



PRIORY SCHOOL
EDGBASTON

CYBER SECURITY POLICY

Trustee Committee:	Risk and Compliance	
Date Approved:	September 2026	
Next of Review:	September 2028	
Member of Staff Responsible:	Nedal Al-Chaama	
Trustee Overseer:	Risk and Compliance Committee	
Intended Audience:	Options: Employees, Volunteers, Parents, Pupils, and Visitors	
Relevance:	Whole School	Yes
	Early Years	Yes
	Preparatory	Yes
	Seniors	Yes
Access:	Website	Yes
	Internal	No
	Restricted	No

Our Mission Statement

Priory School is a thriving, co-educational independent school founded upon a rich Catholic heritage which welcomes those from all faiths and none.

In partnership with parents and guardians we provide a nurturing, family-based ethos, alongside high-standards of teaching and learning, enabling all pupils to achieve their potential.

We embrace diversity and interfaith understanding alongside awareness of environmental and global issues, in response to the needs of our time.

The Governors and staff at Priory School are committed to providing a fully accessible environment which values and includes all pupils, staff, parents and visitors, regardless of their education, physical, sensory, social, spiritual, emotional or cultural needs.

The Governors, staff, and pupils are committed to the safeguarding and welfare of pupils and staff.

To meet the needs of our school community, all our policies, including this policy, can be made available on different formats such as different font sizes or styles, colour, or alternate languages.

The Governing Council understands it has responsibility for ensuring the effective oversight of this policy and will assess, evaluate, and review as necessary.

Response to the Mission Statement

We view all Priory children as children of God and we encourage them to always give their best and treat others as they would like to be treated. We promise an ethos of showing our faith throughout our daily life. Our children deserve to learn and grow in a safe and happy environment which is free from harm and through our safeguarding policy and procedures, we aim to ensure we maintain the highest standards of care for each and every child.

Table of Contents

Aims and scope.....	4
Key principles.....	4
Legal and regulatory framework	4
Roles and responsibilities	5
Governing body / Board of Trustees.....	5
Headteacher / Accounting Officer / Senior Leadership Team.....	5
Senior digital lead / IT lead / IT support provider.....	5
Data Protection Officer (DPO)	5
Designated Safeguarding Lead (DSL)	5
All users.....	6
Cyber risk management.....	6
Asset management and secure configuration.....	6
Network security	7
User accounts, access control and passwords	7
Multi-factor authentication.....	7
Security updates and vulnerability management	8
Malware, email and web security	8
Filtering and monitoring.....	8
Data protection, encryption and removable media.....	8
Remote working and personal devices	9
Cloud services and third-party suppliers.....	9
Backups, recovery and business continuity.....	9
Cyber security awareness and training	10
Cyber incident reporting and response.....	10
External reporting and support	10
Personal data breaches and regulatory reporting	11
Monitoring, assurance and review.....	11
Related policies and useful guidance	11
Related organisational policies	11
Useful guidance.....	12

Aims and scope

[ORGANISATION NAME] is committed to protecting the confidentiality, integrity and availability of its information, systems and digital services. Effective cyber security supports safeguarding, continuity of education, financial resilience, data protection and public confidence.

This policy sets out the minimum cyber security expectations for employees, trustees or governors, volunteers, contractors, temporary staff, pupils where applicable, and any other person who is authorised to use the organisation's digital technology or information.

The policy applies to organisation-owned and managed devices, networks, cloud services, software, data, accounts and communications, together with personal devices where their use for organisational business has been authorised.

Key principles

The organisation will take a proportionate and risk-based approach to cyber security. As part of this approach, the following key principles will apply:

- Access will be limited to what each user needs to carry out their role.
- Digital technology will be securely configured, supported and kept up to date.
- Cyber risks will be identified, assessed, recorded and reviewed.
- Important data and systems will be backed up and recoverable.
- Staff will receive regular cyber security awareness training.
- Cyber incidents and suspected incidents will be reported promptly and managed through an agreed response and recovery process.
- Safeguarding, data protection and cyber security will be considered together where an incident may affect children, staff or personal data.

Legal and regulatory framework

This policy has due regard to relevant legislation, statutory guidance and sector standards, including:

- Computer Misuse Act 1990
- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations 2003, where applicable
- Keeping Children Safe in Education
- Department for Education (DfE) digital and technology standards, including the cyber security and filtering and monitoring core standards
- DfE Cyber Security Hub guidance
- National Cyber Security Centre (NCSC) guidance and Cyber Essentials controls
- Academy Trust Handbook, where applicable
- Risk Protection Arrangement (RPA) requirements, where applicable

The organisation will keep this policy under review as legislation, DfE standards, NCSC guidance and cyber threats change.

