Personal Data Breach and
Cyber Security Incident Handling Procedure 2025-2026

Approved by:	SELT
Date:	22.09.25
Version:	1.2
Review Date:	September 2026

Contents

1 Introduction

This procedure outlines how the school handles personal data breaches and cyber security incidents in compliance with the UK General Data Protection Regulation (the UK GDPR), the Data Protection Act 2018, and guidance from the Information Commissioner's Office (ICO) and the National Cyber Security Centre (NCSC).

This procedure applies to all staff, agency staff, governors, contractors, and service providers who process or have access to the school's data or IT systems.

2 Personal data breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

Breaches are broadly categorised into three types:

- **Confidentiality breaches** - unauthorised or accidental disclosure or access to personal data
- **Integrity breaches** - unauthorised or accidental alteration of personal data
- **Availability breaches** -accidental or unauthorised loss of access or destruction of personal data

Example personal data breach scenarios

Email disclosure
An employee circulates a group email to parents but fails to use the *Bcc* field, thereby disclosing all recipients' personal email addresses to one another.

Incorrect recipient
Sensitive personal information is emailed to the wrong individual due to incorrect or out of data information on the school's systems.

Use of unapproved AI tools
A teacher copies and pastes pupil assessment data, including names, grades and learning difficulties into a free online AI tool to generate differentiated lesson materials. The AI tool is not approved by the school and stores the information on external servers outside the UK and EEA. As a result, confidential pupil data is shared without appropriate safeguards.

Insecure disposal
Confidential paperwork containing personal data is placed in general waste or recycling instead of a secure disposal facility.

Loss of equipment
A laptop, mobile device, or USB stick containing unencrypted personal data is lost or stolen.

Unauthorised amendment or deletion
A staff member alters, shares, or deletes records containing personal data without the proper authority, resulting in a breach of the data subject's rights.

Improper use of credentials
An employee uses another colleague's login credentials to obtain access to restricted information.

Weak access controls
System passwords are shared informally within a team, resulting in unauthorised access to personal data by an individual outside the team.

Cyber intrusion
A malicious actor gains unauthorised access to a system holding personal data, for example through hacking.

Social engineering
A phishing email deceives an employee into providing their system login details, which are then used to access personal data unlawfully.

Ransomware or service disruption
A cyberattack results in systems containing personal data being locked or inaccessible, impeding normal school operations.

Corruption of records
Personal data records become corrupted, and backup files are either unavailable or not recoverable, resulting in a risk to the data subjects' safety or rights.

Environmental damage
A fire, flood, or similar incident damages or destroys physical or electronic records containing personal data.

Misuse of access privileges
*An employee with system access deliberately views the records of a colleague or parent out of personal curiosity or for personal gain, without any legitimate work-related reason.

***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.*

3 Cyber security incidents

A cyber security incident is any event that threatens the confidentiality, integrity, or availability of the school's IT systems, networks, or data. These incidents can arise from malicious external activity, insider threats, technical vulnerabilities, or human error. They may also directly cause or contribute to a personal data breach, where personal data is at risk.

Example cyber security incident scenarios

Malware, ransomware or phishing attacks
A staff member receives what looks like an email from the Headteacher asking them to click a link to a "secure document." When they open it, the link installs malicious software that locks their files and demands payment to release them.

Hacking or unauthorised access
An external attacker guesses a weak password and gains entry to the school's cloud platform, accessing staff email accounts and potentially confidential pupil records.

Denial-of-service attacks
During GCSE results week, the school's website is suddenly flooded with traffic from an external source, making it impossible for parents and pupils to log in to see exam information.

Exploitation of vulnerabilities
A server running outdated software is targeted by attackers who exploit a known flaw. This allows them to bypass the firewall and access the school's internal network.

Unauthorised use of school accounts
A brute-force attack is carried out on a teacher's account, repeatedly guessing passwords until access is gained. The attacker then uses the account to send out phishing emails to parents.

