HAMBLIN EDUCATION TRUST

Cyber Security Governance, Assurance and Incident Management Policy

Version 2.0, June 2026

1. Purpose and Scope

This policy establishes the Hamblin Education Trust's framework for governing, assuring and responding to cyber security risks. It applies to both Trust schools, all staff, governors, trustees, volunteers and third-party suppliers who access Trust systems or data.

Cyber security is a strategic governance responsibility. The Board of Trustees owns the Trust's cyber risk in the same way that it owns financial, safeguarding and health and safety risk.

Responsibility for day-to-day management may be delegated, but accountability remains with the Board.

The lessons of attacks on trusts such as Fylde Coast Academy Trust, Thomas Hardye School and Pates Grammar School demonstrate that a failure of governance, not merely a failure of technology, is frequently the root cause of serious incidents.

This policy replaces Version 1.0 and has been revised to address identified operational weaknesses in the Trust's assurance framework.

2. Policy Objectives

The Trust will:

- Maintain a secure and resilient IT environment across all schools.
- Reduce the likelihood of successful cyber-attacks through layered technical controls.
- Minimise operational disruption caused by security incidents, including during examination periods.
- Ensure rapid, tested recovery following any incident.
- Protect all personal data held, including pupil safeguarding records, SEN data, staff financial and medical information.
- Meet all statutory and regulatory obligations, including under UK GDPR, the Data Protection Act 2018, the Academies Financial Handbook and DfE Digital Standards.
- Maintain current, independent assurance of the Trust's cyber security posture, not rely solely on auto-generated summaries.
- Ensure trustees are informed and can exercise meaningful oversight.

CURRENT 2026-7

3. Governance Structure and Responsibilities

3.1 Board of Trustees

The Board holds ultimate responsibility for cyber security governance.
It shall:

- Receive a formal cyber security report at each Board meeting (minimum quarterly).
- Review the cyber risk register at least annually and whenever a significant incident occurs.
- Approve and review this policy annually.
- Ensure adequate, ring-fenced investment in cyber security controls and independent assurance.
- Receive notification of any significant incident within 24 hours.
- Publish an Annual Trustee Cyber Assurance Statement (see Section 15).
- Confirm annually whether the Trust's external cyber security audit has been commissioned and completed.

3.2 Nominated Cyber Security Trustee

A named trustee shall be appointed as Cyber Security Lead. This trustee shall:

- Meet with the IT Manager each term and receive a written record.
- Report to the Board after each meeting.
- Receive copies of all vulnerability scan reports, penetration test findings and audit reports.
- Escalate any assurance gap, including a failure to commission required audits, to the full Board within 14 days of identification.
- Act as the Board's point of contact in the event of a major incident.
- Confirm in writing each term that they have reviewed assurance reports and are satisfied with, or have escalated concerns about, the Trust's cyber posture.

3.3 Executive Leadership Team

- Ensure this policy is implemented and complied with across both schools.
- Maintain and review the cyber security **risk register.**
- Escalate incidents immediately to the Cyber Security Trustee and Board Chair/Vice Chair.
- Commission all required independent audits and penetration tests in a timely manner.
- Ensure the Trust's Data Protection Officer is informed of any incident that may engage UK GDPR obligations.

3.4 IT Manager

- Maintain all operational technical controls described in this policy.
- Coordinate and support all external audits and penetration tests.
- Produce monthly operational assurance reports for the Cyber Security Trustee.
- Manage the incident response process.
- Clearly differentiate, in all reporting, between:
  (a) auto-generated monitoring summaries such as CyberAlarm reports; and
  (b) independent external audit findings.
  These must never be presented as equivalent.

- Maintain a written log of all security alerts, vulnerability scan results and remediation actions.

CURRENT 2026-7

3A. Board Cyber Risk Appetite

The Board recognises that cyber risk cannot be eliminated. The Trust's objective is to reduce cyber risk to a level that is acceptable, proportionate and consistent with its statutory duties to protect:

- pupils and safeguarding information;
- educational continuity;
- financial resources;
- staff personal information;
- public confidence.

The Board shall review and approve its cyber risk appetite annually.

Where risks exceed the Board's agreed appetite, management shall present either:

- a mitigation plan;
- an investment proposal; or
- a formal recommendation for Board acceptance of the residual risk.

