Good Shepherd Trust
Life in all its fullness

Cyber Security and Resilience Strategy

Meeting Digital and Technology Standards: Cyber Security

Life in all its fullness

About this document

This strategy is in two parts. Part A covers cyber security and preventative measures (the Identify, Protect and Detect pillars of cyber resilience) and is based on the Department for Education's cyber security core standard, part of 'Meeting digital and technology standards in schools and colleges' (updated 10 June 2026), which schools should work towards meeting by 2030.

Part B is a Cyber Response Plan (the Respond and Recover pillars), designed so it can be used independently by the Cyber Recovery Team during a live incident, together with the checklists and appendices at the end of this document.

At the time of publishing the following roles were held:

SLT Digital Lead	NAME
IT Support Lead / Provider	NAME
Data Protection Officer (DPO)	NAME
Trust Board / Governor with IT oversight	NAME

Version History

Version	Version Description	Date of Revision / Review
1	Original, based on the KAHSC Model Cyber Security and Resilience Strategy v3 and the DfE Meeting Digital and Technology Standards — Cyber Security core standard (updated 10 June 2026).	July 2026

This document should not be published externally with contact details included, due to the risk of a data breach. Review annually, and revisit every term to check nothing has significantly changed.

Contents

Part A — Cyber Security and Preventative Measures 3
Part B — Cyber Response Plan 9
Checklist A — Key People 11
Checklist B — Key Roles and Responsibilities 12
Checklist C — Key Contacts 13
Checklist D — Critical Activities and Data Assets 14
Checklist E — Backup Strategy 16
Appendix A — Incident Impact Assessment 16
Appendix B — Communication Templates 17
Appendix C — Incident Recovery Event Recording Form 18
Appendix D — Post-Incident Evaluation 19
Appendix E — Risk Protection Arrangement (RPA) Cover 19

(Right-click the contents above and choose 'Update Field' in Word to populate page numbers.)

Part A — Cyber Security and Preventative Measures

Introduction

The education sector is disproportionately targeted by cyber-attacks compared to other sectors. Cyber security is the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber-attacks. It aims to reduce the risk of an attack and protect against unauthorised access to, or exploitation of, our systems, networks and data.

Cyber incidents and attacks can be an intentional and unauthorised attempt to access, change or damage data and digital technology, made by a person, group or organisation inside or outside the Trust. They can lead to safeguarding issues where sensitive personal data is compromised, a significant data breach, lasting disruption (including school closure), financial loss and reputational damage.

Cyber resilience is our ability to enable business continuity by preparing for, responding to, and recovering from cyber security threats. It is built on five pillars: Identify, Protect, Detect, Respond and Recover. Part A of this strategy concentrates on the Identify, Protect and Detect pillars; Part B sets out our Cyber Response Plan for the Respond and Recover pillars.

The DfE core standard and Cyber Essentials

This strategy follows the Department for Education's (DfE) cyber security core standard, one of six core digital technology standards which schools and colleges should work towards meeting by 2030, set out in 'Meeting digital and technology standards in schools and colleges'. These standards address the core principles of cyber governance, processes and strategy, and are distinct from Cyber Essentials — a government-backed annual certification providing assurance on the technical elements of an organisation's cyber security. Cyber Essentials is a funding agreement requirement for colleges, and while not required for schools, working through this strategy will help the Trust move towards certification if it chooses to pursue it.

Who needs to be involved

The SLT Digital Lead in each school is accountable for, and will prioritise and coordinate, activity relating to this strategy. IT support (whether an internal team or an external provider) is responsible for actioning the technical requirements. The SLT Digital Lead works with:

- IT support, to review outcomes of discussions with key staff and action them within the risk assessment;

- any Trust-wide IT leads, to identify anything needing central action or approval;
- the Data Protection Officer (DPO), who advises on risks to personal and sensitive personal data;
- facilities or estate management, to identify physical security risks affecting core systems and data (for example, a server room door that will not lock);
- the headteacher or principal, who decides on actions suggested by the SLT Digital Lead and IT support;
- school, college or Trust business professionals / the finance team, who help budget and plan for changes, update the risk register, and procure additional services;
- the Local Governing Body and Trust Board, for oversight and strategic risk management — governors and trustees are encouraged to use the NCSC's suggested questions to understand the school's IT estate.

