ZENITH
MULTI ACADEMY
TRUST

Cyber Security Policy

for use by all staff and volunteers in:
All schools in the Trust (including Castledon's Satellite)
Zenith Minds
Local Governing Boards
Trustees
Members

Approved by:	Board of Trustees
Date:	September 2026
Last reviewed:	September 2026
Next review due by:	September 2027

This policy is based on a model from LGfL (London Grid for Learning)

Contents

	Page No.
1. Introduction	1
2. Scope of Policy	1
3. Roles and Responsibilities	1
4. Risk Management	4
5. Physical Security	5
6. Asset Management	5
7. User Accounts	6
8. Devices	7
9. Data Security	8
10. Sharing Files	10
11. Training	10
12. System Security	11
13. Cyber Incident Response Plan	12
14. Maintaining Security	13
15. Reporting Cyber Incidents	13
16. Related Policies	15

1. Introduction

A cyber security incident can take many forms, including phishing, malware, ransomware, denial-of-service, unauthorised access to systems or data, and the accidental or deliberate loss of information.

For a school, this can range from minor disruption and reputational damage to the loss of access to teaching, safeguarding, and business systems, significant financial loss and regulatory action.

The Trust and its schools rely on digital technology to support teaching, safeguarding, communication and it's day-to-day operations. Maintaining the confidentiality, integrity and availability of its systems and data is therefore essential.

This policy sets out the minimum cyber security requirements that all schools within the Trust are expected to meet. It is intended to reduce the risk of cyber incidents and ensure that schools can respond and recover effectively when an incident occurs.

The policy supports the Trust's and school's responsibilities under data protection legislation,, the Academy Trust Handbook, the Department for Education's digital and technology standards, and where applicable, the conditions of the Risk Protection Arrangement (RPA)

2. Scope of Policy

This policy applies to all Trust staff, Trustees, Members, Local Governing Boards, contractors, volunteers, students and third-parties who s have permanent or temporary access to Trust or school systems, hardware, networks or data.

It applies to all digital technology used by or on behalf of the Trust and its schools, including:

- Servers, computers, laptops, tablets and smartphones
- Networks, wireless systems, switches and firewalls
- Cloud services and management information systems
- Email, telephony and communication systems
- CCTV and access-control systems
- Printers and other network connected devices
- Building-management and other internet connected systems

All external providers (including IT support partners and cloud service vendors) must comply with equivalent security standards and contractual arrangements, ensuring alignment with UK GDPR and the Data Protection Act 2018.

3. Roles and Responsibilities

Cyber security is a shared responsibility. However, each school remains responsible for implementing and maintaining appropriate security controls for the systems and services it manages.

Board of Trustees

The Board of Trustees is responsible for:

- Approving this policy and the minimum cyber security requirements applicable across the Trust.
- Providing strategic oversight of Trust-wide cyber security risk.
- Receiving assurance that schools are implementing the requirements of this policy.
- Ensuring that cyber security is considered within the Trust's wider risk-management and internal-scrutiny arrangements.

Chief Executive Officer

The Chief Executive Officer is responsible for:

- Ensuring that appropriate Trust-wide arrangements are in place to oversee cyber security.
- Ensuring that significant cyber security risks are reported to Trustees.
- Ensuring that appropriate action is taken where a school is unable to meet the requirements of this policy.

Headteachers

Headteachers are responsible for:

- Ensuring that this policy is implemented within their school.
- Ensuring that appropriate resources are provided to manage local cyber security risks.
- Appointing an appropriate member of Senior Leadership to act as the school's SLT Digital Lead.
- Ensuring that actions identified through risk assessments, testing or incidents are completed.
- Providing appropriate assurance to Governors and the Trust.

Trust Director of ICT Services

The Director of ICT Services is responsible for:

- Setting and reviewing the Trust's minimum technical and cyber security requirements.
- Providing advice, support and challenge to schools and their IT Support.
- Monitoring schools' progress against this policy and the relevant DfE standards.
- Reporting significant or common risks to the Chief Executive Officer and Trustees.
- Coordinating the response to incidents affecting central systems or more than one school.
- Supporting schools with the escalation and external reporting of significant incidents.
- Maintaining the security arrangements for systems and services managed centrally by the Trust.

