Birchwood High School

your dreams, your future, our challenge

Data Breach Policy & Procedure 2026

Committee	Audit
SLT Link	Mr C Gilbank
Approval Date	March 2026
Scheduled Review Date	March 2029

Birchwood High School

your dreams, your future, our challenge

Contents

Executive Summary

Birchwood High School makes all efforts to ensure the security of its information systems and the Personal Data for which it is responsible. This policy will ensure that where incidents occur, they are managed in a way that supports compliance with the school's legal obligations and individuals' rights. All users of Birchwood High School's Information and information systems are required to familiarise themselves with and comply with this policy.

Definitions of terms:

An Information Security Breach is an incident, which has caused or has the capacity to cause unauthorised disclosure of and / or damage to Birchwood High School's Information, information systems or reputation

- Examples include:
- Accidental loss or theft of data or equipment
- Unauthorised or accidental use, access to or modification of data or information systems
- Unauthorised or accidental disclosure of data
- Compromised user accounts or attempts by criminals to gain access to or disrupt data or systems
- Equipment failure

Some of these incidents may involve Personal Data, in which case these are defined as Personal Data Breaches

- Examples include:
- Unauthorised or accidental disclosure of personal data
- Accidental or unauthorised loss or theft of personal data or equipment
- Damage, destruction, alteration or loss of personal data

Birchwood High School's utilises various information systems and holds a large amount of data / information which may include personal or confidential information (about people), and non-personal information which could be sensitive or commercial, for instance financial data. Care should be taken to protect this Information and information systems from incidents (either accidental or deliberate) that could compromise their security. In the event of a data breach or an information security incident, it is vital that appropriate actions are taken to minimise associated risks.

1. Purpose and scope

This policy sets out how Birchwood High School manages information security incidents and personal data breaches in order to protect the confidentiality, integrity and availability of information and systems.

An information security incident is any event that may compromise the confidentiality, integrity or availability of school information, data or systems. A personal data breach is a subset of information security incidents and refers specifically to incidents involving personal data, as defined by UK General Data Protection Regulation (UK GDPR).

2. Reporting an incident

All staff, governors, volunteers and contractors must report any actual or suspected information security incident immediately.

The first point of contact for all information security incidents is the IT Service Desk. Where personal data may be involved, the Data Protection Officer (DPO) must also be notified without delay.

Individuals reporting an incident must preserve evidence wherever possible. This includes not deleting emails, files or logs, and following instructions provided by IT support or the DPO.

3. Roles and responsibilities

- ### IT Service Desk

The IT Service Desk is responsible for coordinating the technical response to information security incidents and for maintaining a secure log of all information security incidents, including the date, nature of the incident, systems affected, actions taken and outcome.

- ### Data Protection Officer (DPO)

The DPO is responsible for overseeing the management of personal data breaches. The DPO will maintain a secure log of all personal data breaches, including risk assessments, decisions on notification, communications issued and remedial actions, in line with the school's retention schedule.

- ### Principal

The Principal will support the DPO and IT Service Desk in managing incidents, ensure appropriate resources are available, and participate in decision-making relating to notifications and communications.

4. Assessment and containment

Upon notification of an incident, the IT Service Desk and/or DPO will assess the nature and severity of the incident and take immediate steps to contain it. This may include isolating affected systems, changing credentials, recovering data from backups, or taking systems offline where necessary.

5. ICO reporting and external notification

Birchwood High School will notify the Information Commissioner's Office (ICO) without undue delay and, where required, not later than 72 hours after becoming aware of a personal data breach that is likely to result in a risk to the rights and freedoms of individuals.

Where a personal data breach is likely to result in a high risk to individuals, affected individuals will be informed without undue delay, in clear and plain language.

6. Communications and decision-making

Decisions relating to internal and external communications, including notifications to affected individuals, parents, regulators or third parties, will be made jointly by the DPO and the Principal, with reference to the Chair of Governors where appropriate.

7. Incident closure, review and learning

All significant information security incidents and personal data breaches will be subject to a post-incident review to identify root causes, control weaknesses and required remedial actions.

Lessons learned from incidents will inform updates to technical controls, staff training, risk assessments and related policies, including the Cyber and Data Security Policy.

8. Related policies and documents

- Cyber and Data Security Policy
- Data Protection Policy
- Online Safety Policy
- Cyber Response and Recovery Plan

9. Review

This policy will be reviewed at least every three years, or sooner where required due to legislative change, updated Department for Education guidance, or following a significant information security incident.

Members of staff discovering incidents must report an information security incident or Personal Data
breach immediately to the IT Service Desk at itsupport@birchwoodhigh.org.uk , extension 3232, als o to their Line Manager or SLT. Reports of Personal Data breaches must also
be reported to dpo@birchwoodhigh.org.uk Please use the below link to the form to provide details of the incident.

Data Breach Form - Data Breach – Fill in form