Brighter Futures
Educational Trust

CYBER SECURITY POLICY

Policy Number: 88
Review Committee: ELT
Type of Policy**:** Non - Statutory
Review Period: Annually
Approved: September 2026
Next Review: September 2027

VERSION CONTROL

V1.1	September 2025	New Policy
V1.1	September 2026	Changes to job titles and grammatical changes. Policy reviewed and updated to reflect current cyber security arrangements, roles and responsibilities, infrastructure and security controls, supplier requirements, access controls, monitoring, training and incident response processes. Updates also align the policy with current DfE, NCSC, Cyber Essentials and other relevant cyber security guidance, and clarify links with related Trust policies and procedures.

CONTENTS

1. Purpose
2. Scope
3. Cyber Security Framework
4. Sources of Best Practice and Guidelines
5. Suppliers, Contractors and Third-Party Providers
6. Strategy and Approach to Cyber Security
7. Roles and Responsibilities
8. Data Protection and Privacy
9. Infrastructure Security
10. Authentication and Access Control
11. Monitoring and Alerting
12. Cyber Training and Awareness
13. Incident Response Plan
14. Change Management
15. Acceptable Use of Technology
16. Compliance and Regulatory Requirements
17. Cyber Security Insurance
18. Policy and Framework Review and Updates
19. Co-operation Between Functions
20. Enforcement and Disciplinary Actions
21. Links with Other Policies

1. PURPOSE

The purpose of this policy is to establish guidelines for securing Brighter Futures Educational Trust and its schools. The policy covers the IT systems, both on-premises and in the cloud, data, and the protection, privacy and safety of students, staff, and all other stakeholders. This policy aims to provide practical systems and processes that will mitigate the risks associated with the latest cyber threats, such as data breaches, malware, and unauthorised access. The policy is based around a formalised cyber security framework that aligns itself with the guidelines provided by the government, DfE and other internationally accepted standards.

2. SCOPE

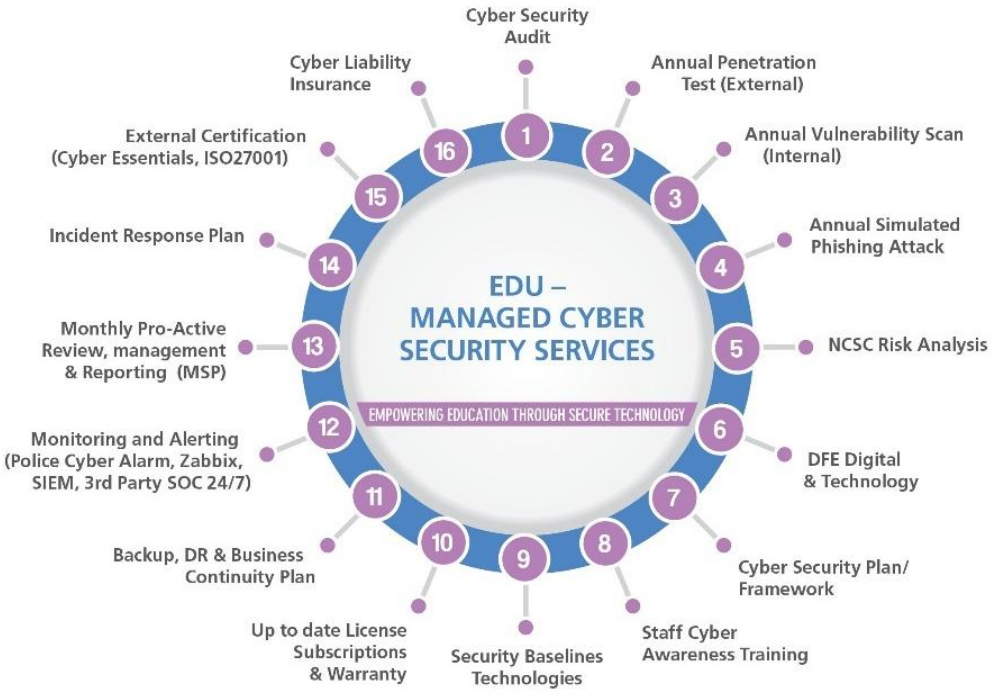
This policy applies to all students, parents/carers, trustees, members, staff, administrators, contractors, and third-party service providers who have access to the trust's systems and data including but not limited to:

- Trust-owned computers and devices
- Personal devices used to access trust systems and data (restricted to members, trustees and governors)
- On premises systems and infrastructure
- Online platforms and cloud services
- The Microsoft 365 Tenant
- User directories and security permissions systems such as Active Directory and Entra ID
- The Management Information Systems
- Financial and payment systems
- The backup and disaster recovery systems

3. CYBER SECURITY FRAMEWORK

Cyber security systems, processes and reporting are based on the following framework which is in turn based on the guidelines from the DfE, NCSC, RPA and CIS. The framework ensures a structured and comprehensive approach to cyber security.