School Network Manager

Each school's SLT Digital Lead is responsible for:

- Providing local leadership and oversight of cyber security.
- Coordinating the school's cyber security risk assessment.
- Working with the school's IT Support, Data Protection Lead, Designated Safeguarding Lead, finance staff and premises staff.
- Ensuring that required reviews, tests and actions are completed.
- Escalating significant risks or failures to the Headteacher and Director of ICT Services.
- Providing appropriate assurance to the Headteacher, Governors and Trust.

School IT Support

Each school's internal or external IT Support is responsible for:

- Implementing, maintaining and monitoring the technical controls required by this policy.
- Maintaining accurate asset, system and network documentation.
- Managing user accounts, devices, updates, backups, firewalls and other security systems.
- Responding to reported security weaknesses and incidents.
- Reporting significant risks, control failures and incidents to the school's SLT Digital Lead and Director of ICT Services.
- Providing evidence that the controls required by this policy are operating effectively.

For centrally managed systems, these responsibilities will be carried out by the relevant central Trust team or provider.

Data Protection and Safeguarding

School Data Protection Leads, the Trust's Data Protection Officer and Designated Safeguarding Leads will provide advice and support in relation to data-protection and safeguarding risks.

All users

All users are responsible for:

- Following this policy and the relevant Acceptable Use Policy.
- Protecting their account credentials and devices.
- Completing required training.
- Reporting suspected cyber incidents, data breaches or security weaknesses immediately.

4. Risk Management

Each school will identify and record its local cyber security risks within its risk register.

The school's Network Manager will coordinate a formal cyber security risk assessment at least annually. The assessment will be reviewed termly and following:

- A significant change to technology, systems or working practices.
- The introduction of a new critical system or service.
- A significant cyber incident or data breach.
- The identification of a new or materially changed threat.

The risk-assessment process will consider:

- Hardware, software, cloud services, networks and information assets.
- Risks to teaching, safeguarding, finance and school operations.
- User access and privileged accounts.
- The security and resilience of suppliers and external IT providers.
- Previous incidents, near misses and identified vulnerabilities.
- Physical and environmental risks to critical systems.
- Business continuity, disaster recovery and backup arrangements.

Schools will report significant risks, common concerns and failures to meet this policy to the Director of ICT Services.

Local Governors will review their school's risk register three times a year. The Trust will maintain oversight of Trust-wide and aggregated cyber security risks. The Trust's Finance, Audit and Risk Committee will review the Trust risk register four times a year and the Trust Board will conduct a full review at least annually.

Schools will also:

- Commission or participate in independent penetration testing or vulnerability assessments at least annually, with the scope and type of testing determined by identified risk.
- Complete additional testing following significant changes where appropriate.
- Support the Trust in working towards Cyber Essentials Plus certification.
- Document risk-treatment plans for significant cyber threats.
- Record and approve exceptions to this policy, including the associated risk, additional controls and planned remediation.
- Review significant supplier risks before procurement and at contract renewal.

The Trust may coordinate common testing, assurance or certification activities on behalf of schools.

5. Physical Security

Each school must ensure that appropriate physical security and environmental controls protect access to its IT systems. Controls will include, where appropriate:

- Air conditioning and environmental monitoring.
- Fire and flood protection.
- Uninterruptible power supplies.
- Lockable communications cabinets.
- Secure server and communications rooms.

Access to server rooms, communications cabinets and other secure IT areas must be limited to authorised staff and contractors who have a genuine business need.

Visitors and contractors requiring access to secure IT areas must be appropriately authorised, escorted where necessary and recorded through the relevant visitor or contractor-management process.

Keys, access cards and access codes for secure IT areas must be controlled and reviewed when staff or contractors leave or no longer require access.

Redundant IT equipment and storage media must be securely erased using approved erasure methods or physically destroyed by an appropriate disposal contractor. Records of disposal and certificates of destruction must be retained where provided.

Equipment must not be removed from school premises without appropriate authorisation. The asset register must be updated where equipment is permanently moved, transferred or disposed of.

6. Asset Management

Each school must maintain up-to-date records of the hardware, software, services and information assets that it manages. These records will include:

- A physical asset register covering servers, switches, firewalls, desktops, laptops, tablets and other managed devices.
- A contracts register covering licences, subscriptions, support arrangements, cloud services and approved applications.
- An information asset register covering systems and services that store or process personal, confidential or operationally critical data.
- Appropriate records of network-connected devices, including printers, CCTV, access control, telephony and building-management systems.

The central Trust team will maintain the relevant registers for centrally managed systems and services.