Data corruption or destruction
Malicious software infects the school's finance system, corrupting pupil payment records and making it impossible to reconcile who has paid for trips or lunches.

Insider threats
A staff member who has special access to the school computer system, secretly sets up an extra login that only they know about. They then use this hidden login to copy confidential employee files and email them to their own personal cloud account (like Dropbox or Google Drive) for non work-related purposes.

4 Reporting and recording

Staff responsibility

All staff have a duty to act quickly. If you suspect or become aware of a personal data breach or cyber security incident, you must report it straight away to the Headteacher and/or the School's Data Protection Link Officer (DPLO) and the Plymouth CAST Chief Operating Officer immediately. Do not attempt to investigate or fix the issue yourself.

Informing the Data Protection Officer

The Headteacher/DPLO will immediately alert Plymouth CAST's Data Protection Officer (DPO) and the Chief Operating Officer of all incidents involving personal data. The DPO will assess the situation, advise on the next steps, and ensure compliance with the UK GDPR reporting obligations.

Involvement of IT Manager

If the incident involves any aspect of the school/Trust's IT systems (e.g. emails, MIS platform, Wi-Fi, laptops, cloud services), Plymouth CAST's IT Manager must be informed so they can:

- Secure and contain affected systems
- Prevent further unauthorised access or data loss
- Preserve evidence for investigation
- Support recovery (e.g. restoring backups, resetting accounts)

Recording incidents

All incidents, whether confirmed, suspected, or even a "near miss" (such as posting confidential data to the wrong address, but the envelope is returned unopened), must be reported to the Trust's Chief Operating Officer and recorded in the Trust's Security Incident Log and onward reported to Plymouth CAST's DPO.

5 Investigating personal data breaches and cyber security incidents

Personal data breaches

When a personal data breach is suspected or confirmed, the school/Trust will undertake a formal investigation within 24 hours of becoming aware of the incident. The investigation will be led by the Headteacher (or delegated role), with support from the Chief Operating Officer, Plymouth CAST's DPO and other relevant staff.

Information to be identified

The investigation shall establish the following:

- Date and time of the incident.
- Date and time when the school/Trust became aware of the incident.
- How the school/Trust discovered the incident.
- How the incident occurred.
- What personal data has been revealed, compromised, or put at risk.
- Who the data subjects are and how many individuals are affected.
- Whether the incident raises any safeguarding or other concerns.
- Whether the incident is likely to cause risk or harm to individuals (e.g. damage, discrimination, detriment, distress).
- The actions taken to contain the breach and prevent recurrence.
- Whether the staff member involved (if relevant) had completed their data protection training.

Personal data breach report

A Personal Data Breach Report shall be completed where any of 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.
- The incident is subject to a complaint or has attracted media interest.
- The incident has been reported to the Information Commissioner's Office (ICO).
- The incident forms part of a disciplinary investigation.
- It would be useful to formally record the event for future learning.

This report must be sent to the Data Protection Officer (dpo@firebirdltd.co.uk) within 48 hours of the school/Trust becoming aware of the incident. The DPO will determine whether notification to the Information Commissioner's Office is required and will support efforts to contain the breach.

When an incident report is not required

Completion of a Personal Data Breach Report is not required if:

- The event does not involve personal data.
- An individual cannot be identified from the data.
- Only low-sensitivity personal data is involved (e.g. name or email address only).
- A personal data breach has not occurred.

Action:

Even if a Personal Data Breach Report form does not need to be completed, the Data Protection Officer must still be informed. All incidents, including 'near misses', must be recorded in the Trust's Security Incident Log.

Notification Requirements

Information Commissioner

The school/Trust has a legal duty to notify the Information Commissioner's Office (ICO) of serious personal data breaches within 72 hours of becoming aware. The DPO will determine whether an incident meets the threshold which requires notification to the ICO and will make the necessary submission, after consultation and agreement with the Trust's Chief Operating Officer or other member of the Trust's Senior Executive Leadership Team.