No significant cyber risk shall remain outside the Board's knowledge.

CURRENT 2026-7

4. What Counts as Assurance: Critical Distinction

This section is mandatory reading for all trustees and the Executive Leadership Team.

Report / Activity	What it covers and what it does NOT
Police CyberAlarm Monthly Report	Auto-generated summary of inbound threat alerts detected by the police monitoring system. Provides useful supplementary threat intelligence. Does NOT assess the Trust's own security controls, patch levels, system configurations, backup integrity or staff awareness. Cannot detect threats that bypass the monitored perimeter. NOT an audit.
External Cyber Security Audit	Independent assessment conducted by a qualified external organisation of the Trust's security controls, policies, configurations, access management, backup and recovery arrangements, staff practices and governance. Provides the Board with an evidence-based view of actual risk exposure. REQUIRED annually under this policy.
Penetration Test	A simulated attack by an authorised external expert to identify exploitable vulnerabilities in internet-facing services, internal networks and wireless infrastructure. Distinct from and complementary to the external audit. REQUIRED annually under this policy.
Cyber Essentials / CE Plus	Government-backed certification scheme. Cyber Essentials (self-assessed) provides a baseline. Cyber Essentials Plus (independently verified) provides stronger assurance. REQUIRED: CE within 12 months, CE Plus within 24 months.
Vulnerability Scan	Automated weekly scanning of Trust systems to identify known vulnerabilities. Operational control, not independent assurance. Results must be reviewed by the IT Manager and reported monthly.

The Board must not regard any single source as providing complete assurance. Only a combination of independent audit, penetration testing, Cyber Essentials certification and ongoing monitoring constitutes a sound assurance framework.

CURRENT

5. Minimum Technical Security Standards

5.1 Identity and Access Management

Multi-Factor Authentication (MFA)

MFA is mandatory. Following attacks on trusts where compromised credentials enabled full network access, MFA represents the single most effective control available.

It shall be enforced, not merely encouraged, for:

- All staff Microsoft 365 and email accounts.
- All remote access systems (VPN, remote desktop, cloud platforms).
- All administrator and privileged accounts.
- All finance system access.
- All trustee and governor accounts.
- All third-party supplier access to Trust systems.

Implementation deadline: Within **90 days of policy approval** for all remaining accounts.

Conditional Access policies shall be configured within Microsoft Entra ID (formerly Azure AD) to block or flag sign-ins from:

(a) locations outside the United Kingdom and expected staff locations;

(b) known malicious IP ranges; and

(c) non-compliant or unmanaged devices.

Password Standards

- Minimum 14 characters for all accounts.
- Trust-provided password manager to be used by all staff. Personal password managers are not acceptable for work credentials.
- **No password reuse between personal and work accounts.**
- No password sharing under any circumstances. Shared accounts are prohibited.
- Privileged administrator accounts must use credentials entirely separate from normal user accounts, no administrator using a single account for both standard and privileged operations.
- Passwords for critical systems (finance, MIS, HR) must be changed immediately upon any member of staff leaving the Trust.

Privileged Access Management

- Administrative privileges are granted only on a documented, need-to-have basis.
- A privileged access register shall be maintained and reviewed quarterly by the IT Manager.
- All privileged access shall be logged and these logs reviewed monthly.
- Stale or unused privileged accounts shall be disabled within 24 hours of identification.
- On departure of any staff member with privileged access, credentials shall be revoked on the final working day and an access review conducted within 48 hours.

CURRENT 2026-7

5.2 Network Segmentation and Conditional Access

A failure of network segmentation was a significant factor in the Fylde Coast attack, where ransomware was able to propagate across all 10 schools simultaneously.

The Trust shall:

- Maintain separate network segments for: staff systems; pupil devices; administrative and finance systems; building management systems; and guest/visitor Wi-Fi.
- Ensure that a compromise of the pupil network cannot propagate to staff or finance systems.
- Document network topology and segmentation annually and include this in the penetration test scope.
- Implement Microsoft Entra ID Conditional Access policies to restrict cloud resource access by geography and device compliance state.