Managed IT equipment must be given a unique asset identifier where practicable and recorded in the school's central asset register. Records will include, where applicable:

- The manufacturer and model of the device
- The serial number and asset number.
- Its location or assigned user.
- The purchase or installation date.
- Its operating system or firmware.
- Its support and end-of-support status.
- Its planned review or replacement date.
- Its disposal date and method of disposal.

Registers must be updated whenever assets or services are added, changed, reassigned or disposed of. They must be formally reviewed at least annually, before financial planning and following a significant IT refresh.

Schools must provide asset or compliance information to the Trust when reasonably requested for assurance, risk management or financial planning.

Operating systems, software, firmware and cloud services that are no longer supported by their supplier must be replaced, removed or isolated from higher-risk systems and data.

7. User Accounts

Each school must maintain documented arrangements for creating, changing, reviewing, disabling and deleting user accounts for the systems it manages.

The central Trust team will manage accounts for centrally managed systems where responsibility has not been delegated to schools.

All users must be authenticated using unique credentials before accessing devices, networks, systems or services.

Users must protect their account credentials and must not share passwords, authentication codes or Multi-Factor Authentication requests with others. Personal accounts must not be used for work purposes.

If a user believes that their credentials may have been compromised, including following a phishing attempt, they must report this immediately to IT Support and change their password when instructed.

Account-security controls will include:

- Passwords of at least 12 characters, unless an alternative secure authentication method has been approved.
- Passwords that are unique to the account and not reused between work and personal services.
- Immediate password changes where a password is known or suspected to have been compromised.
- Technical controls to limit repeated or automated login attempts.
- Removal or replacement of default and vendor-supplied passwords before systems are placed into service.
- Multi-Factor Authentication for all staff accounts with access to cloud services or on-site systems, and for all privileged or administrative accounts, where supported.

Where a system does not support Multi-Factor Authentication, the exception, associated risk and additional controls must be documented and approved by the school's Network Manager in consultation with the Director of ICT Services.

Role-based access controls must be implemented to ensure that users only have access to the systems and data necessary for their role.

Each school must maintain documented joiner, mover and leaver processes. These processes will be coordinated between Human Resources, relevant managers and IT Support.

User accounts must be disabled immediately when a member of staff leaves or when access is no longer required. Email, files and other records must be transferred, retained or deleted in accordance with the school's leaver process and the Trust's data retention policies.

User accounts and access permissions must be reviewed at least termly to identify:

- Accounts that are no longer required.
- Changes in role that have not been reflected in access permissions.
- Dormant or unused accounts.
- Inappropriate or excessive access permissions.

Administrative access must be managed separately from routine user access. Administrative accounts must:

- Be used only for activities requiring elevated privileges.
- Not be used for routine email, internet access or day-to-day work.
- Be protected by Multi-Factor Authentication where supported.
- Be appropriately authorised before access is granted or changed.

Emergency access credentials for critical systems must be securely retained and available to an authorised member of Senior Leadership if normal IT Support is unavailable.

Remote access must be disabled when it is not required and enabled only for authorised users.

Only password managers approved by the school or Trust may be used to store work-related credentials.

8. Devices

Users are required to:

- Lock devices that are left unattended
- Install or allow security updates when prompted
- Report lost or stolen equipment immediately to IT Support
- Follow instructions from IT Support following the loss or theft of a device. This may include revoking active sessions, remotely locking or wiping the device and resetting affected credentials.
- Report suspected malware, unusual device behaviour or security weaknesses immediately.
- Not disable, bypass or interfere with security controls installed by the school or Trust.

Each school must ensure that devices it manages are configured with the following security controls as a minimum:

- Password, PIN, biometric or other approved authentication
- Centrally managed and actively monitored anti-malware software, including anti-virus protection, where supported
- Automatic security updates or centrally managed patching
- Removal of unnecessary, unauthorised and unsupported software
- Autorun disabled
- USB storage restricted by default, except where there is an approved school need.
- Approved removable storage scanned for malware before use.
- Users not given local administrative access by default
- Separate administrative accounts where elevated access is required
- A software firewall enabled on devices used outside the school network
- Full-disk encryption on laptops, tablets, smartphones and other mobile devices that store school or Trust data.
- Automatic screen locking after a maximum of 15 minutes of inactivity
- Remote lock or wipe capability where technically possible
- Enrolment in an approved Mobile Device Management (MDM) solution where technically feasible.

Where device cannot support an applicable control the exception and any additional security measures must be documented and approved.

Only applications approved by the school or Trust and obtained from a known or trusted supplier may be installed on school devices.