Data Subjects

Where the breach is likely to result in a 'high risk' to the rights and freedoms of individuals (e.g. identity theft, psychological harm, reputational damage, or physical harm), affected data subjects (or their parents) shall be informed promptly and without undue delay. Notifications shall be sent by the Headteacher (or delegate)/ Chief Operating Officer (or delegate), (under advice from Plymouth CAST's Data Protection Officer), and will include the following information:

- The nature of the incident.
- The likely consequences of the breach.
- Actions taken to mitigate adverse effects.
- The name and contact details of the Data Protection Officer.

Governing Body

The Headteacher (or delegate) shall notify the Chair of the Local CAST Board without undue delay of all serious or 'high risk' personal data breaches in respect of the school. The Chief Operating Officer (or delegate) shall notify the Chair of the Trust's Audit & Risk Committee without undue delay of all serious or 'high risk' personal data breaches in respect of the Trust. Breaches shall also be reported in the Trust's Data Protection Compliance Reports, prepared by the Data Protection Officer.

Unintended Recipients

If personal data has been sent in error, the Headteacher (or delegate))/ Chief Operating Officer (or delegate) shall contact the unintended recipient(s) to secure the data and contain the breach.

Action:

The individual who caused the breach must not contact recipients directly without Headteacher (or delegate)/Chief Operating Officer (or delegate) approval.

Cyber security incidents

In the event of a cyber security incident, the school/Trust shall act quickly to contain the threat, minimise disruption, and protect the school/Trust's data and assets.

The following steps shall be followed:

Immediate Containment

IT Manager (or external IT support provider) shall:

- Disconnect or disable affected devices, systems, or accounts to prevent the incident spreading.
- Change passwords and revoke access rights where compromise is suspected.
- If email is compromised, suspend the account and block suspicious activity.

Non-IT staff shall:

- Stop using the affected devices or accounts immediately.
- Report any unusual messages, system errors, or suspicious files without delay.
- Seek further advice from IT about next steps.

Preserve Evidence

IT Manager (or external IT support provider) shall:

- Keep system logs, error reports, alerts, suspicious files, or emails intact for investigation.
- Not delete, edit, or overwrite potential evidence.
- Make secure copies of relevant logs or forensic data before initiating recovery actions.
- Take screenshots to document suspicious messages, pop-ups, or ransom notes.

Technical Recovery

IT Manager (or external IT support provider) shall:

- Scan systems for malware and remove malicious software.
- Restore data from secure, verified backups.
- Patch vulnerabilities by updating software, firmware and security settings.
- Reset passwords and enforce multi-factor authentication (MFA) where available.
- Monitor systems closely for signs of continued or repeat activity.

Escalation and Reporting

IT Manager (or external IT support provider) shall:

- Keep the Headteacher, Data Protection Link Officer (DPLO), Plymouth CAST's Chief Operating Officer and Plymouth CAST's Data Protection Officer informed of their cyber investigation progress and outcome.
- Report large-scale or criminal attacks to the National Cyber Security Centre (NCSC).
- Report suspected fraud, ransomware, or hacking to Action Fraud (the UK's national cybercrime reporting centre).
- Notify the Police if there is an immediate safeguarding or criminal risk or activity.
- Support the school/Trust by informing third-party providers or partners (or drafting the notification) if the incident relates to, or may compromise, their systems or services.

Communication and Containment with Stakeholders

Headteacher/Chief Operating Officer shall:

- Inform employees, parents and students if they are directly affected by a cyber incident (e.g. phishing emails sent from a school/Trust account). Individuals should be informed promptly and advised on the protective measures they can take, such as password resets.
- Keep Governors/Directors updated if the incident is serious or disruptive.
- Develop a communication plan (following advice and support from relevant professionals) if serious reputational or operational impacts are likely, before contacting parents, students, media, or external agencies.

6 Post incident review

Following containment and recovery of a personal data breach or cyber security incident, the school/Trust shall conduct a review to ensure that lessons are learned and improvements are embedded to minimise the risk of recurrence.