5.3 Device Management and Endpoint Protection

- All Trust-owned devices shall be enrolled in a Mobile Device Management (MDM) solution.
- Endpoint Detection and Response (EDR) software shall be deployed on all managed devices, not merely traditional antivirus.
- Personal devices shall not access Trust systems without explicit IT Manager approval and enrolment in the MDM solution.
- USB and removable media use shall be restricted by policy and enforced technically where possible.
- All devices shall be encrypted at rest.

CURRENT 2026-7

6. Vulnerability Management

Ransomware groups including those responsible for attacks on UK schools routinely exploit known but unpatched vulnerabilities (such as PrintNightmare, exploited in multiple school attacks). Vulnerability management is therefore a primary control.

6.1 Automated Vulnerability Scanning

- Weekly automated vulnerability scanning shall be conducted across all Trust systems.
- Results shall be reviewed by the IT Manager weekly and a monthly summary report produced for the Cyber Security Trustee.
- Critical vulnerabilities shall trigger an immediate escalation to the Cyber Security Trustee.
- External-facing systems shall be scanned at least fortnightly.

6.2 Patch Management

Patch Category	Timescale / Requirement
Critical security patches	Within 14 days of release
High-risk patches	Within 30 days of release
Routine patches	Within 60 days of release
Compliance target	95% of systems patched within required timescales
Reporting	Monthly compliance report to Cyber Security Trustee; quarterly summary to Board
Legacy systems	Any system unable to receive patches must be isolated from the main network, documented in the risk register and a replacement timeline agreed within 30 days

Legacy and unsupported systems represent a critical risk. The IT Manager shall maintain a register of all systems running unsupported software and present a remediation or isolation plan to the Executive Leadership Team within 30 days of identification.

CURRENT 2026-7

7. Penetration Testing

Penetration testing by qualified, independent specialists is a non-negotiable assurance requirement. CyberAlarm reports and vulnerability scans do not replace penetration testing. The Trust shall commission:

7.1 Annual External Penetration Test

Scope shall include as a minimum:

- All internet-facing services and systems.
- School websites and any public-facing applications.
- Firewall and perimeter controls.
- VPN and remote access systems.
- Email security controls (including phishing simulation capability).
- Microsoft 365 tenant configuration review.

7.2 Annual Internal Network Penetration Test

Scope shall include:

- Staff and administrative networks.
- Pupil networks.
- Wireless infrastructure (including testing from a guest/student device perspective).
- Active Directory and Microsoft Entra ID configuration.
- Network segmentation effectiveness, specifically, whether a compromise of one segment can reach others.

7.3 Reporting and Remediation

- Full written penetration test reports shall be provided to the Cyber Security Trustee within 14 days of testing completion.
- A remediation tracker shall be maintained and reviewed monthly.
- Critical findings must be addressed within 30 days. High findings within 60 days.
- Unresolved findings shall be reported to the Board quarterly.
- Re-testing shall be conducted following remediation of critical findings.

CURRENT 2026-7

8. Backup, Recovery and Business Continuity

The Thomas Hardye School attack encrypted both the school's primary systems and its backup copies, rendering recovery impossible without significant forensic intervention. The Trust's backup arrangements must be designed to survive a complete ransomware encryption event.

8.1 Backup Requirements

- Daily automated backups of all critical systems.
- Immutable backup copies that cannot be modified or deleted by ransomware or any user, including administrators.
- Off-site backup storage, geographically separate from the primary Trust network.
- At least one set of backups that is air-gapped (offline) or cloud-isolated with access controls fully separate from the main Trust IT environment.
- Backups must be encrypted in transit and at rest.
- The backup system must itself be protected by MFA and have separate credentials from the main network.

8.2 Backup Testing

Test Type	Frequency / Requirement
Restore test, sample files	Monthly
Restore test, full system	Quarterly
Annual full disaster recovery exercise	Annually, must simulate a complete ransomware encryption of all primary systems
Test results reported to	Cyber Security Trustee within 7 days; Board quarterly
Failed restore tests	Immediate escalation to Cyber Security Trustee; remediation within 14 days

8.3 Recovery Time Objectives

System Category	Target Recovery Time
Critical systems (MIS, safeguarding, finance, email)	24 hours
Administrative systems	48 hours
Non-critical systems	5 working days
Maximum acceptable data loss (RPO)	24 hours

8.4 Manual Continuity Procedures

Schools must maintain paper-based continuity procedures for use in the event that all IT systems are unavailable. These must cover:

- Pupil registration and attendance recording.
- Safeguarding reporting routes and contact details (maintained in paper form, not solely on network systems).
- Emergency contact details for parents and carers.
- Exam centre contingency arrangements.
- Finance and payroll emergency contact details.
- Communication plan for staff, parents and carers that does not depend on Trust email systems.

