



Cornerstone Academy Trust

Cyber Security Policy

Trust-wide policy for pupils, staff and the wider school community

Policy owner	Trust IT Lead
Approval body	Board of Trustees
Updated	October 2026
Review cycle	Annual, or earlier following a change in law or guidance
Next review	Autumn Term 2027 or earlier if legislation, statutory guidance or technology materially changes
Applies to	All schools and operations of Cornerstone Academy Trust

Purpose

To protect the confidentiality, integrity and availability of Trust information and systems, and to establish clear governance for cyber risk and incident response.

Contents

Purpose.....	2
1. Purpose	5
2. Scope	5
3. Legal and regulatory framework	5
4. Definitions	6
5. Core principles.....	6
6. Roles and responsibilities	6
6.1 Board of Trustees	6
6.2 Executive Headteacher and Accounting Officer	6
6.3 Designated SLT Digital Lead.....	6
6.4 Trust IT Lead and IT support	7
6.5 Data Protection Officer.....	7
6.6 Leaders, system owners and users	7
7. Cyber risk management	7
8. Asset and system management.....	7
9. Identity and access management.....	7
10. Passwords and authentication	8
11. Privileged access.....	8
12. Secure configuration and change management.....	8
13. Patching and vulnerability management	8
14. Malware, firewall and network protection.....	8
15. Email, phishing and payment fraud.....	9
16. Data security and secure transfer	9
17. Mobile devices, remote working and BYOD	9
17.1 Remote working	9
17.2 Personally owned devices.....	9
18. Physical security	9
19. Backups and recovery.....	10
20. Logging, monitoring and alerting.....	10
21. Procurement, suppliers and cloud services.....	10
22. Cyber incident reporting.....	10
23. Cyber incident response	11
24. Personal data breaches	11
25. Business continuity and disaster recovery	11

26. Training and awareness	11
27. Pupil use of technology	12
28. Testing and assurance	12
29. Acceptable use and prohibited activity	12
30. Artificial intelligence and automated services	12
31. Secure disposal.....	12
32. Reporting weaknesses and responsible behaviour	13
33. Non-compliance	13
34. Monitoring and review.....	13
35. Related Trust documents.....	13
At least annually.....	14
At least termly	14
Following a significant incident or material change.....	15

1. Purpose

Cornerstone Academy Trust depends on digital technology to deliver education, safeguard pupils, communicate with families, administer its workforce and manage public funds.

A successful cyber attack could compromise safeguarding and personal information, interrupt teaching and essential services, cause financial loss, prevent access to important records and affect more than one campus or service across the Trust.

This policy establishes the Trust's approach to cyber security, assigns responsibility for cyber risk, protects the confidentiality, integrity and availability of information and systems, and provides a consistent minimum standard across all Trust campuses and services.

Policy position Cyber security is a Trust-wide governance, safeguarding and operational responsibility. It is not solely an IT function.

2. Scope

This policy applies across all Cornerstone Academy Trust campuses and services, whether access takes place from Trust premises, remotely or through a third-party service.

- Members and Trustees;
- employees, agency staff, contractors, consultants, trainees and volunteers;
- pupils and any other authorised users;
- third-party IT providers and suppliers;
- Trust-owned and authorised personally owned devices;
- networks, servers, cloud services, websites, applications, email and communication systems;
- removable media, backups, archives, operational technology and internet-connected equipment;
- electronic information and information transferred by electronic means.

3. Legal and regulatory framework

This policy is informed by relevant legislation, statutory guidance, government standards and contractual requirements, including:

- UK General Data Protection Regulation and the Data Protection Act 2018;
- Computer Misuse Act 1990;
- Human Rights Act 1998;
- Copyright, Designs and Patents Act 1988;
- Privacy and Electronic Communications Regulations 2003;
- Education Act 2002 and current Keeping Children Safe in Education guidance;
- Department for Education digital and technology standards for schools and colleges;
- National Cyber Security Centre guidance;
- academy trust risk management requirements;
- the Trust's funding agreement, Articles of Association and applicable Risk Protection Arrangement, insurance and contractual requirements.

This policy must be interpreted alongside related Trust policies and procedures. Where legislation or formal guidance changes, the Trust will implement necessary controls without waiting for the next scheduled policy review.

4. Definitions

Cyber security: Measures used to protect systems, services, devices and information from unauthorised access, damage, disruption, theft or misuse.

