



CYBER SECURITY POLICY

2026/2027

Governance, prevention, detection, response and recovery



Document control	Details
Policy owner	Trust Digital Lead / Chief Operating Officer
Executive owner	Chief Executive Officer
Approved by	Trust Board
Approval date	[insert date]
Review cycle	At least annually and after a significant incident
Next review	June 2027
Classification	Internal - publishable policy; operational contact details restricted
Related plan	Cyber Incident Response Plan (Appendix A)

Important document distinction

This policy states the Trust's mandatory cyber security requirements. Appendix A is the operational response plan required for RPA cyber cover.

Contents

1. Purpose and policy principles
 2. Scope and definitions
 3. Governance, accountability and assurance
 4. Cyber risk management
 5. Required technical and organisational controls
 6. Threats, warning signs and prevention
 7. Incident reporting, response and recovery
 8. Data breach, safeguarding and communications
 9. Supplier and cloud security
 10. Training, testing, monitoring and review
- Appendix A: RPA-aligned cyber incident response plan
- Appendix B: Staff quick-action cards
- Appendix C: Incident severity and escalation matrix
- Appendix D: Minimum technical control schedule
- Appendix E: Recovery priorities and manual workarounds
- Appendix F: Incident log and post-incident review
- Appendix G: Standards mapping and references

Using this policy

Highlighted text is to be edited by each setting. Named products should be checked at each annual review so the policy remains accurate when suppliers or systems change.

1. Purpose and policy principles

This policy sets out how the HMFA protects the confidentiality, integrity and availability of its information, digital services and technology. It supports safeguarding, education continuity, financial control, data protection and statutory governance across all academies and central services.

The Trust will take a proportionate, risk-based and evidence-led approach aligned to the Department for Education (DfE) digital and technology standards, National Cyber Security Centre (NCSC) guidance, UK GDPR, the Data Protection Act 2018 and the cyber conditions of the DfE Risk Protection Arrangement (RPA).

Core principle

Cyber security is a whole-Trust safeguarding and business-continuity responsibility, not solely an IT function. Technical controls, human behaviour, governance and tested recovery arrangements must operate together.

The Trust will:

- assign clear accountability at Board, executive, school and technical levels;
- conduct an annual cyber risk assessment and review it at least termly;
- maintain accurate registers of hardware, software, cloud services, data, privileged accounts and suppliers;
- implement layered controls to prevent, detect and contain attacks;
- maintain ransomware-resistant, tested backups and viable manual workarounds;
- train all users and rehearse the incident response plan;
- report and manage incidents promptly, preserving evidence and meeting legal, safeguarding and RPA obligations;
- learn from incidents, near misses, audits and threat intelligence.

1.1 Security objectives

Objective	Meaning in a primary MAT
Confidentiality	Only authorised people can access pupil, safeguarding, staff, financial and operational information.
Integrity	Information, configurations and records are accurate, complete and protected from unauthorised alteration.
Availability	Critical services and information remain accessible, or can be restored within approved recovery targets.
Authenticity	Users, devices, messages and transactions can be verified.
Resilience	The Trust can continue essential safeguarding and education functions during disruption and recover safely.

2. Scope and definitions

This policy applies to trustees, governors, employees, agency staff, volunteers, contractors, pupils and any other person using Trust accounts, devices, networks, data or services. It applies whether access takes place on site, at home, while travelling or through a third party.

It covers all Trust-managed or Trust-authorised technology, including:

- Microsoft 365, Entra ID, Exchange Online, OneDrive, SharePoint and Teams;
- Arbor MIS and connected applications;
- Barracuda email security and Microsoft 365 backup;
- Bitdefender endpoint protection and any replacement endpoint detection and response service;
- Altaro or other server backup systems retained during migration (Acronis);
- firewalls, filtering and monitoring systems, switches, wireless networks, broadband and DNS services;
- servers, laptops, desktops, tablets, mobile devices, interactive displays, printers and Internet of Things devices;
- Sign In App, Single Central Record systems, MyConcern safeguarding, HR, payroll, finance and Insight Tracking assessment systems;
- websites, domains, social media accounts and public-facing services;
- third-party applications, integrations, APIs and managed service providers.