Personally owned devices may only access school or Trust systems and data where this has been authorised and appropriate security controls are in place.

9. Data Security

Each school must take appropriate technical and organisational measures to protect confidential information and reduce the risk of its loss, unauthorised disclosure, alteration or unavailability.

The Trust defines confidential data as:

- Personally identifiable information as defined by the ICO
- Special Category personal data as defined by the ICO
- Safeguarding and child-protection information
- Unpublished financial information
- Passwords, authentication information and security configurations
- Information classified as confidential by the school or Trust
- Information subject to a contractual duty of confidentiality

Access to confidential information must be restricted according to role and business need. Systems that process personal data must be recorded in the relevant Information Asset Register (IAR) and Record of Processing Activities (ROPA).

A Data Protection Impact Assessment must be completed where the processing is likely to result in a high risk to individuals or where otherwise required by the Trust's data-protection procedures.

Each school is responsible for identifying the critical data and systems it manages and ensuring that appropriate backup and recovery arrangements are in place.

The central Trust team is responsible for backup and recovery arrangements for centrally managed systems.

Critical data and systems must be backed up in accordance with a documented backup plan and the 3-2-1 backup methodology as a minimum:

- At least three copies of important data
- Copies held on at least two separate devices, platforms or types of media
- At least one copy held offsite and protected through offline or immutable storage.

Schools must also meet any current RPA condition requiring an offline backup.

Backup arrangements must include:

- Backup frequency and retention based on the criticality of the data and the school's agreed recovery requirements
- Daily or more frequent backups for critical systems where required.
- Weekly full backups where this is appropriate to the technology being protected.
- Appropriate incremental, full or cloud-based backup arrangements according to the system being protected
- Separate credentials and restricted administrative access for backup systems
- Encryption of physical backups and secure off-stie storage
- Monitoring of backup jobs and investigation of failures
- Total restorations completed and recorded at least termly
- An annual review of the backup plan and an additional review following significant changes
- Documented restoration priorities and expected recovery times for critical systems

A documented alternative may be used where a cloud or managed service does not use traditional incremental and full backups, provided it meets the school's agreed recovery requirements.

Physical backups must not be stored at an employee's home.

Schools must not assume that information held within a cloud services is adequately backed up by the provider. Backup and recovery arrangements for cloud services must be assessed before procurement and reviewed throughout the contract.

Schools must provide evidence of successful backup and restoration testing to the Trust when requested.

Where cloud services process personal data, the school must ensure that processing complies with UK GDPR. Appropriate safeguards and transfer risk assessments must be used where personal data is transferred outside the UK and an adequacy decision does not apply. .

Please refer to the Trust's Security Measures document for more information.

10. Sharing Files

The Trust recognises the risks associated with storing, sending and receiving confidential data. To minimise the risk of a data breach, users are required to:

- Only use Trust-approved platforms (e.g. SharePoint, OneDrive, Google Workspace) for storing and sharing files.
- Store school and Trust information on approved systems rather than personal devices or accounts.
- Not use personal email accounts or personal cloud-storage services for school or Trust information.
- Check the intended recipient, content and sharing permissions before sending or sharing information.
- Use secure sharing links with access limited to the intended recipients wherever possible.
- Remove external access when it is no longer required.
- Use approved email encryption or other secure transfer methods where confidential information cannot be shared through an approved platform.
- Send passwords or encryption keys through a separate communication method where this is necessary.
- Share safeguarding, SEN or other sensitive information only where there is a legitimate need and using an approved secure method.
- Consider whether an email or message could be fraudulent or whether the sender's account may have been compromised.
- Verify unusual requests using another communication method, particularly requests involving financial transactions, changes to payment details, website links or unexpected attachments.
- Report suspected data breaches, malicious activity or scams immediately to IT Support and the school's Data Protection Lead.

All external file transfers must use approved secure methods, such appropriately restricted cloud sharing, SFTP or an encrypted portal approved by the Trust.

Email systems must be configured with anti-spoofing protections including SPF, DKIM, and DMARC to reduce the risk of impersonation and phishing attacks.

Each school must ensure that the security controls protecting its email domains are appropriately configured and monitored. The central Trust team will be responsible for any email domains or systems it manages centrally.

11. Training

Each school must ensure that appropriate cyber security training and awareness activities are completed.

Cyber security training must be provided at least annually to:

- All employees.
- Governors and Trustees with access to school or Trust IT systems.
- Other users according to their role, level of access and associated risk.

