Character Education Trust

Cyber Security Risk Assessment

& Incident Response Framework

Ratified by	Reviewed by	Date	Date to be reviewed
Trust Board	Finance, Audit, Risk and H&S Committee	March 2026	March 2027

Owner of Policy: CEO / Accounting Officer

Purpose and Context

This framework sets out how the Character Education Trust identifies, manages, and responds to cyber security risks across its schools. It establishes a clear, consistent, and proportionate approach to cyber security as a **strategic operational and safeguarding risk**.

The framework supports the Trust's statutory and regulatory duties under:

- UK GDPR and the Data Protection Act 2018
- Keeping Children Safe in Education (KCSIE)
- ESFA Academy Trust Handbook (risk management and internal control)
- Ofsted expectations regarding safeguarding, leadership, and operational resilience
- Data (Use and Access Act 2025)

The Trust adopts a recognised cyber security framework to protect the **Confidentiality, Integrity, and Availability (CIA)**of information systems and data.

Cyber security is explicitly recognised as a **Trust-level strategic risk** with direct safeguarding, legal, financial, and reputational implications.

Continuous Improvement Statement

The Character Education Trust is committed to **continuous improvement** in cyber security governance and practice.

This appendix evidences the Trust's intention to:

- Regularly review and strengthen cyber controls
- Respond to emerging threats and regulatory expectations
- Develop the policy framework in a structured and proportionate way

These enhancements will be considered as part of:

- Annual policy review
- Post-incident reviews
- Tabletop exercises and assurance activity
- Trustee oversight and challenge

CONTENTS

1. Access Control

The Trust implements robust access control measures to protect systems and data.

1.1 Multi-Factor Authentication (MFA)

- MFA is mandatory for all staff accessing Trust systems where personal, safeguarding, or financial data is held.
- At least two authentication factors must be used.
- In school access may not require 2 factor on login within the internal school systems.
- Access from outside of the UK is switched off by default and requires staff to request access on a 1-2-1 basis. The same standards of access apply.

1.2 Password Standards

All passwords must:

- Meet defined complexity requirements (minimum length, upper- and lower-case letters, and numbers)
- Be changed immediately if compromise is suspected
- Never be reused across Trust and personal systems

1.3 Accountability

- User credentials must never be shared.

Staff are personally responsible for the security of their access credentials

---

2. Trust Cyber Risk Assessment

2.1 Scope of Assessment

The assessment covers all Trust systems, data, people, and suppliers including:

- Management Information Systems (MIS)
- Safeguarding systems (e.g. CPOMS)
- Email and collaboration platforms (Microsoft 365)
- File storage (SharePoint / OneDrive)
- Finance and payroll systems
- Staff and pupil devices
- Backups and disaster recovery arrangements
- Third-party suppliers

2.2 Risk Assessment Methodology

Each risk is assessed using:

- **Likelihood:** Low / Medium / High
- **Impact:** Low / Medium / High
- **Overall Risk Rating:** Derived and recorded in the Trust Risk Register

Impact considers:

- Safeguarding risk
- Data protection impact
- Operational disruption
- Financial loss
- Reputational damage

2.3 Core Cyber Risks (Summary)

Risk	Likelihood	Impact	Mitigation	Owner
Loss or compromise of authentication credentials (phishing/vishing)	Medium	High	MFA, staff training, email filtering	IT Lead
Unavailability of systems/data (e.g. ransomware)	Medium	High	Offline backups, patching, endpoint protection, network segregation	IT Lead
Compromise of safeguarding or personal data	Low	High	Restricted access, encryption, user access reviews	DSL
Supplier compromise	Low	Medium	Due diligence, contractual controls	CFO
Device loss or theft	Medium	Medium	Encryption, remote wipe	IT Lead

3. Cyber Incident Response Plan

The Trust's response to a cyber incident will:

- Protect children and safeguarding information
- Contain and minimise damage
- Meet legal and regulatory duties
- Restore services safely
- Communicate clearly and proportionately