Key definitions

Term	Definition
Cyber incident	An event that threatens or compromises information or technology, including attempted attacks and near misses.
Personal data breach	A security breach causing accidental or unlawful loss, destruction, alteration, unauthorised disclosure of, or access to personal data.
Critical system	A service whose loss creates immediate safeguarding, legal, financial or major operational risk.
Privileged account	An account with administrative, configuration, security or broad data-access rights.
RTO	Recovery Time Objective: the target time to restore a service after disruption.
RPO	Recovery Point Objective: the maximum acceptable amount of data loss measured in time.
Offline/immutable backup	A backup protected from routine production access and resistant to alteration or deletion by an attacker.

3. Governance, accountability and assurance

Role	Mandatory responsibilities
Trust Board / Audit and Risk Committee	Approve policy and risk appetite; scrutinise termly assurance; ensure adequate resources; challenge recovery readiness; receive reports on significant incidents.
CEO / Accounting Officer	Overall executive accountability; authorise major incident decisions, closures, public communications and material expenditure.
SLT Digital Lead / Trust Digital Lead	Own cyber strategy and risk assessment; coordinate implementation; maintain standards roadmap; lead incident management unless delegated; report to the Board.
Chief Operating Officer / Operations Lead	Coordinate business continuity, finance, estates, procurement, insurance/RPA and operational communications.
Headteachers	Implement controls locally; ensure staff awareness; maintain local emergency arrangements; escalate incidents immediately; protect pupil welfare.
Data Protection Officer	Advise on personal data breach risk, ICO notification, affected individuals, processor obligations and documentation.

Role	Mandatory responsibilities
Designated Safeguarding Leads	Assess safeguarding consequences, maintain safe access to critical records and coordinate welfare actions during disruption.
IT support provider / internal IT team	Operate and evidence technical controls; monitor alerts; patch; maintain backups; isolate and investigate incidents; preserve logs; support recovery.
Finance Director / CFO	Maintain anti-fraud controls, payment verification and banking escalation arrangements.
System and information owners	Approve access, classify data, review suppliers, define recovery needs and test workarounds.
All users	Follow policy and acceptable use rules; complete training; protect credentials and devices; report suspicious activity immediately.

No single point of failure

At least two authorised people must be able to access emergency contacts, RPA membership details, critical supplier records, backup consoles and recovery documentation. Emergency information must not exist only within the systems it is intended to recover.

3.1 Board assurance dashboard

Measure	Minimum evidence / frequency
Cyber risk assessment	Annual full assessment; termly review of risks and actions.
Asset and systems registers	Termly reconciliation; unsupported technology highlighted.
MFA coverage	Monthly report; all staff, trustees and privileged accounts, with documented exceptions.
Patching	Monthly compliance report; critical/high-risk exceptions tracked.
Backups	Daily success monitoring; quarterly sample restores; annual full recovery exercise.
Training	Annual completion; new starters before or promptly after access; phishing simulations or equivalent learning.
Incidents	Termly trend report; immediate Board notification for critical incidents.
Supplier assurance	At procurement/renewal and risk-based annual review.
Response exercise	At least annually, plus after material changes or incidents.

4. Cyber risk management

The Trust will maintain cyber security as a standing risk within the corporate risk register. A detailed cyber risk assessment will be completed annually and reviewed every term, and whenever a major system, supplier, threat or organisational change occurs.

Cyber risk management cycle



The assessment must consider:

- safeguarding and pupil welfare;
- personal and special category data;
- loss of teaching, MIS, communications, payroll and finance services;
- Trust-wide propagation between academies;
- dependency on cloud, broadband, identity and managed service providers;
- single points of failure and loss of key personnel;
- unsupported or end-of-life technology;
- ransomware, credential theft, fraud, insider misuse and supplier compromise;
- physical events such as theft, fire, flood and power loss;
- recovery capability, including RTOs, RPOs and manual workarounds.

4.1 Asset, system and data registers

The Trust will maintain accurate IT Asset registers, Contract registers, and Data Mapping.

Discovery tools may support the registers but do not replace accountable ownership.

5. Required technical and organisational controls

5.1 Identity and access management

- Use unique named accounts; shared accounts are prohibited except where technically unavoidable and formally controlled.
- Apply least privilege and role-based access.
- Use joiner, mover and leaver processes with prompt removal of access; urgent leavers must be disabled immediately.
- Review privileged accounts monthly and all other access at least termly or risk-based.
- Maintain separate day-to-day and administrator accounts.
- Block legacy authentication and inactive accounts where supported.
- Protect service accounts with long managed credentials, restricted permissions and monitored use.