Where technical expertise is not available in-house, the Trust will seek advice from an external support provider, or arrange training for internal IT staff. Where IT support is outsourced, the Trust will discuss with the provider how they meet this standard, including how they mitigate any cyber incident on their own network affecting the Trust's network, and whether they hold Cyber Essentials or Cyber Essentials Plus certification.

Identify

To identify our vulnerabilities, we must understand the hardware and software that make up our IT infrastructure and networks, and the threats these may be exposed to. In conjunction with our IT provider(s), we will:

- maintain an up-to-date inventory of all IT hardware and software used in day-to-day operations, and check it is licensed, supported and updated;
- maintain an up-to-date inventory of all information/data sets the school has access to (see Checklist D), evaluating sensitivity, vulnerability and risk tolerance, and identifying which are critical to business continuity;
- complete a Record of Processing Activities (ROPA) for all systems storing or processing personal and sensitive personal data, using an ICO template where helpful;
- assess staff access and permissions to systems and data, and check password policies;
- check that email is set up securely and reduces the risk of imitation emails from third parties;

- keep network documentation up to date, including network diagrams, changes made, settings and IP addressing information, and agree the level of logging required to help identify the source of any incident;
- regularly review our IT Security Policy and Data Protection Policy to ensure they remain current and reflect emerging threats;
- assess our current security measures against Cyber Essentials requirements — firewall rules, secure device configuration, security update management, user access control and malware protection — as a baseline standard we will strive to meet;
- understand our greatest cyber risks and the likelihood and impact of each, capture how many incidents have already occurred to identify common themes, and identify pupil or staff behaviour that could expose the school to risk (for example, downloading an unapproved application);
- create a simple reporting structure so cyber risks are captured, escalated, actioned and placed in the risk register and a regularly tested business continuity plan, with documentation held in at least one diverse location (for example, in the cloud and as a hard copy), and any risks flagged to governors or trustees.

A cyber risk assessment should be completed as soon as possible and repeated annually, or following significant technology or process changes or an incident. Assessments should then be revisited every term to check whether anything has significantly changed.

Protect

Once we understand the scope of our IT infrastructure, we can develop and implement protection measures to mitigate or reduce our vulnerability. In conjunction with our IT partner(s), we will ensure the following safeguards are in place:

- all devices on every school network are protected by a properly configured boundary or software firewall;
- all devices that can access the network (including personal devices where permitted) are known, recorded, and have security features enabled, correctly configured and kept up to date;
- account holders only have the access they require to perform their role;
- users are authenticated with unique credentials, including strong passwords, before accessing devices or services;
- account holders with access to personal or sensitive operational data and functions are protected by multi-factor authentication (MFA);

- anti-malware software protects all devices on the network, including cloud-based systems;
- an administrator checks the security of all applications before they are downloaded onto the network;
- all online devices and software are licensed and patched with the latest security updates;
- we hold at least 3 backup copies of important data, on at least 2 separate devices, with at least 1 copy off-site and at least 1 offline at any time, tested regularly to confirm services can be restored;
- our Cyber Response Plan (Part B) is regularly tested, communicated to all those likely to be affected, and key staff know their roles and responsibilities in advance of any incident;
- our measures comply with the requirements of the Risk Protection Arrangement (RPA) or our insurers, as applicable;
- we report any suspicious cyber incident to the relevant agency — Report Fraud, the DfE sector cyber team, the ICO and/or the NCSC — depending on the type and severity of the incident;
- we complete a Data Protection Impact Assessment (DPIA) for personal data we hold, as required by UK GDPR;
- all employees and governors with access to the school's IT system complete NCSC Cyber Security Training annually, with certificates held centrally as evidence for any RPA claim;
- trustees and governors ask pertinent questions to assure themselves of the school's cyber risk position, for example using the NCSC's guidance for governors and trustees;
- we make use of free resources from SWGFL and the NCSC, including the CyberSecure Check for Schools tool, and support available from the North West Cyber Resilience Centre;
- all users have read the relevant policies and signed IT acceptable use (and device loan, where applicable) agreements;
- accounts are disabled as soon as someone leaves the Trust;
- staff are made aware that an incident caused by misuse could give rise to disciplinary measures and referral to the police.