3.2 Incident Roles and Responsibilities

Role	Responsibility
Incident Lead (CEO)	Overall decision-making and escalation
Headteacher	School-level coordination
IT Lead / MSP	Technical containment and recovery
Data Protection Officer	GDPR assessment and ICO liaison
Designated Safeguarding Lead	Safeguarding continuity
Chair of Trustees	Strategic oversight

3.3 Incident Classification

- **Low:** Isolated issue, no data risk
- **Medium:** Systems disrupted, possible data exposure
- **High/Critical:** Safeguarding data, ransomware, prolonged outage

3.4 Immediate Response Actions

1. Isolate affected systems
2. Disable compromised accounts
3. Preserve evidence
4. Notify Incident Lead
5. Engage IT provider and insurer
6. Record all actions

The DFE/ Trust/ Schools do NOT pay ransoms or other requests in kind to release data etc following a cyber-attack or attempted extortion.

3.5 Safeguarding Continuity Arrangements

If digital systems are unavailable:

- DSLs will use offline safeguarding records
- Concerns will be logged using paper forms
- Referrals to external agencies will continue via telephone
- All records will be uploaded once systems are restored

3.6 Data Protection and ICO Reporting

The DPO will determine:

- Whether a personal data breach has occurred
- Whether ICO notification is required (within 72 hours)
- Whether affected individuals must be informed

All decisions will be documented.

3.7 Communications Management

All external communications will be approved by the Incident Lead.

- Staff briefings: factual, timely
- Parent communications: proportionate and accurate
- Media: no comment unless authorised

3.8 Recovery and Review

Following resolution:

- Restore systems securely
- Review root causes
- Update controls and training
- Report to Trust Board

4. Preventative Controls

The Trust maintains the following baseline controls:

- Multi-factor authentication
- Regular, tested backups (including offline)
- Patch management
- Anti-malware and email filtering
- Device encryption
- Role-based access controls
- Annual staff cyber awareness training
- Leaver and joiner procedures

Alignment with **NCSC Cyber Essentials** is maintained.

5. Staff Quick Guide: What To do If you Suspect a Cyber Incident

- Do not click links or open attachments
- Disconnect from the network if advised
- Report immediately to IT and SLT
- Do not attempt to fix the issue yourself
- Follow instructions issued centrally
- Do not communicate about suspected incident to anyone outside school

6. Governance and Review

- Cyber risk is reviewed termly by SLG
- Reported annually to Trustees
- Reviewed after any significant incident

7. Trust Cyber Risk Register Entry (Detailed)

Cyber security is recorded as a **strategic risk** on the Character Education Trust Risk Register.

7.1 Risk Statement

There is a risk that a cyber security incident (including phishing, ransomware, data breach, or supplier compromise) could result in loss or compromise of safeguarding and personal data, disruption to education provision, financial loss, regulatory non-compliance, and reputational damage to the Trust.

7.2 Inherent Risk Assessment (Pre-Control)

- **Likelihood:** Medium
- **Impact:** High
- **Inherent Risk Rating:** High

Impact includes:

- Exposure of child protection and SEND records
- Inability to access safeguarding systems
- Operational disruption or school closure
- ICO enforcement or regulatory scrutiny
- Loss of stakeholder confidence

7.3 Existing Controls

- Trust-wide Cyber Security Risk Assessment
- Multi-factor authentication on core systems (containing personal and financial data as a minimum)
- Secure MIS and safeguarding platforms
- Regular, tested backups (including offline/immutable)
- Patch and update management
- Managed IT service provision
- Staff cyber awareness training (annual minimum)
- Clear joiner / mover / leaver processes
- Supplier due diligence and contractual controls

- Cyber Incident Response Plan (Section 3)

7.4 Residual Risk Assessment (Post-Control)

- **Likelihood:** Low to Medium
- **Impact:** High
- **Residual Risk Rating:** Medium