5.2 Multi-factor authentication and sign-in security

- MFA is mandatory for staff, trustees, governors, contractors and privileged users on Microsoft 365 and other critical services wherever supported.
- Prefer phishing-resistant methods such as passkeys, FIDO2 security keys or certificate-based methods for privileged and high-risk users; Microsoft Authenticator number matching is preferred over SMS texts.
- Users must never approve an unexpected prompt. Suspected MFA fatigue attacks must be reported immediately to Computeam.
- Conditional Access should restrict risky sign-ins, legacy protocols, unmanaged devices and administrator access where licensing and operational needs permit.
- Exceptions require documented risk acceptance, compensating controls, an owner and an expiry/review date.

5.3 Passwords and secrets

- Follow current NCSC password guidance: permit long passphrases, block common/compromised passwords and avoid routine expiry unless compromise is suspected or a system requires it.
- Do not reuse Trust passwords elsewhere or share credentials.
- Provide an approved password manager for users who manage multiple complex credentials.
- Store API keys, recovery codes and administrative secrets in an approved secure vault, not email or ordinary documents.

5.4 Devices and endpoint security

- All supported Trust devices must be centrally managed, encrypted where appropriate, protected by endpoint security and configured to lock automatically.
- Remove local administrator rights from ordinary users.
- Enable device inventory, remote lock/wipe and compliance controls where supported.
- Prohibit unauthorised software, removable media and personal devices unless explicitly approved.
- Lost or stolen devices must be reported immediately.

5.5 Vulnerability, patch and configuration management

- Use supported operating systems, firmware, applications and network equipment.
- Apply security updates promptly using a risk-based schedule; internet-facing and actively exploited vulnerabilities receive highest priority.
- Maintain secure configuration baselines and monitor deviations.
- Replace or isolate unsupported technology, with time-limited risk acceptance where replacement cannot be immediate.
- Undertake periodic external vulnerability checks and remediate findings.

5.6 Network, internet and DNS security

- Use business-grade firewalls with supported firmware, restricted management interfaces, secure remote administration and logged changes.
- Segment staff, pupil, guest, server, management and Internet of Things networks according to risk.
- Use secure wireless authentication and prevent guest networks from accessing internal services.
- Implement appropriate filtering and monitoring, protective DNS where available, and controls against malicious domains.
- Review firewall rules, remote access, VPNs and exposed services at least annually and after significant change.

5.7 Email, web and collaboration security

- Use Barracuda Email Protection or an equivalent secure email gateway for anti-phishing, malware, impersonation and link/attachment inspection.
- Configure SPF, DKIM and DMARC for Trust domains, progressing to an enforcement policy after monitoring.
- Disable automatic forwarding to external accounts unless approved and monitored.
- Apply safe-sharing defaults, external sharing controls and sensitivity appropriate to safeguarding and personal data.
- Verify requests to change bank details, make urgent payments, buy gift cards or disclose sensitive information using an independently sourced contact method.

5.8 Backups and recovery

- Protect Microsoft 365 using Barracuda Cloud Backup or an equivalent independent backup service; do not rely solely on native retention or recycle bins.

- Maintain backups of critical on-premises systems using Altaro or its approved successor (Acronis) while those systems remain in use.
- Keep at least one offline, immutable or logically isolated backup copy, using separate administrative credentials and MFA.
- Monitor backup success daily; investigate failures promptly.
- Test representative restores at least quarterly and conduct an annual end-to-end recovery exercise against agreed RTOs and RPOs.
- Record exactly what is and is not backed up, including configurations, websites, network equipment, cloud applications and encryption keys.

5.9 Logging, detection and monitoring

- Enable and retain appropriate audit logs for identity, email, endpoints, firewalls, critical cloud services, backups and administrative actions.
- Monitor alerts proportionately and define out-of-hours escalation for high-severity events.
- Synchronise system clocks.
- Protect logs from unauthorised alteration and retain them for a period based on risk, legal needs and investigation capability.
- Use available threat intelligence, supplier advisories, NCSC services and Police CyberAlarm where required for RPA cover.