Technical requirements: Firewall

- Protect digital technology with a correctly configured boundary firewall or software firewall, including protection against denial-of-service attacks.
- Keep firewall firmware up to date and on supported versions, checked termly.

- Ensure all external connections run through the firewall; change default administrator passwords and restrict remote access to those who need it for maintenance.
- Protect the firewall's administrative interface with MFA where available, and prevent internet access except for those who maintain it.
- Actively monitor firewall traffic and enable alerts to help detect suspicious activity; block inbound unauthenticated connections by default.
- Document and review, at least termly, why inbound traffic has been permitted, signed off by the SLT Digital Lead, and keep firewall rules to an absolute minimum.
- Enable a software firewall for devices used outside school (for example, at home or on public wifi), and consider a VPN to encrypt data in transit.

Technical requirements: Anti-malware and security checks

- Anti-malware software must scan web pages as used, scan files and applications on access/download, scan email attachments, and send alerts to IT support for investigation.
- Anti-malware software must have a centralised monitoring console and prevent access to potentially malicious websites.
- USB storage devices are prohibited by default unless required for a specific need (for example, exam board requirements); permitted USB drives are scanned before use.
- IT support checks downloads for malware before installation, approves all current and future applications, maintains a current list of approved applications, and only installs software verified as coming from a known supplier.
- Browser settings are reviewed to ensure the highest level of protection and prevent users installing extensions or bypassing security features.
- Email is set up securely to reduce the risk of imitation (spoofed) emails from third parties.

Technical requirements: Passwords and multi-factor authentication

- Enforce password strength at system level — the NCSC suggests machine-generated passwords or a three random word approach.
- Immediately change any password that has been, or is suspected to have been, compromised.
- Protect all passwords, for example by allowing no more than 10 guesses in 5 minutes, or locking devices after no more than 10 unsuccessful attempts.

- Use a password or PIN of at least 6 characters to physically access network switches and boot-up settings.
- Senior leaders, and staff (including IT support) working with confidential, financial, personal or sensitive personal data, must use MFA, combining at least 2 of: a password, a text message code (staff only), an automated phone call, a secure portable device, a security key, a trusted-account authentication, or a biometric test.
- Where MFA is not available, a more complex password should be used. For younger pupils, those with SEND, or EAL, consider alternative logon methods such as a PIN, or a teacher-supervised account that still identifies the pupil, in line with the Trust's filtering and monitoring standards.

Technical requirements: Account management

- Disable accounts as soon as someone leaves; maintain a joiners/movers/leavers process with HR and business professionals, ideally linked to the MIS.
- Ensure students and staff only have access to the data and systems they need.
- Apply MFA to accounts and cloud-based applications for staff working remotely or away from school; disable remote access when not required.
- Review accounts with business professionals every term to identify changes that may have been missed, including suspending or deleting unused accounts.
- Ensure global or administrative accounts are not used for routine business; dedicated accounts with enhanced privileges are used instead, with changes approved by a member of SLT or a trustee before IT support actions them.
- Ensure SLT have access to a dedicated administrative account for emergencies where IT support is unavailable.