Cyber incident: An event that compromises, or may compromise, the confidentiality, integrity or availability of a system, service or information.

Personal data breach: A security breach resulting in accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Privileged account: An account with enhanced administrative or system-management permissions.

Multi-factor authentication (MFA): Use of two or more independent methods to verify identity.

System owner: The person responsible for the business purpose, controls and authorised user base of a system.

5. Core principles

1. Cyber security is a Trust-wide responsibility.
2. Controls will be proportionate to the sensitivity of information and the effect of loss, alteration, disclosure or unavailability.
3. Access will be based on role, business need and least privilege.
4. Trust information will be handled only through approved systems, services and devices.
5. Systems will be secured throughout their lifecycle.
6. Cyber risks, incidents and near misses will be reported openly and promptly.
7. The Trust will learn from incidents, exercises, assurance reviews and testing.
8. Material cyber risks will be visible to senior leaders and Trustees.

6. Roles and responsibilities

6.1 Board of Trustees

- approve this policy and oversee cyber risk strategically;
- ensure cyber risk is addressed through the Trust's risk-management framework;
- receive proportionate assurance on significant risks, controls, incidents and remedial action;
- ensure appropriate resources are considered through strategic and financial planning;
- seek assurance that incident response, business continuity and recovery arrangements are tested;
- complete required cyber security and data protection training.

6.2 Executive Headteacher

- ensure appropriate governance, controls and resources are in place;
- assign responsibilities and escalate significant risks to Trustees;
- ensure material incidents are managed appropriately;
- integrate cyber security with safeguarding, data protection, finance, risk management and business continuity.

6.3 Designated Digital Lead

- coordinate implementation of this policy;
- oversee the annual cyber risk assessment and termly reviews;
- monitor the cyber security improvement plan;
- ensure significant risks are recorded and escalated;
- provide assurance to the Executive Team and Trustees;
- oversee preparation and testing of incident-response arrangements.

6.4 Trust IT Lead and IT support

- implement approved technical controls and maintain inventories and technical documentation;
- manage accounts, permissions, secure configuration, updates, endpoint protection and firewalls;
- oversee backups, restoration testing, logging and monitoring;
- investigate alerts and incidents and retain appropriate evidence;
- advise on procurement, system changes and unresolved technical risk.

6.5 Data Protection Officer

- advise on protection of personal data, DPIAs, data breaches and regulatory reporting;
- advise on controller and processor duties and data-protection contract terms.

6.6 Leaders, system owners and users

- leaders must promote compliance, ensure training and notify IT promptly of starters, role changes and leavers;
- system owners must authorise access, assess significant changes and oversee secure retirement of systems;
- all users must protect accounts and devices, use approved systems, complete training and report incidents immediately.

7. Cyber risk management

The Trust will complete a formal cyber security risk assessment at least annually and revisit it at least termly. It will also be reviewed following a significant incident or a material organisational, system or process change.

- identify information, systems, threats, vulnerabilities and safeguarding implications;
- consider interdependencies across campuses, suppliers, cloud services and physical environments;
- record existing controls, likelihood, impact and residual risk;
- identify a named risk owner, required actions and target dates;
- inform the Trust risk register and cyber security improvement plan;
- escalate risks exceeding approved tolerance to the Executive Team and Trustees.

8. Asset and system management

The Trust will maintain accurate inventories and ownership records for significant hardware, software, cloud services, websites, network equipment, data stores, backups and internet-connected equipment.

- systems must have a defined purpose and owner;
- technology must be appropriately licensed, supported and securely configured;
- network documentation and significant configuration changes must be maintained and protected;
- support and end-of-life dates must be monitored;
- unauthorised hardware, software, browser extensions and cloud services must not be used;
- systems and storage media must be securely retired and asset records updated.

9. Identity and access management

- provide individual user accounts wherever practicable and avoid shared named-user accounts;
- apply least privilege and separate standard from administrative access;
- use MFA for appropriate systems, particularly privileged, remote and sensitive-data access;
- authorise account creation and access changes through an appropriate manager or system owner;
- amend access promptly for role changes and disable it promptly for leavers;
- review accounts, privileges, dormant access and supplier access periodically;
- investigate unexplained or unauthorised access.