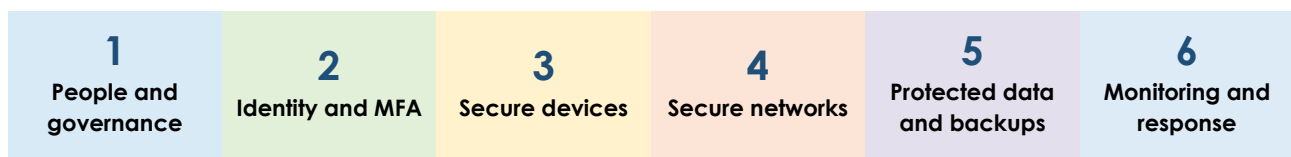
5.10 Data security and secure handling

- Classify information and apply appropriate access, encryption, sharing, retention and disposal controls.
- Restrict safeguarding, SCR, HR, payroll, medical and special category information to those with a genuine need.
- Use approved secure transfer methods; do not use personal email or unapproved consumer services.
- Apply “check twice, send once” for sensitive communications and verify recipients and attachments.
- Securely erase devices and media before reuse or disposal and retain disposal evidence.

5.11 Physical and environmental security

- Secure server/network rooms, cabinets and backup media; restrict and review physical access.
- Protect against theft, power failure, overheating, fire and water damage.
- Do not display passwords, recovery information or sensitive system details in public or insecure locations.

Layered defence model



Layered defence

No single product prevents every incident. The Trust expects overlapping controls so that the failure of one control does not lead directly to loss of safeguarding data or Trust-wide disruption.

6. Threats, warning signs and prevention

Threat	Typical warning signs	Principal prevention / mitigation
Phishing and credential theft	Unexpected sign-in prompts; fake login pages; urgent or unusual requests; inbox rules; sent messages not created by user	MFA; email filtering; user training; DMARC; conditional access; verify requests; rapid password/token reset
Business email compromise and payment fraud	Changed bank details; secrecy/urgency; invoice or payroll diversion; supplier impersonation	Two-person approval; call-back to known number; payment limits; finance training; mailbox monitoring
Ransomware / malware	Files renamed or encrypted; ransom note; endpoint alerts; sudden widespread slowness; disabled security tools	Patching; endpoint protection; segmentation; least privilege; macro controls; secure backups; application control
Account takeover	Impossible travel; new MFA methods; password reset messages; external forwarding; unusual downloads	MFA; risky sign-in monitoring; revoke sessions; review OAuth apps and inbox rules
Data exfiltration	Large downloads; unusual sharing; new external links; high outbound traffic	DLP/sharing controls; audit logs; least privilege; supplier monitoring; user awareness
Denial of service / service outage	Public services unavailable; high traffic; supplier status alerts	Resilient connectivity; supplier escalation; alternative communications; tested continuity plans
Lost or stolen device	Device missing; unauthorised access alerts	Encryption; screen lock; inventory; remote wipe; prompt reporting
Insider misuse / error	Unusual access; bulk copying; misdirected email; unauthorised software	Least privilege; supervision; separation of duties; logging; training; supportive reporting culture
Supplier / supply-chain compromise	Supplier alert; unauthorised integration activity; service changes or suspicious updates	Due diligence; contracts; MFA; limited integrations; incident clauses; exit plans; monitoring
Website/domain/social media compromise	Defacement; unexpected posts; DNS changes; certificate alerts	MFA; registrar lock; limited admin accounts; backups; monitored expiry and DNS changes
AI-enabled scams and deepfakes	Convincing voice/video request; unusual urgent payment or data disclosure	Independent verification; dual authorisation; staff awareness; do not rely on voice/video alone

7. Incident reporting, response and recovery

Report first - investigate safely

Users must report suspected incidents immediately. They should not delay reporting while trying to prove what happened. Staff must not delete evidence, communicate with an attacker, pay a ransom or attempt technical remediation unless instructed.

Incident lifecycle



7.1 Immediate staff actions

1. Stop and think. Do not continue entering information or approving prompts.
2. Where malware or ransomware is suspected, disconnect the network cable and switch off Wi-Fi if this can be done safely. Leave the device powered on unless the incident plan or IT support instructs otherwise, because volatile evidence may be required.
3. Call the designated incident number using a safe device. If normal email or Teams may be compromised, use the offline contact method.
4. Record what was seen, the time, device, account, actions already taken and any people contacted.
5. Follow instructions from the incident lead or IT support.

Important correction to older guidance

The previous draft instructed staff routinely to shut down an infected device. Current response should normally prioritise network isolation and expert direction; powering off can destroy useful evidence. The operational plan may specify shutdown only where continued operation would create greater immediate harm.