Technical requirements: Licensing and security updates

- All software must be licensed and eligible for security updates; unlicensed software is removed or licensed.
- Licence expiry dates are recorded in the contracts register, and end-of-support dates for operating systems are captured in the asset register.
- Vulnerability fixes (patches, updates, configuration changes, vendor scripts) are applied within 14 days of release where the vendor describes the vulnerability as critical or high risk, where it scores 7.0 or above on the CVSSv3.1 scale, or where the vendor gives no severity rating.
- Where DfE issues instructions on security updates, IT support applies these within 5 working days of notification.

- Where a high-risk patch is unavailable, the affected device is isolated from the network or separated from higher-risk systems and data.

Detect

Early detection of cyber threats significantly reduces their impact on our IT infrastructure and helps preserve business continuity. We will:

- install and regularly update anti-malware software to help detect and mitigate the effects of an attack;
- deliver cyber security training to all staff and governors to heighten awareness and encourage prompt reporting of potential breaches;
- use the NCSC's Exercise in a Box toolkit to help staff understand what an attack might look like and to test our response plans;
- register with Police CyberAlarm, connecting the school to the local police cyber protect team and, where installed, a free monitoring tool that records network traffic without risk to personal data;
- as soon as an attack is detected, work with our IT partner(s) to evaluate and continuously monitor affected systems, and initiate our Cyber Response Plan (Part B) by convening the Cyber Recovery Team.

Part B — Cyber Response Plan

Introduction and aims

This Cyber Response Plan forms part of our overall Emergency Plan, and covers all essential and critical IT infrastructure, systems and networks. Its aim is to ensure we can effectively deliver the Respond and Recover pillars of our cyber resilience strategy, giving staff and key stakeholders a clear understanding of who to contact and what actions to take to minimise disruption and restore normal business functioning.

The Plan sets out who is involved in the Cyber Recovery Team, key roles and responsibilities, which data assets are critical and how long we can function without each, and our internal and external communications approach. This will help the Trust to: take immediate and appropriate action; enable prompt internal reporting; have immediate access to relevant contacts; maintain pupil and staff welfare; minimise disruption; respond consistently; restore functionality as soon as possible; and report incidents to the relevant authorities.

Respond — actions in the event of an incident

Speed is critical during a cyber incident. The DfE Cyber Security Hub contains advice on what to do during a live attack. Where we suspect, or are informed, that we have been the victim of ransomware or another cyber incident, we will take the following steps immediately:

1. Convene the Cyber Recovery Team.
2. Verify the initial incident report as genuine and record it on the Incident Recovery Event Recording Form (Appendix C).
3. Assess and document the scope of the incident using the Incident Impact Assessment (Appendix A) to identify which key functions are operational and which are affected.
4. Start the Actions Log to record actions taken.
5. Contact the RPA Cyber Emergency Assistance 24-hour helpline (0800 368 6378, or RPAresponse@CyberClan.com), where a guaranteed response within 15 minutes can be expected, incident information recorded, and, subject to a valid claim, an expert Incident Response team deployed.
6. Ask our IT partner(s) to isolate affected devices from the network.
7. To assist data recovery, ensure staff do not turn off electrical power to any computer, try to run a suspect hard drive/backup disc or tape, or tamper with or move damaged computers, discs or tapes.
8. Decide, in liaison with the Trust, whether it remains safe for the school to stay open.
9. Identify legal obligations and any required statutory reporting, for example to the ICO in the event of a data breach, involving the DPO and, where relevant, the police.
10. Execute the communications strategy, including a media/press release if applicable — communications with staff, governors and parents/pupils should precede any media release.
11. Contact the local police via the Report Fraud website or on 0300 123 2040.
12. Contact our Data Protection Officer.

Recover — restoring data and services

Once the initial threat is contained, quarantined or removed, we will begin restoring normal business functions. The NCSC's step-by-step guide to recovering hacked accounts may help. We will:

13. Continue to liaise with the RPA Incident Response Team or our insurance provider for advice.
14. Check email accounts for unwanted forwarding rules.