Roles and responsibilities

Governing body / Board of Trustees

- Provide oversight of cyber security and ensure proportionate controls are in place.
- Ensure cyber security is considered within organisational risk management and business continuity arrangements.
- Receive appropriate assurance on significant cyber risks, incidents and improvement actions.
- Ensure the organisation works towards the DfE digital and technology standards and, where applicable, complies with the Academy Trust Handbook and RPA requirements.

Headteacher / FD/SBM / Senior Leadership Team

- Ensure this policy is implemented and responsibilities are clearly allocated.
- Appoint a senior leadership team member with responsibility for digital technology and cyber security.
- Ensure sufficient resources, support and training are available to manage cyber risk.
- Ensure significant incidents are escalated promptly to the governing body or trust board as appropriate.

Senior digital lead / IT lead / IT support provider

- Maintain secure configurations, inventories, access controls, firewalls, anti-malware and security monitoring.
- Apply security updates and manage unsupported or vulnerable technology.
- Maintain backup, recovery and technical incident response arrangements.
- Maintain records of technical risks, exceptions and actions.
- Provide assurance that outsourced or third-party services meet the organisation's security requirements.

Data Protection Officer (DPO)

- Advise on personal data security and data protection obligations.
- Support assessment of cyber incidents involving personal data and advise on notification to the ICO and affected individuals where required.
- Provide independent advice on data protection risks arising from new systems, suppliers and processing activities.

Designated Safeguarding Lead (DSL)

- Consider safeguarding implications of cyber incidents and ensure appropriate safeguarding action is taken.
- Work with the senior digital lead and IT support on filtering and monitoring arrangements and relevant incidents.

All users

- Follow this policy and the Acceptable Use Policy.
- Protect passwords and authentication methods and never share accounts.
- Lock devices when unattended and take reasonable care of equipment.
- Be alert to phishing, social engineering and unusual requests.
- Report suspected cyber incidents, lost devices, suspicious emails and accidental disclosures immediately.
- Complete required cyber security and data protection training.

Cyber risk management

A cyber security risk assessment will be completed at least annually and reviewed at least termly, and sooner following a significant technology or process change or a cyber incident. Risks and agreed actions will be recorded through the organisation's risk management arrangements. The assessment will

- consider critical systems and data.
- consider known vulnerabilities and unsupported technology.
- consider user access and privileged accounts.
- consider third-party and cloud services.
- consider backup and recovery arrangements.
- consider network, wireless and remote access.
- consider email, phishing and social engineering.
- consider safeguarding and filtering and monitoring.
- consider physical security of digital technology.
- dependencies on key suppliers and IT support.

Where a required control cannot be implemented, the exception will be documented, risk assessed, approved by an appropriate senior leader and reviewed regularly.

Asset management and secure configuration

An up-to-date inventory of hardware, software, cloud services and other significant digital assets will be maintained. Organisation-managed devices will be securely configured using centrally managed settings where practicable, with unnecessary software, services, ports and features removed or disabled. Default passwords and unnecessary default accounts will be changed or disabled before systems are placed into service.

Devices holding organisational data will use appropriate encryption and automatic screen locking. Administrative privileges will be restricted, with separate administrative accounts used for privileged tasks. Unsupported or end-of-life technology will be replaced, isolated or otherwise risk-managed, with exceptions recorded and reviewed.

Network security

The organisation will protect its networks using correctly configured firewalls and other appropriate security controls. Inbound connections will be blocked by default unless there is a documented business need, and firewall or network administration interfaces will be protected from unauthorised access and secured with multi-factor authentication (MFA) where available.

Network devices, firewall rules and significant configuration changes will be documented and reviewed. Guest and unmanaged devices will be separated from networks containing sensitive organisational systems and data. Remote access will use approved secure methods and individual user accounts, and network logs and alerts will be reviewed proportionately to identify suspicious activity.

User accounts, access control and passwords

Each user will have an individual account and access will be based on their role and the principle of least privilege. Shared accounts will be avoided unless technically necessary and formally controlled. Joiner, mover and leaver procedures will ensure that access is created, amended and removed promptly, and privileged accounts will not be used for routine email, web browsing or day-to-day work.

Passwords must be unique to the user, protected from unauthorised access and supported by technical controls that reduce the risk of compromise. The organisation will follow current DfE and National Cyber Security Centre (NCSC) guidance. Where users create their own passwords, the NCSC recommends a long, memorable approach such as combining three random words. Passwords should not be based on easily guessed personal information and should not be reused across personal and organisational services.