7.2 Incident management principles

- Life safety and safeguarding take priority.
- Assume an incident may affect more than one school or cloud service until evidence shows otherwise.
- Use clean communication channels and devices for response coordination.
- Preserve logs, emails, screenshots, device state and a decision timeline.
- Contain proportionately; emergency isolation may be authorised without prior consultation where delay creates material risk.
- Do not restore systems until the entry route is understood and compromised credentials, persistence and vulnerable configurations have been addressed.
- Recover in an agreed priority order, validate integrity and monitor closely for recurrence.
- A lessons-learned review will assign actions, owners and deadlines.

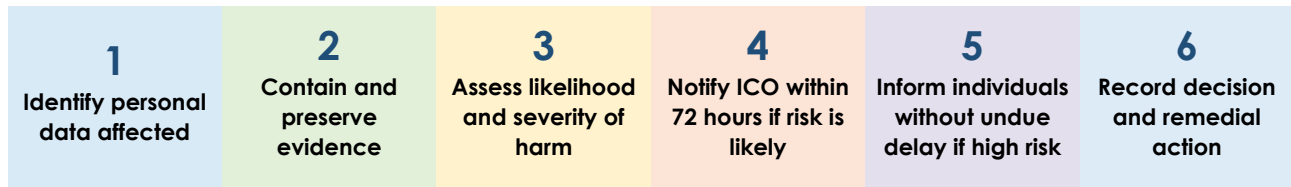
7.3 Authority during an incident

Decision	Authorised role (or deputy)
Declare a major cyber incident	CEO or Trust Digital Lead
Disconnect a school/site or service	Incident Lead or IT technical lead where delay is unsafe
Invoke business continuity / close a setting	CEO with Headteacher and safeguarding/operations advice
Contact RPA incident support / make a claim	CFO or nominated RPA contact
Notify ICO	Data controller through CEO/authorised lead, advised by DPO
Notify affected individuals	CEO/communications lead, advised by DPO and DSL
Engage law enforcement / NCSC / DfE	Incident Lead or executive owner
Pay ransom	The Trust will not normally pay. Any exceptional decision requires Board-level, legal, law-enforcement and RPA advice; payment does not guarantee recovery or lawful handling.

8. Data breach, safeguarding and communications

Not every cyber incident is a personal data breach, and not every personal data breach is caused by a cyber attack. The DPO must be informed without delay whenever personal data may have been lost, altered, disclosed or accessed without authority.

Personal data breach decision path



- The 72-hour period begins when the Trust becomes aware of a notifiable breach; incomplete information can be supplied in phases.
- All personal data breaches must be recorded, including those not reported to the ICO.
- Safeguarding risk may arise from loss of availability as well as unauthorised disclosure.
- The DSL must help identify vulnerable pupils, confidential addresses, court orders, medical needs and any immediate protective action.
- Communications must be accurate, timely and coordinated. Staff must not post or comment publicly unless authorised.
- Parent, pupil, staff and media messages must avoid speculation and must not compromise the investigation.

9. Supplier and cloud security

Security requirements must be considered before procurement, during implementation, throughout the contract and at exit. Risk ownership remains with the Trust even where services are outsourced.

Due-diligence area	Required assurance
Data and service scope	Purpose, data categories, hosting locations, integrations, sub-processors and critical dependencies are understood.
Security controls	MFA, encryption, patching, logging, access management, backups, vulnerability management and secure development are proportionate.
Incident obligations	Contract requires prompt notification, cooperation, evidence preservation, regulatory support and clear contacts.
Resilience and exit	Documented continuity, recovery commitments, data export, deletion, transition and supplier failure arrangements.
Independent assurance	Relevant certifications, penetration test summaries, Cyber Essentials/Plus or equivalent evidence where proportionate.
Access and administration	Supplier access is named, time-limited, least-privileged, MFA-protected, logged and removed when no longer needed.
Contract review	Security and data protection clauses reviewed at renewal and after material service change or incident.

10. Training, testing, monitoring and review

- All staff must complete NCSC-aligned cyber security training annually and as part of induction.