7.5 Risk Ownership and Oversight

- **Risk Owner:** CEO / Accounting Officer
- **Operational Lead:** IT Lead / Managed Service Provider
- **Safeguarding Oversight:** Designated Safeguarding Leads
- **Governance Oversight:** Trust Board

7.6 Review and Assurance

- Risk reviewed termly by SLG
- Reported annually to Trustees
- Reviewed following any significant cyber incident
- Assurance drawn from audits, incident logs, and training records

---

8. Cyber Incident Response Flowchart (Narrative Detail)

The following section describes, in detail, the decision-making flow during a cyber incident. A visual flowchart may be derived directly from this section for operational use.

8.1 Detection and Initial Alert

A cyber incident may be identified through:

- Staff reporting suspicious emails or behaviour
- Automated alerts from IT systems
- Supplier notifications
- Unusual system behaviour or outages

Any staff member identifying a potential incident must report it immediately to IT and a senior leader.

8.2 Initial Containment (First 0–2 Hours)

- IT isolates affected systems or devices
- Compromised user accounts are disabled
- Network access may be restricted
- Evidence is preserved
- Incident Lead is notified

No unauthorised system restoration should take place at this stage.

8.3 Incident Classification and Escalation (Within 2–6 Hours)

The Incident Lead, with IT and the DPO, will classify the incident as:

- Low
- Medium
- High / Critical

Classification determines:

- Level of senior leadership involvement
- Safeguarding actions required
- External notifications
- Communications approach

8.4 Safeguarding Continuity Decision Point

If safeguarding systems are unavailable:

- DSLs implement offline safeguarding procedures
- Paper records are activated
- External agency referrals continue
- A safeguarding continuity log is maintained

This decision point is prioritised above all other operational concerns.

8.5 Data Protection Assessment (Within 24–48 Hours)

The DPO will:

- Assess whether personal data has been breached
- Determine reportability to the ICO
- Decide whether individuals must be informed
- Document all decisions and rationale

8.6 Communications Decision Point

All communications are approved by the Incident Lead.

- Staff are informed promptly with clear instructions
- Parents are informed only when appropriate and proportionate
- Media enquiries are managed centrally

8.7 Recovery and System Restoration

- Systems restored only after security assurance
- Backups verified before restoration
- Monitoring increased post-restoration

---

9. Cyber Incident Tabletop Exercise Programme

9.1 Purpose

Tabletop exercises test preparedness, decision-making, and communication under realistic conditions. They provide strong evidence of governance maturity and compliance.

9.2 Frequency

- Conducted at least annually
- Conducted following any significant cyber incident
- Additional exercises may be held following system changes

9.3 Participants

- CEO / Incident Lead
- Headteachers (Wrotham and Aylesford)
- DSLs
- IT Lead / MSP
- DPO
- Trust Chair or nominee

9.4 Example Scenario: Ransomware Affecting Safeguarding System

Scenario: A safeguarding system becomes inaccessible during the school day. Staff report ransom messages and file encryption.

Key Discussion Points:

- How is the incident identified and reported?
- Who assumes the Incident Lead role?
- How is safeguarding continuity maintained?
- What communications are issued to staff?
- Is ICO notification required?
- When and how are parents informed?
- How is recovery authorised?

9.5 Outputs and Evidence

- Exercise notes and decisions
- Identified gaps or weaknesses
- Action plan with owners and deadlines
- Report to Trust Board

9.6 Continuous Improvement

Outcomes of exercises are used to:

- Update the risk assessment
- Amend incident response procedures
- Improve training and controls

10. APPENDIX ONE – Staff Training Sheet

(Staff-Facing Guidance)

This document is staff-facing and applies to all employees, volunteers, and contractors working within the Character Education Trust, including Wrotham School and Aylesford School.

This drill sheet explains exactly what staff must do **immediately** if they suspect a cyber security incident. It is designed for use during a live incident or as part of training and drills.