10. Passwords and authentication

- users must create strong, unique passwords or passphrases and must not reuse Trust passwords for personal accounts;
- passwords, MFA codes and approval requests must never be shared by email, telephone, messaging service or in person;
- users must not approve unexpected MFA requests;
- default passwords must be changed before equipment or systems enter service;
- suspected compromise must be reported immediately and affected credentials secured;
- shared operational access must use an approved, controlled arrangement such as delegated access, an approved password manager or a formally managed service account.

Important IT support will not require a user's password to provide routine assistance.

11. Privileged access

- use separate administrator and standard accounts;
- require MFA for privileged accounts wherever technically possible;
- document and approve privileged access;
- restrict routine email and web browsing through administrator accounts;
- monitor privileged activity and review administrator accounts periodically;
- protect and control emergency access arrangements.

12. Secure configuration and change management

- remove or disable unnecessary accounts, services and applications;
- apply device encryption, screen locking, endpoint protection and firewall controls as appropriate;
- restrict local administrator rights and software installation;
- secure wireless networks and separate guest access from internal services;
- authorise, risk assess, test and document significant system or network changes;
- maintain a practical reversal or recovery route for material changes where appropriate.

13. Patching and vulnerability management

- monitor relevant vendor and security notifications;
- prioritise remediation according to risk and expedite critical or actively exploited vulnerabilities;
- use automatic updates where appropriate;
- identify unsupported and end-of-life technology;
- record outstanding vulnerabilities, temporary controls, owners and target resolution dates;
- replace, isolate or formally risk-treat unsupported systems.

14. Malware, firewall and network protection

- centrally managed endpoint protection, firewalls, email filtering and web filtering where appropriate;
- security alert monitoring and proportionate network separation;
- secure wireless and management interfaces;
- control of applications, removable media and external access;
- users must not disable or bypass protective controls;

- suspected malware must be reported immediately and evidence preserved.

15. Email, phishing and payment fraud

Users must treat unexpected requests for credentials, information, urgent payments, bank-detail changes, software installation or departures from normal procedure as potentially suspicious.

- verify unusual or sensitive requests using a separately obtained trusted contact route;
- report suspected phishing using the approved method;
- do not forward malicious content unnecessarily;
- contact IT immediately after clicking a suspicious link, opening an attachment or disclosing information;
- independently verify changes to supplier, employee or other payment details through approved finance procedures.

16. Data security and secure transfer

- use only approved Trust systems and accounts;
- check recipient identity and authority and disclose only the minimum information necessary;
- apply appropriate permissions and review sharing links and recipient lists;
- protect safeguarding, medical, SEND, personnel and financial information carefully;
- do not use personal email, personal cloud storage, unauthorised messaging or unauthorised removable media;
- encrypt sensitive and personal information in transit and at rest where appropriate;
- report misdirected information immediately.

17. Mobile devices, remote working and BYOD

17.1 Remote working

- use only approved devices, systems and security arrangements;
- prevent access by family members or other unauthorised people;
- lock devices when unattended and protect screens and confidential conversations;
- avoid unnecessary local downloads and report lost or stolen equipment immediately;
- do not use public or shared devices for Trust access.

17.2 Personally owned devices

Personally owned devices may access Trust systems only where expressly authorised and where required security standards are met. The Trust may require a supported operating system, current updates, encryption, screen lock, device-management controls, separation of Trust data and remote removal of Trust information.

18. Physical security

- restrict access to server, network and communications rooms;
- protect critical equipment against physical and environmental risks;
- secure portable devices and equipment in publicly accessible areas;
- control visitor access and keys or access cards;
- securely erase or destroy equipment and storage media before disposal;
- lock devices whenever unattended.

19. Backups and recovery

- define backup frequency and retention according to system importance;
- protect backups against unauthorised access, deletion and ransomware;
- separate backups from live services where appropriate;
- monitor backup success and failure;
- document restoration procedures and recovery priorities;
- test restoration periodically and record findings and remedial actions;
- restrict access to delete or alter backups.

20. Logging, monitoring and alerting

The Trust will maintain proportionate logging and monitoring for legitimate safeguarding, security, administration, legal-compliance and investigation purposes.

- record appropriate sign-ins, account and permission changes, privileged activity, system changes, security alerts and relevant network events;
- protect logs against unauthorised alteration or deletion;
- restrict access to authorised personnel;
- retain logs according to defined need and risk;
- review alerts and relevant records following incidents;
- provide appropriate information to users about monitoring.