- Trustees and governors with access to Trust IT systems must complete training required by current RPA conditions.
- Role-specific training will be provided for IT administrators, finance, HR, safeguarding, communications and senior leaders.
- Pupils will receive age-appropriate cyber security and online safety education.
- The Trust will conduct at least one annual cyber response exercise; scenarios should include loss of Microsoft 365/MIS, ransomware, payment fraud and safeguarding data compromise over a rolling programme.
- The plan, offline contacts, recovery information and manual workarounds will be reviewed termly and after changes.
- Internal audit or independent assurance will be commissioned according to risk.

10.1 Compliance and exceptions

Non-compliance may result in access being restricted and may be managed under disciplinary, capability, pupil behaviour, contract or supplier processes as appropriate. Security exceptions must be documented, risk assessed, approved by the accountable owner, time limited and reviewed. Emergency exceptions must be recorded retrospectively as soon as practicable.

Appendix A - RPA-aligned Cyber Incident Response Plan

Restricted operational information

Complete the fields below and maintain a controlled offline copy. Do not publish personal mobile numbers, security architecture, backup credentials or detailed recovery instructions in a public policy.

Plan field	Current detail
24/7 RPA cyber incident support / claim route	Membership number: 116907 Contact the 24/7/365 RPA Cyber Emergency Assistance: By telephone: 0800 368 6378 or by email: RPAsupport@CyberClan.com
Trust incident lead and deputy	Liz Orton and Vic Goodman
IT technical lead and MSP emergency line	John Finch Antony Fernandez infosec@jfcsupport 01432 656584
CEO / CFO	Liz Orton – Nicky Jones
DPO	SchoolPro TLC – 01452 947633 dpo@schoolpro.uk
DSL escalation	Liz Orton and Vic Goodman
Communications lead	Liz Orton
HR support	Hoople
Police / Action Fraud / NCSC routes	[details and links in Appendix G] Action Fraud Action Fraud website or call 0300 123 2040 National Cyber Security Centre (NCSC) - https://report.ncsc.gov.uk
Offline plan locations	Hard copy in school office

A1. Activation triggers

- ransomware, widespread malware or suspected attacker presence;
- compromise of privileged, finance, safeguarding or executive accounts;
- loss of Microsoft 365, MIS, internet or other critical services beyond normal outage tolerance;
- suspected exfiltration or high-risk personal data breach;
- fraudulent payment or bank detail change;
- incident affecting multiple academies or a critical supplier;
- any event likely to attract media attention, cause closure or exceed internal capability.

A2. First 60 minutes checklist

Time / action	Owner	Record / evidence
Declare incident and nominate incident lead, scribe and technical lead.	Executive / Digital Lead	Start incident log; record awareness time.
Use clean communications; tell staff how to report and what not to use.	Incident Lead	Channel and message issued.
Contain affected accounts/devices/services proportionately.	Technical Lead	Actions, timestamps and authoriser.

Time / action	Owner	Record / evidence
Contact RPA incident support as soon as a significant incident is suspected; follow its instructions before appointing external specialists or incurring material costs.	RPA contact	Call reference, advice and claim requirements.
Assess safeguarding, personal data, finance and operational impact.	DSL / DPO / Finance / Heads	Initial impact assessment.
Preserve logs, emails, screenshots and affected devices.	Technical Lead	Evidence register and chain of custody.
Decide whether business continuity arrangements are required.	CEO / Heads	Decision and workarounds invoked.
Set next briefing time and external reporting decisions.	Incident Lead	Decision log.

A3. RPA conditions and evidence

- Maintain offline backups.
- Complete required NCSC cyber security training and retain completion evidence. Export Spreadsheet of results. Collate NCSC Cyber Security training certificates to send to the RPA.
- Register with Police CyberAlarm and maintain evidence of registration.
- Maintain and test this cyber response plan.
- Keep RPA membership details, incident records, invoices, specialist instructions, recovery evidence and proof of compliance.
- Check current RPA membership rules and follow the incident support/claim process in force at the time; requirements may change.

A4. Technical response phases

Phase	Key actions	Exit criteria
Triage	Validate report; classify severity; identify affected identities, devices, sites, data and services; establish timeline.	Incident is scoped sufficiently to choose containment.
Containment	Isolate devices/network segments; disable or restrict accounts; revoke sessions/tokens; block malicious indicators; preserve evidence.	Attacker activity is stopped or bounded and essential safety risks controlled.
Eradication	Remove persistence/malware; close vulnerabilities; reset credentials; review OAuth apps, inbox rules, admin changes and supplier access.	Known entry route and persistence addressed.
Recovery	Restore from known-good backups; rebuild securely; validate data and configurations; reconnect in phases; communicate status.	Critical services stable, monitored and accepted by owners.
Post-incident	Complete legal/RPA reporting; lessons learned; update controls, risk register, plan and training.	Actions assigned, tracked and Board assurance completed.