CURRENT 2026-7

9. Monitoring and Detection

The Trust shall maintain the following monitoring and detection controls:

- Police CyberAlarm participation, treated as supplementary threat intelligence only, not as primary assurance.
- Firewall monitoring with alerting for unusual outbound traffic patterns (a common indicator of ransomware data exfiltration).
- Endpoint Detection and Response (EDR) across all managed devices.
- Email threat monitoring including anti-phishing, anti-spoofing (DMARC, DKIM, SPF) and attachment sandboxing.
- Microsoft 365 security alert monitoring via the Security and Compliance Centre.
- Audit log retention for a minimum of 12 months.
- Security alerts from all systems to be routed to the IT Manager with defined escalation procedures.

10. Staff Awareness and Training

A 2023 survey found that one in three UK teachers had received no cyber security training at all. Human error, particularly falling for phishing emails, remains the most common initial attack vector in school cyber incidents. The Trust's training programme is therefore a primary, not secondary, control.

10.1 Mandatory Annual Training

All staff, including part-time and supply staff with system access, must complete annual training covering:

- Phishing and social engineering recognition and reporting.
- Password security and use of the Trust password manager.
- UK GDPR and data protection obligations.
- Ransomware, what it is, how it spreads and what to do if suspected.
- Safe use of AI tools (including what data must not be entered into public AI systems).
- Incident reporting procedures, who to contact, when and how.
- Remote working security.
- Safeguarding data handling, given the consequences of leaks in the Pates Grammar and Guildford County School attacks.

New starters: Training must be completed within 10 working days of joining. System access shall not be granted until initial cyber security induction is complete.

10.2 Phishing Simulation Exercises

- A minimum of four phishing simulations per academic year (at least one per term).
- Simulations must vary in type, including impersonation of senior leaders, finance requests, HMRC/payslip themes and IT helpdesk themes.
- Simulations must be targeted at all staff, including senior leaders, governors and trustees.
- Results, including click rates, report rates and follow-up training completion, must be reported to the Board.
- Any staff member who fails more than two simulations in an academic year must complete enhanced one-to-one training.

CURRENT 2026-7

10.3 Trustee and Governor Training

- All trustees and governors must complete annual cyber security awareness training.
- The Cyber Security Trustee must complete additional training relevant to their role, such as the NCSC Board Toolkit training.
- Compliance with trustee training requirements shall be recorded and reported to the Board Chair.

11. Third-Party Supplier Security

Third-party suppliers with access to Trust systems or data represent a significant attack surface.

All suppliers granted access must:

- Hold Cyber Essentials certification (minimum) or equivalent recognised standard.
- Use MFA to access any Trust system or data.
- Operate under a written contract that includes: data protection obligations; incident reporting requirements (notification within 4 hours of a suspected incident affecting Trust systems or data); right to audit; and the requirement to maintain and provide evidence of their own cyber security controls.
- Access Trust systems only from managed, encrypted devices.
- Be granted access only to the specific systems required for their contracted purpose (principle of least privilege).
- Have their access reviewed and re-authorised annually and revoked immediately on contract termination.

The IT Manager shall maintain a register of all third-party suppliers with system or data access. This register shall be reviewed quarterly and presented to the Audit Committee annually.

12. Cyber Incident Response

The Trust shall maintain a standalone Cyber Incident Response Plan. This section sets out the minimum requirements for that plan and the escalation procedures that must be followed.

12.1 Immediate Escalation Triggers

The following incidents shall trigger immediate response procedures:

- Any suspected or confirmed ransomware infection on any Trust device or system.
- Any suspected or confirmed personal data breach (affecting staff, pupil or third-party data).
- Any confirmed compromise of staff credentials.
- Any IT service outage exceeding four hours.
- Any loss or theft of an unencrypted device containing Trust data.
- Any confirmed phishing email that has resulted in credential entry or malware download.
- Any demand for ransom or threat to publish Trust data.

