaches include (but are not limited to):

- Revealing personal email addresses to multiple recipients by not using the 'Bcc' field (e.g. 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 ego 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
- Someone 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 e.g. 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

*Individuals who handle the Trust's data should be aware that 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 security breach is suspected or has occurred, this must be reported immediately to the school's Headteacher (and / or the Trust's Data Protection Link Officer), who will notify the Data Protection 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 Data Protection Link Officer on the Trust's Personal Data Security Breach Log.

Investigating the breach

Personal data breaches will be investigated promptly by the Headteacher (or other delegated role), with the support and direction from the Data Protection Officer. The person carrying out the investigation will establish the following facts:

- Date of the incident
- Date the Trust became aware of the incident
- Exactly what personal data has been put at risk
- How many data subjects may be affected
- How the incident occurred
- What actions have been taken to address the incident

This information shall be relayed to the Data Protection Officer by email to dpo@firebirdltd.co.uk without undue delay.

If a 'serious breach' has occurred a Personal Data Security Breach Investigation Form shall be completed and sent to the Data Protection Officer for review and comment, without undue delay.

A serious breach is where the incident is likely to result in a *risk* to someone, for example if they could suffer damage, discrimination, disadvantage, or distress as a result of the breach.

Notifying the Information Commissioner's Office

The Trust has a legal duty to notify the Information Commissioner's Office (ICO) of serious personal data security 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 Trust has a legal duty to notify data subjects (i.e. 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 is to be informed, the communication shall be sent by the Headteacher (or another delegated role).

When informing a data subject of a personal data security 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 Board of Trustees (or other nominated person) of all serious personal data breaches without undue delay and keep them informed of the outcome following investigation. The Data Protection Officer shall include a list of all personal data security breaches within the GDPR compliance reports, which have occurred during that relevant period.

Learning from breaches

It is important the Trust learns from personal data security 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 Trust

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