A5. Communications principles

- Use one authorised source of truth and scheduled situation reports.
- State what is known, what is not yet known, action being taken and what recipients should do.
- Do not name suspected attackers, speculate on cause or guarantee that data is safe before investigation.
- Consider accessible alternatives where normal email, websites or telephony are unavailable.
- Coordinate messages to staff, parents, pupils, suppliers, regulators, law enforcement and media.

Appendix B - Staff Quick-Action Cards

Scenario	Immediate action
Suspicious email, link or MFA prompt	Do not click, reply or approve. Use the reporting method. If credentials were entered or a prompt approved, call IT immediately from a safe device.
Suspected malware or ransomware	Disconnect network cable / turn off Wi-Fi if safe. Do not connect USB media. Do not delete files or run "clean-up" tools. Call IT. Leave powered on unless instructed otherwise.
Email or account compromise	Call IT. Use a safe device. IT should reset credentials, revoke sessions, review MFA methods, inbox rules, forwarding, OAuth apps and recent activity.
Lost or stolen device	Report immediately to IT and line manager, giving device, time, location and whether it was unlocked. Do not wait to see if it is found.
Wrong recipient / accidental disclosure	Contact the DPO and manager immediately. Do not rely solely on recalling an email. Record what was sent, to whom and whether it was opened/downloaded.
Payment or bank-detail fraud	Stop payment if possible. Call the bank using a trusted number, then finance leadership, IT and the incident lead. Preserve the message and transaction details.
Suspicious phone/video call or deepfake	End the interaction. Verify through a known number or in person. Never make a payment or disclose information solely on voice/video authority.
Website/social media compromise	Do not engage publicly. Call the incident lead/IT. Preserve screenshots and timestamps; secure registrar and admin accounts.

Appendix C - Incident Severity and Escalation Matrix

Level	Examples	Response target	Escalation
Critical	Trust-wide/multi-school impact; ransomware; confirmed high-risk data exfiltration; critical safeguarding records unavailable; major fraud; likely closure or media interest.	Immediate; activate full plan.	CEO, Chair/Board lead, RPA, DPO/DSL, relevant authorities and communications.
High	One school or critical service substantially affected; privileged account compromise; likely personal data risk; material financial or reputational impact.	Immediate; incident team within 30 minutes where practicable.	Executive, Trust Digital Lead, IT, DPO/DSL/Finance and RPA as appropriate.
Medium	Contained service/device incident; limited data exposure possible; workaround available; no immediate high risk.	Same working day.	IT and responsible leader; DPO/DSL/Finance according to impact.
Low / Near miss	Blocked phishing, minor isolated event, no evidence of compromise or data loss.	Prompt normal support process.	Record, remediate and trend; escalate if new evidence emerges.

Severity is not based only on staff percentages

Safeguarding, sensitivity of data, attacker privilege, cross-Trust spread, recovery uncertainty and legal/financial consequences can make a small technical incident critical.

Appendix D - Minimum Technical Control Schedule

Control	Minimum requirement	Evidence / frequency
MFA	All staff/trustee/admin accounts; critical services where supported; stronger methods for privileged users.	Monthly coverage report; exceptions register.
Privileged access	Separate accounts, least privilege, MFA, limited membership, logged use.	Monthly review.
Patching	Supported systems; risk-based prompt deployment; urgent exploited vulnerabilities prioritised.	Monthly compliance and exception report.
Endpoint security	Central management, encryption, endpoint protection, screen lock, no ordinary local admin.	Continuous monitoring; termly inventory reconciliation.
Email/domain	Secure gateway, SPF/DKIM/DMARC, forwarding controls, anti-impersonation.	Quarterly configuration review.
Backups	Independent backups; offline/immutable copy; separate credentials/MFA; documented scope.	Daily monitoring, quarterly restore, annual recovery test.
Network	Supported firewall, segmentation, secure Wi-Fi, logging, protected admin interfaces.	Annual review and after change.
Logging	Identity, endpoint, firewall, cloud, backup and admin logging retained and protected.	Monthly alert review / risk-based retention.
Asset registers	Hardware, software, services, owners, support status, criticality and recovery details.	Termly review.
Vulnerability checks	External exposure and public-facing services checked; findings remediated.	At least annually and after material change.
Response plan	Offline, role-based, contact details, RPA route and tested scenarios.	Termly contact check; annual exercise.
Training	NCSC-aligned annual training; role-specific modules.	Annual / induction records.