Where a school is covered by the Risk Protection Arrangement, training must meet the current NCSC training requirements that form part of the conditions of cyber cover.

Each school must retain completion records and provide evidence to the Trust when requested.

The Trust may provide or commission a common training package to support schools in meeting this requirement.

Students must receive age-appropriate cyber security awareness as part of the curriculum or wider online-safety education.

Supply staff, agency workers, contractors and other temporary users with a login must receive appropriate security information or training as soon as reasonably practicable.

Staff responsible for maintaining IT systems or handling higher-risk information must receive appropriate specialist or role-specific training.

Schools may undertake phishing simulations and other awareness exercises to identify areas of weakness and inform future training.

All staff, students, supply staff, contractors and visitors with access to school or Trust systems, data or networks must be made aware of and agree to the relevant Acceptable Use Policy.

12. System Security

Each school, working through its internal or external IT Support, must implement and maintain the following minimum security controls for the systems and services it manages. The central Trust team will apply the same requirements to centrally managed systems and services.

Security controls will include:

- Keeping network hardware, operating systems, applications and firmware licensed, supported and up to date.
- Completing vulnerability fixes within 14 days where the vulnerability is rated critical or high risk, has a CVSS score of 7.0 or above, or has not been assigned a severity rating by the vendor.
- Applying security updates specifically directed by the DfE within five working days.
- Isolating or otherwise protecting devices where a high-risk vulnerability fix is unavailable.
- Centrally managing, monitoring and maintaining anti-malware systems.
- Ensuring that anti-malware systems scan files, downloads, applications, removable media and email attachments where supported.
- Monitoring backups and completing and recording test restorations at least termly.
- Reviewing and testing disaster-recovery arrangements at least annually and following significant changes.
- Using a correctly configured boundary firewall and ensuring that external network connections pass through the appropriate firewall.
- Blocking unauthenticated inbound connections by default.
- Keeping firewall rules to a minimum and documenting the reason for permitted inbound connections.
- Risk-assessing and reviewing permitted inbound firewall rules at least termly, with appropriate SLT sign-off.
- Protecting firewall and other critical administrative interfaces with Multi-Factor Authentication where supported.

- Restricting remote administrative access to authorised IT staff and approved providers.
- Monitoring appropriate firewall, network, identity and security logs and alerts.
- Maintaining up-to-date network diagrams, configuration records and IP-addressing information.
- Configuring networks to reduce the risk of malware spreading to critical systems.
- Segregating wireless networks used for visitors and personal devices from school systems.
- Applying appropriate security controls to internet-connected devices, including CCTV, access control, telephony, printers and building-management systems.
- Maintaining a list of approved applications and removing unauthorised or unnecessary software.
- Reviewing centrally managed anti-malware and firewall arrangements at least termly to ensure that they remain appropriate.
- Using appropriate threat-intelligence and early-warning services, including NCSC Early Warning where suitable.
- Maintaining filtering and monitoring arrangements in accordance with the Trust's Filtering and Monitoring Policy and the applicable DfE standard.
- Applying zero-trust principles where feasible.
- Proactively planning for the replacement of hardware, operating systems and software before suppliers stop providing security support.
- Assessing the security risk of new systems, services and projects before procurement or implementation.
- Reviewing the security of existing systems following significant changes and at appropriate intervals.
- Identifying and securely managing service accounts, shared technical accounts, API keys, application secrets and security certificates.
- Recording the owner, purpose and expiry date of certificates, client secrets and other time-limited credentials and renewing them before expiry.
- Reviewing service and shared technical accounts at least termly and removing those that are no longer required.
- Maintaining secure backups of critical firewall, switch, wireless, telephony and other infrastructure configurations.
- Documenting significant changes to network, security and cloud-service configurations, including the reason for the change and any required rollback arrangements.

Each school must retain appropriate evidence that these controls are being monitored and reviewed. Evidence may include system reports, update records, firewall reviews, backup logs, test-restoration results and risk assessments.

13. Cyber Incident Response Plan

Each school must maintain a Cyber Incident Response Plan that reflects its local systems, staffing, suppliers and business-continuity arrangements.

Schools should use the Trust's template, but local responsibilities, contact information, restoration priorities and alternative working arrangements must be completed and kept up to date.

The Trust will maintain an overarching incident-response framework covering escalation, external reporting, central services and incidents affecting more than one school.