Where appropriate, the organisation will provide or approve the use of a password manager. Password managers can generate and securely store strong, unique passwords, reducing the need for users to remember multiple passwords. Users must protect the primary password for any password manager and must not store organisational passwords in an unapproved service.

Passwords will be changed immediately where they are known or suspected to have been compromised. Routine forced password changes will not normally be required unless a particular system, risk assessment or other security requirement makes this necessary. Common or compromised passwords will be blocked where the technology supports this.

Multi-factor authentication

Multi-factor authentication (MFA) provides an additional layer of protection by requiring more than one method of verifying a user's identity. In line with the DfE cyber security core standard, MFA must be enabled for staff accounts that access cloud services or remotely access on-site systems, and for IT administrative accounts. MFA should also be used more widely where systems support it, particularly for accounts that provide access to confidential, personal or sensitive information.

Where MFA is not available, the risk will be assessed and stronger alternative controls applied. Significant exceptions will be recorded and reviewed. Passkeys or other secure authentication methods may also be considered where supported and appropriate.

Security updates and vulnerability management

Operating systems, applications, firmware and security products will be supported and kept up to date. Security updates and vulnerability fixes will be applied within timescales appropriate to their severity and in line with the DfE cyber security standards. Automatic updating and centrally managed patching will be used where appropriate.

The organisation will maintain oversight of end-of-life dates and plan replacement before support expires. High-risk devices or systems that cannot be updated will be isolated from higher-risk systems and data, removed from the network, replaced or subject to a documented risk assessment and compensating controls.

Malware, email and web security

Appropriate anti-malware or endpoint protection will be enabled and kept up to date on supported devices. Email and web security controls will be configured to reduce the risk from phishing, spoofing, malicious attachments, impersonation and known malicious websites.

Users must not disable security software, bypass security controls or install unauthorised software or browser extensions. Autorun functionality and removable media will be restricted where appropriate, and suspicious emails, links, attachments or unexpected requests must be reported promptly.

Filtering and monitoring

The organisation will maintain appropriate filtering and monitoring systems in accordance with Keeping Children Safe in Education and the DfE filtering and monitoring standards. These arrangements form part of safeguarding as well as cyber security.

- Roles and responsibilities for filtering and monitoring will be clearly defined.
- Filtering will block harmful, illegal and malicious content without unreasonably affecting teaching and learning.
- Monitoring alerts will be reviewed by appropriately authorised staff and escalated where safeguarding or cyber security concerns arise.
- The effectiveness of filtering and monitoring arrangements will be reviewed regularly and following significant changes.
- Attempts to bypass filtering, including unauthorised VPNs or proxy services, will be addressed in accordance with the organisation's policies.

Data protection, encryption and removable media

Personal and confidential data will only be accessible to authorised users and will be stored in approved locations. Appropriate encryption will be used for portable devices and removable media where they hold organisational or personal data. Personal data must not be transferred to personal email accounts or unauthorised storage services.

Removable media will be restricted to approved business use and subject to appropriate security controls. Loss or theft of a device or storage medium containing organisational data must be reported immediately. Where a cyber incident affects personal data, the organisation's Data Breach Policy will also apply.

Remote working and personal devices

Only approved devices, systems and methods will be used to access organisational data remotely. Users must prevent family members or other unauthorised people from accessing organisation-owned devices, lock devices when unattended and take reasonable precautions to protect them from loss or theft. Public or untrusted Wi-Fi should be avoided for sensitive work unless an approved secure method is used.

Personal devices may only be used for organisational business where expressly authorised and subject to appropriate security controls. Organisational data must not be permanently stored on personal devices unless specifically authorised and appropriately protected.

Cloud services and third-party suppliers

Cloud services and third-party systems must be subject to proportionate due diligence before use. Security, data protection, resilience, backup and incident-management arrangements will be considered as part of procurement and contract management. Due diligence will consider

- the supplier's security certifications and independent assurance where relevant.
- MFA, access management and administrative controls.
- encryption in transit and at rest.
- backup, restoration and data portability arrangements.
- data location, sub-processors and data protection terms.
- security incident and breach notification obligations.
- business continuity, disaster recovery and service availability.
- support arrangements, vulnerability management and end-of-life planning.
- secure return or deletion of data when the contract ends.

Contracts and service level agreements will clearly allocate security responsibilities between the organisation and the supplier. Material supplier risks will be recorded and reviewed.