Appendix E - Recovery Priorities and Manual Workarounds

Priority	Service / information	Illustrative target	Manual / alternative arrangement
1 - Immediate	Safeguarding contacts and critical pupil welfare information	RTO [2-4 hours]; RPO [24 hours or better]	Offline emergency pupil/parent contact and medical/safeguarding extracts, securely controlled and regularly refreshed.
1 - Immediate	Emergency communications, telephony and leadership coordination	RTO [2 hours]	Alternative mobiles, emergency messaging service, pre-agreed parent communications.
2 - Essential	MIS attendance, contacts and registers	RTO [same day]	Paper registers and secure offline emergency lists; later controlled reconciliation.
2 - Essential	Identity / Microsoft 365 core communication	RTO [same day]	Clean-device emergency accounts and alternative channel.
2 - Essential	Finance, payroll and banking controls	RTO [1-2 working days]	Bank contact procedures, controlled payment deferral, dual authorisation and offline supplier contacts.
3 - Important	Teaching resources, file storage and collaboration	RTO [1-3 days]	Locally held contingency resources and non-digital teaching plans.
3 - Important	Websites, visitor and peripheral systems	RTO [1-3 days]	Manual visitor log, alternative public notice and safeguarding controls.

Targets above are examples and must be replaced by approved Trust RTOs/RPOs after business impact analysis. Offline extracts must be minimised, encrypted or physically secured, access logged and destroyed/replaced safely when refreshed.

Appendix F - Incident Log and Post-Incident Review

Incident log field	Record
Incident ID / title	
Date/time first event occurred (if known)	
Date/time detected and Trust became aware	
Reporter and contact	
Affected schools, users, accounts, devices, systems and suppliers	
Initial symptoms / indicators	
Personal data and safeguarding impact	
Financial / operational impact	
Decisions and actions with exact timestamps and authorisers	
Evidence preserved and location	
External contacts, references and advice	
Recovery validation and service-owner acceptance	
Closure date / residual risks	

Post-incident review questions

- What happened, and what is the evidence-based timeline?
- How did the attacker or error bypass controls?
- What worked well in detection, escalation, containment, communications and recovery?
- Were safeguarding, data protection, RPA and legal duties met?
- Were backups usable and recovery targets realistic?
- What control, contract, training, staffing or governance changes are required?
- Could the incident recur elsewhere in the Trust?
- Who owns each action, by when, and how will completion be assured?

Appendix G - Standards Mapping and References

Source expectation	Where addressed
DfE: annual cyber risk assessment and termly review	Sections 3-4; Board dashboard.
DfE: cyber response plan and business continuity	Section 7; Appendices A, C, E and F.
DfE: control and secure user accounts, including MFA and least privilege	Sections 5.1-5.3; Appendix D.
DfE: registers, supported technology, patching and secure configuration	Sections 4.1 and 5.4-5.6; Appendix D.
DfE/NCSC: staff training and governance	Sections 3 and 10.
NCSC: layered protection, incident management and ransomware-resistant backups	Sections 5-7; Appendix A.
ICO: detect, investigate, assess, document and notify notifiable breaches within 72 hours	Section 8; Appendix A.
RPA cyber conditions: offline backups, NCSC training, Police CyberAlarm, cyber response plan	Sections 5.8 and 10; Appendix A3.

- [Department for Education - Cyber security: core standard \(updated 24 June 2026\)](#)
- [Department for Education - Meeting digital and technology standards in schools and colleges](#)
- [DfE Cyber Security Hub - Risk Protection Arrangement conditions of cover](#)
- [GOV.UK - Make a claim through the Risk Protection Arrangement](#)
- [National Cyber Security Centre - Cyber Security for Schools](#)
- [NCSC - Cyber incident response processes](#)
- [NCSC - Mitigating malware and ransomware attacks](#)
- [NCSC - Principles for ransomware-resistant backups](#)
- [NCSC - Cyber security in schools: questions for governors and trustees](#)
- [Information Commissioner's Office - Personal data breaches: a guide](#)
- [GOV.UK - Where to report a cyber incident](#)