CURRENT 2026-7

12.2 Escalation Contacts, Hardcopy Required

The following contacts must be maintained in hardcopy at each school office and at the Trust central office. These must not be stored only on network-connected systems, which may be unavailable during an incident.

Role	Contact Details
Trust CEO	Tim Gartside.
Board Chair	Michael Thompson. 07710033501. V/C Sharon Forster
Cyber Security Trustee	Michael Thompson
IT Manager	Jan Timmins
Data Protection Officer	
Cyber Incident Response Provider	[Insert provider name, contract reference and emergency number]
National Cyber Security Centre (NCSC)	0300 020 0973 / report.ncsc.gov.uk
Information Commissioner's Office	0303 123 1113
Local Police / Action Fraud	0300 123 2040
ESFA / DfE Incident Line	[contact number]
Exam Board Emergency Contacts	[Board contacts, critical during exam season]

12.3 Response Phases

Phase	Actions
IDENTIFY	Confirm the nature and scope of the incident. Isolate affected systems immediately to prevent spread. Do not switch off devices unless instructed by the incident response provider.
CONTAIN	Disconnect affected systems from the network. Preserve evidence, do not wipe or restore systems before forensic review. Engage the cyber incident response provider.
NOTIFY	Notify the CEO, Board Chair/VC and Cyber Security Trustee within 4 hours. Notify the NCSC. Assess whether the ICO must be notified within 72 hours (UK GDPR obligation). Notify exam boards if incident affects exam-related systems.
RECOVER	Begin recovery from immutable backups only after the incident response provider has confirmed systems are clean. Document all recovery actions. Maintain paper-based operations in the interim.
REVIEW	Within 28 days of incident resolution, produce a formal post-incident review. Share lessons learned with the Board. Update the cyber risk register and this policy if required.

CURRENT 2026

12.4 Communication Plan

The Trust must maintain a communication plan that does not depend on Trust email or telephony systems, which may be unavailable.

The plan must include:

- Personal mobile contacts for all Headteachers and the CEO.
- A holding statement for parents and carers that can be issued via text message and posted to school websites.
- A media enquiry protocol, all press enquiries during an incident must be routed to the CEO.
- A template notification letter for affected individuals in the event of a personal data breach.

12.5 Ransom Payment

The Trust's policy is not to pay ransoms. Payment does not guarantee the return of data or restoration of systems and funds future criminal activity. Any demand for ransom must be reported immediately to the NCSC and local police. The decision not to pay must be confirmed by the Board.

13. Cyber Insurance

Government data indicates that fewer than half of schools know whether they hold cyber security insurance. This represents a critical financial planning failure.

The Trust must:

- Establish within 30 days of this policy's approval whether it holds cyber security cover and the scope of that cover.
- If covered: document the insurer's name, policy number, incident notification requirements and the emergency contact number. Store this in hardcopy at the Trust central office and each school.
- If not covered: present a risk assessment and options paper to the Board within 60 days.
- Include the cyber insurance position in the quarterly cyber report to the Board.
- Review coverage annually to ensure it reflects the current threat landscape.

Note: If we participate in the DfE's Risk Protection Arrangement (RPA) we should confirm whether cyber cover is included and the limits and exclusions that apply.

CURRENT 2026-7

14. Independent Assurance Programme

Assurance Activity	Detail
Annual external cyber security audit	Commissioned by: Executive Leadership Team. Report to: Cyber Security Trustee and Board. Deadline: Must be completed by end of each academic year.
Annual external penetration test (internet-facing)	Commissioned by: IT Manager. Report to: Cyber Security Trustee. Findings to Board: Quarterly.
Annual internal penetration test	Commissioned by: IT Manager. Report to: Cyber Security Trustee. Findings to Board: Quarterly.
Cyber Essentials certification	Target: Within 12 months of policy approval.
Cyber Essentials Plus	Target: Within 24 months of policy approval.
Quarterly vulnerability scan reports	IT Manager to Cyber Security Trustee.
Monthly CyberAlarm report review	IT Manager, treated as supplementary intelligence only.
Annual disaster recovery exercise	Results to Board.