15. Contact account contacts to advise that an email or social media account has been compromised, and to treat recent messages from it with suspicion.
16. Change passwords for any hacked account, and any account sharing the same password.
17. Agree a process with our IT partner(s) for safely restoring affected systems and databases.
18. Maintain the Actions Log to record recovery steps and monitor progress.
19. Maintain dialogue with IT partner(s) to estimate recovery time and likely impact.
20. If money has been lost, inform the bank and report it to Report Fraud.
21. Keep stakeholders informed of progress and likely timescales.

Post-incident evaluation

Once the Respond and Recover processes are complete, we will evaluate the effectiveness of our response using the Post Incident Evaluation form (Appendix D) and review this Plan accordingly. In particular, we will consider whether any information or data would have significantly helped our response but was difficult or impossible to obtain, and plan to gather this ahead of any future incident. We will communicate findings to staff and key stakeholders, and keep this Plan up to date with new suppliers, contact details and policy changes.

Checklist A — Key People

Cyber Recovery Team

In the event of this plan being initiated, the following personnel will form the Cyber Recovery Team:

Role	Name	Role in School	Contact Details
Recovery Team Leader			
Data Management			
IT Restore / Recover			
Site Security			
Public Relations			
Communications			
Resources / Supplies			

Facilities Management			

Server and MIS admin access

Record all people with administrative access to the server and to the Management Information System (MIS):

Role	Name	Contact Details
Headteacher		
School Business Manager		
IT Support Technician		
Third Party IT Provider		
MIS Provider		

It is also helpful to consider in advance how staff would access registers, staff/pupil contact details, and current child protection concerns if systems were unavailable.

Checklist B — Key Roles and Responsibilities

Every school is unique, and the structure and staffing levels will determine who is assigned which task. This checklist is not exhaustive.

Headteacher / SLT Digital Lead

- Seeks clarification from the person notifying the incident and sets up an incident log.
- Convenes the Cyber Recovery Team, liaises with the Chair of Governors and the DPO.
- Informs staff and prepares statements/letters for media, parents and pupils.
- Liaises with the School Business Manager on contacting parents, and ensures site access for external IT staff.

Designated Safeguarding Lead (DSL)

- Establishes whether there is a safeguarding aspect to the incident.
- Considers whether a referral is required to Cyber Protect Officers, Early/Family Help, or the local Safeguarding Hub/MACH.

School Business Manager

- Ensures phone lines and mobiles are operative and numbers are communicated to relevant staff.

- Ensures office staff understand the standard response and know the media contact.
- Contacts the RPA/insurance provider and IT support; manages parent communications; assesses impact on payroll/HR.

Data Protection Officer (DPO)

- Uses the data map and information asset register to assess whether data has been put at risk, lost, or is beyond reach.
- Liaises with the Headteacher/Chair of Governors and determines whether a report to the ICO is necessary.

Chair of Governors / Trust Board

- Supports the Headteacher and ensures decisions are based on sound judgement and advice.
- Has a process to approve additional funds if required, and ensures governors do not comment to third parties or the media.
- Reviews the response after the incident to consider changes to working practice or policy.

IT Provider

- Verifies the most recent successful backup and, liaising with the RPA/insurer's Incident Response Service, restores it.
- Advises on the likely cost of repair/restore, provides a downtime estimate, and protects unaffected records.

Teaching staff and teaching assistants

- Reassure pupils within the agreed standard response, and record any relevant information pupils provide.
- Follow any temporary procedures for data storage or IT access.