Each school's plan must form part of its wider business continuity and disaster recovery arrangements and must be reviewed:

- At least annually.
- Following significant changes to systems, suppliers or responsibilities.
- Following a significant cyber incident.
- Where exercises or testing identify a weakness.

Schools must test their local incident-response arrangements at least annually. This may include a tabletop exercise, technical recovery test or simulated loss of a critical system. Schools must provide assurance to the Trust that testing has been completed and that identified actions are being addressed.

Copies of the plan and essential contact information must be maintained in more than one secure location, including an appropriately protected cloud location and an offline or hard-copy version.

Each school must maintain its registration with Police CyberAlarm where this is required as a condition of RPA cyber cover.

14. Maintaining Security

Each school must make proportionate financial provision for maintaining secure and resilient IT systems.

This will include provision for:

- Maintaining supported hardware, software and security systems.
- Replacing unsupported or high-risk technology.
- Maintaining appropriate backup and recovery arrangements.
- Providing cyber security training.
- Obtaining appropriate specialist advice, testing and incident-response support.

Cyber security requirements must be considered within each school's financial planning, procurement, business continuity and risk-management arrangements.

The Trust will consider common risks and requirements within its digital strategy and central financial planning. The Trust may coordinate common procurement, testing, training or security services where this provides improved protection or value for money.

15. Reporting Cyber Incidents

All staff and students must report suspected cyber incidents, attacks or significant security weaknesses immediately to the school's IT Support and Network Manager.

Examples include:

- Suspected phishing or account compromise.
- Malware or ransomware.
- Unauthorised access to a system or account.
- Loss or theft of a device.
- Unexpected system or network activity.
- Disruption or loss of access to critical systems.
- Attempts to bypass security controls.
- The accidental exposure or loss of information through a cyber incident.

Users must not attempt to investigate a suspected incident themselves unless instructed to do so. They must not delete messages, files or other potential evidence.

When an incident is reported, the school will:

- Assess the nature, severity and potential impact of the incident.
- Activate its Cyber Incident Response Plan where appropriate.
- Take immediate action to contain the incident and protect unaffected systems.
- Preserve relevant logs, messages and other evidence.
- Notify the Headteacher and other relevant Senior Leaders.
- Notify the Data Protection Lead, Data Protection Officer or Designated Safeguarding Lead where the incident may involve personal data or safeguarding information.
- Record the incident or near miss within its incident-reporting arrangements.
- Investigate the cause and determine what further action is required.
- Complete a post-incident review following significant incidents.

Schools must report significant cyber incidents, suspected compromises and material failures of security controls to the Director of ICT Services without delay.

The school remains responsible for taking immediate local action to contain the incident, protect unaffected systems and preserve evidence.

The Director of ICT Services will support the school and coordinate escalation where an incident:

- Affects a centrally managed system.
- Affects or has the potential to affect more than one school.
- Presents a significant financial, operational, safeguarding or reputational risk.
- Requires formal external reporting.
- Requires specialist incident-response support.

The school's RPA or cyber-response provider must be notified as soon as possible and in accordance with the applicable conditions of cover.

External reporting will be coordinated between the school and the central Trust team to ensure that reports are accurate, timely and consistent.

Where appropriate, cyber incidents will be reported to:

- Report Fraud.
- The DfE sector cyber team at Sector.Incidentreporting@education.gov.uk.
- The National Cyber Security Centre, including where an incident results in long-term school closure, the closure of more than one school or serious financial damage.

Where a cyber incident has resulted, or may have resulted, in a personal data breach, the school must also follow the Trust's separate Data Breach Policy and associated reporting procedure.

Material cyber incidents must be reported promptly to the Headteacher, Governors and Trust. Trustees will receive appropriate assurance reporting on significant incidents, near misses and resulting actions.

The Trust and its schools will not pay ransom or extortion demands under any circumstances.

16. Related Policies

This policy should be read alongside the Trust's and schools':

- Acceptable Use Policies.
- Data Protection Policy.
- Security Measures document.
- Filtering and Monitoring Policy.
- Business Continuity Plans.
- Disaster Recovery Plans.
- Cyber Incident Response Plans.
- Records Retention Policy.
- Backup and restoration procedures.
- Information Asset Register.
- Records of Processing Activities.
- Relevant IT technical standards and operating procedures.

This version puts the operational responsibility with each school while allowing the Trust to set expectations, request evidence and coordinate anything significant or cross-Trust. It reflects the current DfE cyber security standard, digital leadership and governance standard and RPA cyber conditions.