21. Procurement, suppliers and cloud services

Cyber security and data protection must be considered before acquiring or materially changing a digital service.

- undertake proportionate due diligence covering data, hosting, authentication, encryption, backup, patching, availability, sub-processors and incident notification;
- put appropriate written terms in place where a supplier processes personal data;
- require suppliers to notify the Trust without undue delay of relevant security or personal data breaches;
- authorise, limit, protect, monitor and remove supplier access;
- review material suppliers and services periodically according to risk;
- ensure secure data return or deletion at contract termination.

22. Cyber incident reporting

All users must report actual or suspected cyber incidents immediately through the approved IT and data-breach routes. If the normal route is unavailable, the user must contact their manager or a senior leader directly.

- phishing, malware, unexpected MFA prompts or suspected account compromise;
- lost or stolen devices, misdirected information or unauthorised disclosure;
- payment fraud, unusual system behaviour or loss of availability;
- unexpected deletion or encryption of files;
- supplier-reported security incidents;
- attempts to bypass controls or any weakness that may expose the Trust.

Users must not conceal an incident, delay reporting while investigating, delete evidence, pay a ransom, communicate with an attacker or make public statements unless authorised.

23. Cyber incident response

The Trust will maintain a separate cyber incident response plan that remains accessible if normal systems are unavailable.

9. Initial reporting and triage.
10. Activation of the response team.
11. Assessment of severity, safeguarding implications and potential impact.
12. Containment and preservation of evidence.
13. Eradication and secure recovery.
14. DPO involvement where personal data may be affected.
15. Business continuity and authorised communications.
16. Contact with insurers, RPA, regulators, law enforcement or specialists where appropriate.
17. Restoration and validation of systems.
18. Recording of decisions, post-incident review and tracked remedial action.

24. Personal data breaches

Any cyber incident involving personal data must be reported immediately to the DPO through the Trust's data-breach procedure.

- assess the nature and extent of the data, affected individuals, protection applied and likely consequences;
- decide whether the Information Commissioner's Office must be notified;
- notify a reportable breach without undue delay and, where feasible, within 72 hours of awareness;
- inform affected individuals without undue delay where the breach is likely to result in a high risk to their rights and freedoms;
- record all personal data breaches, whether or not notified;
- document facts, effects, containment, decisions, communications, lessons learned and remedial action.

25. Business continuity and disaster recovery

Cyber security will be integrated into business continuity and disaster recovery arrangements. Plans will address loss or compromise of critical services, including safeguarding information, emergency contacts, management systems, communications, finance, payroll, identity services, teaching platforms, telephony, websites and backup services.

- maintain critical procedures and contacts in a secure location accessible during system outage;
- define system priorities, responsibilities and dependencies;
- test realistic disruption scenarios;
- record and monitor actions arising from exercises.

26. Training and awareness

- mandatory cyber security training during induction and at least annually thereafter;
- periodic updates on current threats and lessons from incidents;
- role-specific training for IT, leaders, finance and other higher-risk functions;
- appropriate training for Trustees and senior leaders;
- age-appropriate cyber security education for pupils;
- central records of required training and follow-up of non-completion;
- evaluation through knowledge checks, exercises, incident trends, feedback or assurance review.

27. Pupil use of technology

- pupils will receive age-appropriate guidance on passwords, suspicious communications, reporting concerns and responsible use;
- pupils must not use another person's account, disclose passwords, bypass controls, gain unauthorised access, install unauthorised software or interfere with systems;
- detailed requirements will be contained in pupil acceptable-use and online-safety arrangements.

28. Testing and assurance

- account and access reviews;
- vulnerability and configuration assessments;
- backup restoration and incident-response tests;
- business continuity exercises;
- supplier assurance reviews;
- internal audit or authorised external technical testing;
- review of alerts, incidents and improvement-plan progress.

No user may scan, probe, test or attempt to exploit Trust systems without prior written authorisation. Significant findings will be risk assessed and assigned to named owners.

29. Acceptable use and prohibited activity

Trust systems must be used lawfully, responsibly and primarily for authorised Trust purposes. Users must not:

- access information without authority or share credentials;
- bypass security, disable protective software or install unauthorised applications;
- connect unauthorised equipment or use unapproved cloud or AI services for confidential information;
- introduce malicious code or perform unauthorised security testing;
- access, create or distribute unlawful or inappropriate material;
- commit fraud, conceal activity or disclose Trust information without authority;
- use systems in a way likely to damage security, reputation or operations.