Checklist C — Key Contacts

Suppliers

Supplier	Contact / Tel Number	Account / Reference Number
Internet Connection		
Backup Provider		
Telecom Provider		
Website Host		

Electricity Supplier		
Burglar Alarm		
Text Messaging System		
RPA Cyber Emergency Assistance	0800 368 6378	
Report Fraud	0300 123 2040	
Local Constabulary	101	
Legal Representative		

Staff media contact and standard responses

Assigned staff will co-ordinate with the media, working to pre-approved guidelines. The media contact should only provide verified facts — 'I don't know at this stage' is an acceptable response while details are confirmed. Likely questions will include what happened, how it happened, and what the school is doing about it. Staff without delegated media responsibility should not respond to enquiries and should refer callers to the assigned staff member.

The information provided should be factual, including the time and date of the incident. Staff should not speculate on restoration timescales unless one has been agreed, and should direct further enquiries to the assigned contact, website, or other pre-determined route. For pupils, staff should reassure them that incidents are well prepared for, that alternative arrangements are in place, and that systems will be back online shortly, without speculating on timescales unless authorised to share them.

Name	Role
	Headteacher
	Chair of Governors

Checklist D — Critical Activities and Data Assets

List the data assets each school has access to, and decide which are critical and how long the school could function without each one (for example: 4 hours / 12 hours / 24 hours / 48 hours / 72 hours / 1 week / 2 weeks / 1 month). Note any temporary workaround, referring to the Inventory / Data Map where helpful.

Category	Data / System	Recovery Timescale	Workaround?

Leadership and Management	Access to the headteacher's / SLT digital lead's email		
Leadership and Management	Minutes of SLT meetings and agendas		
Leadership and Management	Head's / SLT reports to governors (past and present)		
Leadership and Management	Key stage, departmental and class information		
Safeguarding / Welfare	Systems which report and record safeguarding concerns		
Safeguarding / Welfare	Attendance registers		
Safeguarding / Welfare	Referral information / outside agency records		
Safeguarding / Welfare	Child protection records		
Safeguarding / Welfare	Looked After Children (LAC) records / PEPs		
Safeguarding / Welfare	Pastoral records and welfare information		
Medical	Medical conditions information and administration of medicines record		
Medical	First aid / accident logs		
Teaching	Schemes of work, lesson plans and learning platform access		
Teaching	Pupil reports and parental communications		
SEND Data	SEND list and records of provision, including EHCPs		
Conduct and Behaviour	Behaviour and reward system records, sanctions and exclusions		
Assessment and Exams	Exam entries, results, targets and tracking data		
Governance	School development plans, policies and governor records		
Administration	Admissions, transfers, contact details and census/statutory return data		

Human Resources	Payroll, staff attendance and disciplinary records		
Office Management	Email, MIS, website, social media and payments systems		
Site Management	Visitor sign-in, CCTV, maintenance logs and risk assessments		
Catering	Supplier contacts, payment records and dietary/allergy information		

Checklist E — Backup Strategy

School Process	Backup Type (on-site / off-site)	Frequency
Main File Server		
School MIS		
Cloud Services		
Third Party Applications / Software		
Email Server		
Curriculum Files		
Teaching Staff Devices		
Administration Files		
Finance / Purchasing		
HR / Personnel Records		
Inventory		
Facilities Management / Bookings		
Website		
USBs / Portable Drives		

Appendix A — Incident Impact Assessment

Understanding the type and severity of an incident allows the Trust to determine how urgent the response needs to be, and ensures the correct people are involved from the outset.

Operational Impact	Description
No Impact	There is no noticeable impact on the school's ability to function.
Minor Impact	Some minor loss of ability to function; work takes longer with a loss of efficiency.
Medium Impact	Loss of some critical services to some users; workarounds are possible with planning.
High Impact	No critical services can be provided; school closure or considerable disruption is likely.
Informational Impact	**Description**
No Breach	No information has been accessed, compromised or lost.
Data Breach	Access or loss of non-personal data, e.g. action plans or policies.
Personal Data Breach	Sensitive personal data accessed or extracted; report to the ICO within 72 hours if significant impact is likely.
Integrity Loss	Data, potentially including sensitive personal data, has been changed, deleted or corrupted.
Restoration	**Description**
Existing Resources	Recovery can be promptly facilitated with resources readily available.
Facilitated by Additional Resources	Recovery is possible within an identified timescale with additional, easily accessed resources.
Third Party Services	Recovery is not guaranteed and requires outside services.
Not Recoverable	Recovery is not possible; data may be extracted, encrypted, or backups may have failed.