Backups, recovery and business continuity

The organisation will maintain a documented backup and recovery plan covering critical systems and data. Backup arrangements will be designed so that a cyber incident affecting the live environment does not automatically compromise every recoverable copy.

- Critical data and systems will be identified and appropriate recovery priorities agreed.
- Backups will be taken at a frequency appropriate to the organisation's recovery needs.
- At least one backup copy will be protected from routine user access and from alteration or deletion by a compromised account, wherever practicable.
- Backup administration will use secure, restricted accounts and MFA where supported.
- Restoration will be tested regularly and evidence of testing retained.
- Recovery procedures, dependencies and supplier contacts will be documented.

- Business continuity and disaster recovery plans will include cyber scenarios such as ransomware, loss of cloud services, loss of internet connectivity and compromise of key accounts.
- The backup and recovery plan will be reviewed at least annually and following significant changes or incidents.

Cyber security awareness and training

Cyber security is a shared responsibility. Staff will receive cyber security awareness training on induction and refresher training at least annually, with additional training where risk or role requires it. Training will include:

- phishing and social engineering.
- passwords and MFA.
- email and payment fraud.
- safe use of devices and remote working.
- removable media.
- reporting cyber incidents and personal data breaches.
- safeguarding implications of online threats.

Where the organisation participates in the Risk Protection Arrangement, it will retain evidence that relevant users have completed the required NCSC cyber security training annually.

At least one governor or trustee should receive appropriate cyber security training, and governance awareness will be refreshed as standards and risks change.

Cyber incident reporting and response

All actual or suspected cyber incidents must be reported immediately through the organisation's agreed reporting route. Users should not investigate an incident themselves or take action that could destroy evidence unless required to prevent immediate harm.

REPORT CYBER INCIDENTS TO: IT Lead or Mr Nedal Al-Chamaa if the IT lead is not available

The organisation will maintain a Cyber Response and Recovery Plan. Depending on the incident, immediate actions may include isolating affected devices, disabling compromised accounts, changing credentials, preserving logs and evidence, contacting IT support, activating business continuity arrangements and notifying relevant senior leaders.

External reporting and support

The incident lead will consider whether notification or support is required from relevant external bodies, including the DfE, Report Fraud, NCSC, police, insurers or the RPA, local authority and other regulators or partners as appropriate.

Academy trusts must not pay ransom or extortion demands, including cyber ransomware demands. Other education settings should also follow NCSC and law-enforcement advice and must not make payments without appropriate legal, insurance and governance advice.

Following an incident, the organisation will review root causes, lessons learned, security controls, training needs and recovery arrangements. Actions will be recorded and monitored to completion.

Personal data breaches and regulatory reporting

A cyber incident may also be a personal data breach. Where personal data is affected, the incident must be referred promptly to the DPO and managed in accordance with the Data Breach Policy.

The DPO will advise whether the breach is reportable to the Information Commissioner's Office and whether affected individuals need to be informed. Where notification to the ICO is required, it must be made without undue delay and, where feasible, within 72 hours of becoming aware of the personal data breach.

Monitoring, assurance and review

This policy will be reviewed at least annually and sooner where there is a significant cyber incident, a material change in technology, or a relevant change in legislation or guidance. Compliance will be monitored through risk assessment, technical assurance, internal scrutiny or audit, incident review, supplier assurance and governance oversight as appropriate.

Cyber security risks and significant control weaknesses will be reported through the organisation's risk management arrangements. The organisation will also keep its progress against the DfE digital and technology standards under review and ensure agreed improvement actions are monitored to completion.

Related policies and useful guidance

Related organisational policies

- Acceptable Use Policy
- Data Protection Policy
- Data Breach Policy
- Online Safety Policy
- Filtering and Monitoring Policy / arrangements
- Business Continuity and Disaster Recovery Plan
- Cyber Response and Recovery Plan
- Records Management and Retention Policy
- Staff Code of Conduct
- Remote Working / Bring Your Own Device Policy, where applicable
- Risk Management Policy

Useful guidance

- DfE – Meeting digital and technology standards in schools and colleges: <https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges>
- DfE – Cyber security: core standard: <https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-core-standard>
- DfE Cyber Security Hub: <https://cyber-security-hub.education.gov.uk/>
- NCSC – Cyber security guidance: <https://www.ncsc.gov.uk/>
- NCSC – Cyber Essentials: <https://www.ncsc.gov.uk/cyberessentials/overview>
- ICO – Personal data breaches: <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/>
- Academy Trust Handbook: <https://www.gov.uk/government/publications/academy-trust-handbook>