PUDSEY
GRAMMAR SCHOOL
EST. 1905

Cyber Security Policy 2026 - 2027

This policy has been agreed by the Governing Body of Pudsey Grammar School

Approved: Resources

Date approved: 18th March 2026

Date of review: March 2027

Contents

1. Introduction and aims

This policy sets out Pudsey Grammar School's approach to protecting its digital systems, data, staff, and students from cyber threats. It aims to:

- Safeguard sensitive and personal data in compliance with UK GDPR and the Data Protection Act 2018.
- Ensure all staff, students, governors, and third parties use technology responsibly and securely.
- Protect the school's IT systems and infrastructure against malware, ransomware, unauthorised access, and cyber-attacks.
- Support the welfare and safety of students in line with the Keeping Children Safe in Education (KCSIE) statutory guidance.

2. Scope

This policy applies to:

- All staff (teaching, support, temporary, and volunteers).
- All students.
- Governors and contractors with access to school systems.
- All devices (school-owned or personal) used to access the school's network or data.

3. Roles and Responsibilities

Headteacher & Governing Body

- Approve and oversee implementation of the policy.
- Ensure adequate resourcing for cyber security measures.
- Data Protection Officer (DPO)
    - Ensure compliance with data protection law.
    - Act as the point of contact for data breaches.

IT Network Manager / IT Support Provider

- Maintain secure networks, servers, and devices.
- Implement access controls, monitoring, and regular updates.
- Respond to Cyber incidents.

Staff

- Follow this policy and attend mandatory cyber security training.
- Report any suspicious activity or breaches immediately.

Students

- Use school technology responsibly in line with the Acceptable Use Policy (AUP).
- Report suspicious or inappropriate activity to staff.

4. Security Controls

4.1 Access Control

- All users must have unique usernames and strong passwords.
- Multi-Factor Authentication (MFA) must be enabled where possible (e.g. staff email).
- Staff accounts must be disabled immediately upon leaving employment.

4.2 Data Protection

- Personal data must be stored on secure, encrypted systems.
- Cloud services must meet UK GDPR standards.
- Sensitive data must not be stored on unencrypted personal devices.
- Regular backups must be performed and tested.

4.3 Device & Network Security

- All devices must run up-to-date antivirus and security patches.
- Firewalls and filtering systems must be in place to block malicious websites and harmful content.
- Students' internet access will be filtered and monitored in line with safeguarding obligations.

Any school-owned device that is lost or stolen must be reported immediately to the IT Network Manager and the Data Protection Officer. Where the device may contain personal or sensitive data, the incident will be treated as a potential data breach and handled in line with the school's data breach procedures.

4.4 Email & Phishing Protection

- Staff and students must not click on suspicious links or open unknown attachments.
- Phishing awareness training will be provided annually.

4.5 Software & Updates

- Only authorised software is to be installed.
- Automatic updates must be enabled where possible.

5. Incident Response

In the event of a suspected cyber incident:

1. Report immediately to the IT Manager and DPO.
2. Contain the incident (e.g. disconnect compromised devices).
3. Investigate and document findings.
4. Notify affected individuals and the ICO (if a data breach has occurred), in line with legal requirements.
5. Review and update security controls to prevent recurrence.

Where a personal data breach is identified, the school will assess the severity and potential risk to individuals. If the breach is likely to result in a risk to the rights and freedoms of individuals, the Data Protection Officer (DPO) will notify the Information Commissioner's Office (ICO) without undue delay and, where feasible, within 72 hours of becoming aware of the breach, in accordance with UK GDPR requirements.

Where required, affected individuals will also be informed without undue delay where the breach is likely to result in a high risk to their rights and freedoms.

6. Training and Awareness

- All staff must complete annual cyber security and data protection training.
- Students will be taught safe online behaviours as part of the curriculum.
- Regular awareness campaigns will highlight new threats and safe practices.

7. Compliance

Failure to comply with this policy may result in disciplinary action in line with the school's staff code of conduct or student behaviour policy.

8. Review

This policy will be reviewed annually, or sooner if:

- There are significant changes to UK legislation or statutory guidance.
- A major incident highlights the need for policy amendments.

Appendix 1: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber-attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.

TERM	DEFINITION
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.