What counts as a suspected cyber incident?

You must treat the situation as a cyber incident if you notice any of the following:

- A suspicious or unexpected email asking you to click a link, download a file, or provide login details
- An email that appears to come from a senior leader or colleague but feels unusual or urgent
- Files that suddenly become inaccessible, encrypted, or renamed
- A ransom message appearing on your screen
- Your device behaving unusually (slow, crashing, pop-ups)
- You believe you may have clicked on a malicious link or attachment
- You believe your login details may have been compromised
- Loss or theft of a Trust device (laptop, tablet, phone, USB)
- Unexpected repeated MFA prompts (aka. MFA bombing or MFA fatigue)
- An unusual telephone call from a colleague or SLT member inquiring about sensitive information These attacks are on the rise and use AI to convincingly copy colleague voices. If in doubt – check via other means.

If in doubt, **treat it as an incident**.

What to do immediately (first actions)
You must do the following immediately:

1. **Stop and do not click anything further**

2. **Disconnect if instructed**
   - If IT or a senior leader advises, disconnect from Wi-Fi or unplug network cables

3. **Report immediately**

   - Report the issue to IT support / Managed Service Provider
   - Inform your line manager or a member of SLT
   - If safeguarding systems may be affected, inform the DSL immediately

4. **Preserve evidence**

What NOT to do

Staff must **not**:

- Do not reply to the email
- Do not delete emails or files
- Do not enter credentials (including passwords)
- Do not attempt to investigate
- Do not Attempt to resolve the issue independently
- Do not Reset passwords unless instructed
- Do not Download or run any software
- Do not Restore files from backups
- Do not Communicate with parents or external parties
- Do not Share screenshots or details on social media or messaging apps
- Do not power off unless specifically told to do so

Uncoordinated actions can make the situation worse and may compromise safeguarding or legal compliance.

Safeguarding during a cyber incident

If safeguarding or pastoral systems are unavailable:

- Continue to respond to concerns in the usual way
- Report safeguarding concerns verbally to the DSL immediately
- Use paper safeguarding forms if instructed
- Do not delay reporting concerns due to system issues

Safeguarding **always takes priority** over IT or operational concerns.

Communications expectations

During a cyber incident:

- All external communications are managed centrally
- Staff must not speculate or share information
- Direct any queries from parents or students to SLT

Clear and accurate communication protects staff, pupils, and the Trust.

After the incident

Once advised that the incident is resolved:

- Follow any instructions regarding password resets or system changes
- Complete any required training or follow-up actions
- Report anything unusual that continues

Training and compliance

- All staff must complete cyber security awareness training annually
- This drill sheet will be used during induction and refresher training
- Failure to follow this guidance may be treated as a disciplinary matter

11. APPENDIX TWO – SLG/SLT Incident Checklist

SLG/SLT Cyber Incident Checklist (Senior Leadership Use)

This checklist is for use by the Strategic Leadership Group (Trust SLG), Senior Leadership Teams (SLT), Headteachers, and Trust leaders at Wrotham School and Aylesford School during a suspected or confirmed cyber incident.

It is designed to be used **in real time**, alongside Section 3 (Cyber Incident Response Plan) and Section 8 (Incident Flow Narrative).

Immediate Actions (First 0–2 Hours)

☐ Treat the issue as a cyber incident until confirmed otherwise
☐ Notify the Incident Lead (CEO / Accounting Officer) immediately
☐ Contact IT Lead / Managed Service Provider
☐ Instruct staff **not** to take independent action
☐ Preserve evidence – do not delete emails, files, or logs
☐ Consider temporary restriction of systems or accounts if advised

Safeguarding Priority Check

☐ Confirm whether safeguarding systems (e.g. CPOMS) are affected
☐ Inform the Designated Safeguarding Lead immediately
☐ Activate safeguarding continuity arrangements if required
☐ Ensure staff know how to report safeguarding concerns offline
☐ Maintain a safeguarding continuity log

Safeguarding considerations must take precedence over operational recovery.