Appendix B — Communication Templates

The following templates provide a starting point for communications during an incident. Bracketed text should be adapted to the circumstances.

1. School remaining open — letter to parents/carers

Confirms the school has identified a cyber-attack or serious system outage affecting some or all IT systems (for example telephones, email, server or MIS); that the Trust is liaising with its DPO and will report to the ICO if required; that a risk assessment has been completed with the Trust to address safeguarding concerns; that the school will remain open with any necessary changes described; and how further updates will be shared.

2. School closure — letter to parents/carers

As above, but confirms that, following a risk assessment completed with the Trust, the school will close to pupils from a stated date, with an expected reopening date, and an apology for the disruption to childcare arrangements.

3 & 4. Staff statements (school open / school closed)

Describes the incident and affected systems, confirms any workarounds or remote learning arrangements, confirms DPO involvement and ICO reporting where necessary, reminds staff not to comment to the press, parents or wider community, and directs queries to the assigned staff contact.

5. Media statement

A short factual statement confirming the date of the incident, whether the school remains open or is closed, that the Trust's DPO is involved and the ICO will be informed where necessary, and that the incident is being investigated with remedial action under way. Staff should reflect only information already made public by the school.

Appendix C — Incident Recovery Event Recording Form

Used to record key events completed while following the stages of this Cyber Response Plan.

Field	Detail
Description or reference of incident	e.g. malware, denial of service, phishing, data breach, targeted attack, insider action, unauthorised access
Date of the incident	
Date of the incident report	
Date/time incident recovery commenced	
Date recovery work was completed	
Was full recovery achieved?	

Relevant referrals

Referral To	Contact Details	Contacted On	Contacted By	Response

Actions log

#	Recovery Task	Person Responsible	Completion Date (Est. / Actual)	Comments	Outcome
1					
2					
3					
4					
5					

Appendix D — Post-Incident Evaluation

Grade each action 1–5 (1 = poor, ineffective and slow; 5 = efficient, well communicated and effective).

Action	Response Grading	Comments for Improvement / Amendments
Initial incident notification		
Enactment of the action plan		
Co-ordination of the Cyber Recovery Team		
Communications strategy		
Impact minimisation		
Backup and restore processes		
Were contingency plans sufficient?		
Staff roles assigned and carried out correctly?		
Timescale for resolution / restore		
Was full recovery achieved?		

Record any requirements for additional training and suggested changes to policy or procedure arising from this evaluation.

Appendix E — Risk Protection Arrangement (RPA) Cover

Since April 2022, the Risk Protection Arrangement (RPA) has included cover for cyber incidents, defined in the RPA Membership Rules as any actual or suspected unauthorised access to computer hardware, electronic data processing equipment, microchips or computer installations that process, store, transmit, retrieve or receive data. RPA cover includes a 24/7 dedicated helpline and email address; in the event of a cyber incident, contact RPA Emergency Assistance (see Checklist C).

To be eligible for RPA cyber cover, the Trust must meet four conditions:

22. Hold offline backups, ideally following the NCSC's 3-2-1 rule: the right data is backed up, backups are held fully offline (not connected to systems, or in cold storage), and backups are tested regularly to confirm services and data can be restored.
23. Ensure all employees and governors with access to the school's IT system complete NCSC Cyber Security Training, with certificates retained as evidence for any claim.
24. Register with Police CyberAlarm, using the code 'RPA Member' when signing up.
25. Have a Cyber Response Plan in place — this document, and its accompanying checklists, fulfils that requirement.

For full terms and conditions, refer to the relevant RPA Membership Rules on GOV.UK.