CURRENT 2026

15. Trustee Reporting Framework

Quarterly cyber reports to the Board must include the following structured sections. The report template must be approved by the Board and must not be reduced in scope without Board approval.

Report Section	Content Requirement
Threat Overview	Number of alerts detected; number of significant attempted attacks; details of any successful attacks or near-misses; current national threat level for education sector.
Assurance Status	External audit: commissioned / completed / overdue. Penetration test (external): status. Penetration test (internal): status. Cyber Essentials: certification status. CyberAlarm: summary of latest report, noted as supplementary only.
Vulnerability Management	Number of critical and high vulnerabilities identified; patch compliance percentage; outstanding critical or high unresolved vulnerabilities; age of oldest unresolved vulnerability.
User Security	MFA compliance rate (with breakdown by school and staff group); staff training completion rate; phishing simulation results; trustee training compliance.
Infrastructure Security	Patch compliance; backup test results (including any failures); date of last restore test; disaster recovery exercise status.
Incidents	Number and nature of incidents in period; regulatory reports made; post-incident reviews completed.
Risk Register	Top three cyber risks; any new emerging risks; investment decisions required.
Cyber Insurance	Current coverage position.
Trustee Decision Required	Clear statement of any Board decisions sought, including investment requests or risk acceptance.

16. Safeguarding Data, Specific Requirements

Attacks on schools including Pates Grammar School, Guildford County School and others have resulted in the publication of highly sensitive safeguarding information, including SEN records, child passport scans and safeguarding case notes. The consequences for affected children and families are severe and long-lasting. The Trust must apply the highest level of protection to safeguarding data.

- Safeguarding records must be stored in systems with access strictly limited to those with a documented need.
- Access to safeguarding systems must be reviewed termly.
- Safeguarding data must never be stored in personal email accounts, shared drives without access controls, or personal devices.
- In the event of any incident that may have compromised safeguarding data, the Designated Safeguarding Lead must be notified immediately alongside the standard incident escalation process.
- Any confirmed or suspected disclosure of safeguarding data must be reported to the Local Authority Designated Officer (LADO) and the ICO in addition to standard incident procedures.

CURRENT 2026

17. Implementation Timetable

Phase	Actions and Success Measures
Phase 1, IMMEDIATE (0–30 days)	Commission external cyber security audit for 2025/26. Confirm cyber insurance position. Confirm hardcopy incident contact lists are in place at all schools. Appoint Cyber Security Trustee (if not already done).
Phase 2, Foundation (0–3 months)	Mandate MFA for all administrator accounts. Review backup arrangements and conduct a restore test. Establish Cyber Risk Register. Begin quarterly Board reporting. Establish hardcopy manual continuity procedures at all schools.
Phase 3, Controls (3–6 months)	MFA for all staff. Deploy vulnerability scanning. Approve Incident Response Plan. Launch staff training programme. Complete first phishing simulation exercise (all staff). Confirm supplier register.
Phase 4, Assurance (6–12 months)	Complete external penetration test. Complete internal penetration test. Complete disaster recovery exercise. Achieve Cyber Essentials certification.
Phase 5, Maturity (12–24 months)	Achieve Cyber Essentials Plus. Establish continuous improvement programme. Embed annual strategic cyber review.

18. Annual Trustee Cyber Assurance Statement

The Board shall publish an Annual Trustee Cyber Assurance Statement confirming:

- Cyber risks have been reviewed by the Board during the year.
- An independent external cyber security audit has been commissioned and its findings considered.
- Annual penetration testing (internal and external) has been completed or an explanation provided.
- Critical and high vulnerabilities identified during the year have been addressed or a documented risk acceptance decision made.
- Backup and disaster recovery arrangements have been tested.
- Cyber incidents during the year have been appropriately managed, investigated and reported.
- Staff and trustee cyber security training requirements have been met.
- The Trust's cyber insurance position has been reviewed.
- The Trust remains committed to continuous improvement in cyber security.

The Board confirms that it has challenged, scrutinised and satisfied itself that appropriate governance arrangements exist to manage cyber risk across the Trust.

Where any of the above cannot be confirmed, the statement shall record the reason and the remediation plan.

Approved by the Board of Trustees	Version 2.0, June 2026
Chair of Trustees:	Date: 2 July 2026
CEO:	Next Review Date: June 2026 _____

CURRENT 2026