Incident Classification and Escalation

☐ Classify the incident (Low / Medium / High / Critical)
☐ Confirm whether personal data may be involved
☐ Assess potential safeguarding impact
☐ Escalate to Chair of Trustees if Medium or High
☐ Check cyber insurance notification requirements

Data Protection and Legal Compliance

☐ Notify the Data Protection Officer (DPO)
☐ Determine whether a personal data breach has occurred
☐ Assess ICO reportability (72-hour requirement)
☐ Decide whether affected individuals must be informed
☐ Ensure all decisions and rationales are documented

Communications Control

☐ Appoint a single communications lead
☐ Brief staff with clear, factual instructions
☐ Agree parent communications (if required) – timing and content
☐ Manage media enquiries centrally (no unauthorised comment)
☐ Avoid speculation or premature assurances

Operational Continuity

☐ Confirm which systems are unavailable
☐ Agree temporary workarounds where safe and appropriate
☐ Prioritise systems required for safeguarding and attendance
☐ Monitor staff wellbeing and workload during disruption

Recovery and Restoration

☐ Authorise system restoration only after IT security assurance
☐ Confirm backups are clean before restoration
☐ Monitor systems closely post-restoration
☐ Ensure password resets or access changes are completed

Post-Incident Review and Governance

☐ Convene post-incident review meeting
☐ Identify root causes and control weaknesses
☐ Update risk assessment and controls
☐ Agree staff training or policy updates
☐ Report incident and lessons learned to Trustees

12. APPENDIX THREE – Staff Cyber Security Expectations (Supplementary Guidance)

Unless covered by a separate standalone staff policy, the Trust sets out the following **baseline expectations for all staff, volunteers, and contractors**. These expectations apply alongside the Staff Drill Sheet (Appendix One) and are intended to reinforce safe day-to-day practice.

Staff must:

- **Not install software or applications** on Trust devices without explicit approval from IT
- **Not enter personal or safeguarding data** relating to pupils or staff into public or unapproved AI tools (e.g. public versions of ChatGPT or similar platforms)
- **Not use unapproved mass storage devices**, including USB drives or external hard drives
- **Never share login credentials** with colleagues or any third party

Failure to follow these expectations may result in:

- Increased cyber risk to the Trust
- Safeguarding and data protection breaches
- Disciplinary action in line with Trust policies

13. APPENDIX FOUR – Continuous Improvement Aims

Device and Network Security (Planned Expansion Area)

The Trust recognises that device and network security are critical components of cyber resilience and will be expanded into a dedicated section in a future version of this policy.
Future iterations are expected to provide more detailed and prescriptive guidance covering, but not limited to:

Managed Devices

- Security configuration standards for Trust-owned devices
- Centralised management and patching
- Endpoint protection and antivirus controls
- Encryption requirements

Bring Your Own Device (BYOD)

- Expectations for staff using personal devices to access Trust systems
- Minimum security standards for BYOD access
- Restrictions on local data storage
- Conditions under which BYOD access may be restricted or withdrawn

Network Security

- Network segregation between administrative, safeguarding, and pupil networks
- Firewall configuration and monitoring
- Intrusion detection and prevention controls
- Secure remote access arrangements

Backups and Disaster Recovery (Planned Expansion Area)

While backups and recovery arrangements are referenced within this policy, the Trust acknowledges that this area would benefit from greater prescription and clarity as the framework matures.

A future iteration of this policy is expected to include a dedicated section addressing:

- Backup frequency and verification requirements
- Use of offline and/or immutable backups
- Secure backup storage locations (including geographic separation)
- Defined Recovery Time Objectives (RTO)
- Defined Recovery Point Objectives (RPO)
- Clear responsibilities for backup testing and assurance

This development will further strengthen operational resilience and continuity planning.