30. Artificial intelligence and automated services

- only Trust-approved AI and automated services may be used for Trust business;
- personal data, safeguarding information, special category data, security configurations, credentials and confidential information must not be entered into an unapproved service;
- use must comply with the Trust's AI Policy, data protection requirements and intellectual property obligations;
- outputs must be checked by an appropriately competent person before being relied upon.

31. Secure disposal

- follow record-retention requirements;
- securely erase information before reuse or disposal;
- destroy media where secure erasure is unsuitable;
- assess disposal suppliers and retain evidence where required;
- remove credentials, certificates and management connections;
- update asset records;
- users must not sell, donate, discard or retain Trust equipment independently.

32. Reporting weaknesses and responsible behaviour

Users are encouraged to report suspected weaknesses, mistakes and near misses promptly. They must not attempt to prove or exploit a weakness unless formally authorised. Reports made in good faith will be handled appropriately and used to contain risk and improve controls.

33. Non-compliance

Failure to comply may result in restriction or withdrawal of access, additional training, investigation under disciplinary procedures, termination of a supplier arrangement or referral to a regulator, police or other appropriate authority. Any response will be proportionate and will consider intent, impact, previous guidance and promptness of reporting.

34. Monitoring and review

The SLT Digital Lead and Trust IT Lead will monitor implementation and provide proportionate assurance reporting to senior leaders and Trustees.

- key cyber risks and significant incidents;
- high-priority outstanding actions;
- training completion;
- patching, vulnerability and unsupported-system risks;
- backup and restoration assurance;
- access-review and supplier-risk findings;
- incident-response and continuity exercises;
- progress against the cyber security improvement plan.

This policy will be reviewed at least annually and sooner following a serious incident, material change, substantial assurance finding or relevant change to legislation or government guidance.

35. Related Trust documents

- Data Protection Policy and Personal Data Breach Procedure;
- Acceptable Use and Online Safety policies;
- Filtering and Monitoring arrangements;
- Artificial Intelligence Policy;
- Staff Code of Conduct and pupil acceptable-use agreements;
- Business Continuity and Disaster Recovery plans;
- Risk Management, Records Retention and Procurement policies;
- Finance and fraud-response procedures;
- Safeguarding and Child Protection Policy;
- remote working, mobile device, BYOD and leaver procedures;
- privacy notices and information-asset and system registers.

Appendix 1: Immediate cyber incident actions

19. Report the incident immediately using the approved IT or data-breach route.
20. Stop interacting with suspicious content.
21. Disconnect the device from the network if safe to do so, but do not switch it off unless instructed.
22. Do not delete messages, files, logs or other evidence.
23. Do not investigate the incident personally.
24. Do not communicate with a suspected attacker or make a payment.
25. Tell IT what happened, including what was clicked, opened, entered, sent or disclosed.
26. Notify the DPO immediately if personal data may be involved.
27. Follow containment instructions issued by IT or the incident-response team.

Appendix 2: Minimum user security requirements

- Use your own account and strong, unique authentication credentials.
- Use MFA where provided and never share passwords or approval codes.
- Keep devices physically secure and lock screens when unattended.
- Install only authorised software and use approved storage and communication services.
- Check recipients before sharing information.
- Verify unusual payment or information requests independently.
- Report suspicious messages, system behaviour and lost devices immediately.
- Install updates when instructed and complete mandatory training.

Appendix 3: Cyber risk and assurance cycle

At least annually

- complete the Trust cyber risk assessment;
- review incident-response and disaster-recovery plans;
- test restoration of critical data or systems;
- review significant suppliers, privileged accounts and unsupported technology;
- deliver mandatory refresher training;
- report assurance and material risks to Trustees;
- review and approve this policy.

At least termly

- revisit the cyber risk assessment and improvement plan;
- review significant incidents, near misses and material control risks;
- confirm critical contacts and escalation information;
- escalate material risks through the Trust's risk-management process.

Following a significant incident or material change

- reassess relevant risks and controls;
- record lessons learned and assign remedial actions;
- update response, continuity, policy and training arrangements as required;
- report material matters to senior leaders and Trustees.