The review shall focus on:

- Establishing what happened and why, identifying the sequence of events and the root cause of the incident.
- Identifying weaknesses in systems, processes, or behaviours that may have contributed.
- Ensuring accountability and accurate record keeping, to meet compliance and governance requirements.

- Strengthening the school/Trust's overall data protection and cyber security resilience.

In the case of sensitive or high-risk incidents, the review will also consider:

- **Timeliness of detection and response** – how quickly the incident was identified, reported, and contained and whether delays can be reduced in future.
- **Staff awareness and training needs** – whether staff recognised and reported the issue appropriately, and whether refresher or targeted training is required.
- **Effectiveness of communication** – whether notifications to affected individuals, the ICO, governors, and (where relevant) law enforcement or NCSC were clear, accurate and timely.
- **Supplier and third-party performance** – whether external IT providers or contractors acted appropriately, and if contracts contain sufficient security obligations.
- **Safeguarding implications** – whether the incident raised or could have raised safeguarding concerns, and how these were addressed.
- **Testing and resilience** – whether further technical measures such as penetration testing, vulnerability scanning, or backup restoration tests are required.
- **Governance oversight** – ensuring governors are updated on findings and improvements, enabling them to provide informed oversight and challenge.

7 Resources and further information

The school/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 Plymouth CAST Portal.

Further information about preventing and managing personal data breaches and cyber security incidents is available at:

- Information Commissioner's Office: Personal Data Breach Guide
- National Cyber Security Centre: Respond to cyber attacks and Cyber Security Resources for Schools
- Department for Education: Cyber security standards for schools and colleges

Appendix A: Summary of Changes

This appendix summarises the key changes made between versions 1.1 and 1.2 of the Personal Data Breach & Cyber Security Incident Handling Procedure. It should be read alongside the updated policy to provide clarity on what has been revised, expanded, or newly introduced.

Title and Scope
V1.1: Personal Data Breach Handling Procedure. V1.2: Expanded to Personal Data Breach and Cyber Security Incident Handling Procedure, explicitly covering cyber incidents.

Structure and Contents
V1.1: 10 sections focused on data breaches. V1.2: 7 streamlined sections but expanded scope to include cyber incidents, post-incident review, and resources.

Introduction
V1.1: Focus on GDPR/DPA obligations; applies to employees, temporary staff, and contractors. V1.2: References ICO and NCSC guidance; applies to staff, agency staff, governors, contractors, and service providers.

Definitions
V1.1: Separate sections for personal data and breaches. V1.2: Focuses directly on personal data breaches, adds separate section on cyber incidents.

Examples
V1.2: Shorter list of personal data breach examples. V1.2: Expanded list including unapproved AI tools, weak access controls, corruption of records, environmental damage, and misuse of access privileges. Also introduces cyber incident scenarios (malware, DoS attacks, insider threats, vulnerabilities).

Reporting and Recording
V1.1: Breaches reported to Headteacher/DPLO → DPO and COO; logged on Personal Data Breach Log. V1.2: Broader reporting requirements; all incidents (including near misses) logged in Security Incident Log. Explicit instruction not to investigate independently; IT Manager involvement required.

Investigation
V1.1: Investigation within 24hrs by Headteacher; report to DPO within 48hrs. V1.2: Expanded investigation checklist; Personal Data Breach Report required for serious incidents; DPO must be informed of all incidents.

Notification Requirements
V1.1: DPO decides if ICO/data subjects must be notified. V1.2: ICO notification within 72hrs required for serious breaches; clearer rules for notifying data subjects, governing bodies, and unintended recipients.

Cyber Security Incident Response
V1.2 only: New section covering containment, preserving evidence, technical recovery, escalation (to NCSC, Action Fraud, Police), and communication planning.

Post-Incident Review
V1.1: Short learning section. V1.2: Expanded framework addressing timeliness, staff awareness, communication, third-party performance, safeguarding, technical testing, and governance oversight.

Resources
V1.1: Template letters on Trust portal. V1.2: Template letters plus references to ICO, NCSC, and DfE cyber standards.