16 Step Cyber Security Framework



4. SOURCES OF BEST PRACTICE AND GUIDELINES

DfE – The Department for Education has released the updated Digital and Technology Standards which clearly describe the cyber security requirements for schools and colleges.

Meeting digital and technology standards in schools and colleges - Guidance - GOV.UK

NCSC – National Cyber Security Centre is a government organisation that plays a key role in safeguarding the United Kingdom's critical infrastructure, public sector organisations, and private businesses against cyber threats. It is part of GCHQ (Government Communications Headquarters)**,** the UK's intelligence and security agency, and serves as the primary authority on cybersecurity, advising government departments, the DfE, schools and businesses.

RPA - The Risk Protection Arrangement (RPA) for schools in the UK, offered by the Department for Education (DfE)**,** provides a government-backed alternative to commercial

insurance for schools. Under RPA, the UK government covers the losses instead of the commercial insurance.

CIS – The Centre for Internet Security (CIS) is an independent, non-profit organisation that develops internationally recognised cyber-security best practices. Its CIS Critical Security Controls provide a prioritised set of safeguards to help organisations reduce common cyber risks, while the CIS Benchmarks provide secure configuration guidance for operating systems, cloud platforms, applications and network devices. For schools and trusts, CIS provides a practical framework for implementing and evidencing technical controls that support DfE standards, NCSC guidance and data-protection obligations.

5. SUPPLIERS, CONTRACTORS AND THIRD-PARTY PROVIDERS

Management of suppliers, contractors and third-party providers is critical, as external relationships can introduce security risks or lead to data breaches if not properly managed. The Trust can assume that the cyber security of suppliers or providers is in place and fit for purpose.

The Trust's approach is as follows:

Assess the cyber security risk of critical and / or relevant suppliers. Perform a risk assessment to understand the cyber risks introduced by each third party and evaluate their ability to meet the trust's cyber security requirements.

Where possible, third-party contracts will contain cyber security clauses within that clearly define the roles and responsibilities of both parties in maintaining the confidentiality, integrity, and availability of data.

All suppliers must have a cyber security framework in place and clear guidelines on backup and disaster recovery processes and systems. The Trust will request that suppliers share this information, so that it can be reviewed and documented internally.

Ideally, all suppliers that have access to systems or data will have a form of formalised cyber security framework or process in place such as:

- Cyber Essentials (a UK government-backed certification that sets out basic security controls)
- ISO 27001 (Information Security Management Systems)
- NIST Cybersecurity Framework (National Institute of Standards and Technology)
- GDPR (General Data Protection Regulation) compliance.

Access to data and sensitive information will be managed on a least privilege basis and restricted to only what is needed in order to fulfil the supplier service or contract.

The incident response plan addresses supply chain risks and the Trust approach to a supplier experiencing an attack or breach.

We must ensure that there is a clear exit and transition plan for any supplier or provider.

6. STRATEGY AND APPROACH TO CYBER SECURITY

Our Trust's Managed Service Provider (MSP) uses the following approach for cyber security:

Cyber Defence

Ensuring there is the minimum baseline of technologies in place to protect data, creating the minimum layers of defence needed.

Cyber Readiness

Maintaining and testing systems to ensure that they are up-to-date and fit for purpose.

Cyber Recovery

Ensuring that there is a disaster backup plan addressing cyber risk. Deploying the plan is an IT task, incorporating the latest government requirements for offsite/offline backups not kept on the main network.

Cyber Certification

Cyber Essentials is a government recommended certification, providing the Trust, schools, staff and other stakeholders with peace of mind that systems and processes have been externally vetted.

7. ROLES AND RESPONSIBILITIES

Cyber Security Management Team

The first key step to a cyber security framework is to assign key roles and responsibilities. The team includes the Extended Leadership Team (ELT) members responsible for IT, the MSP Virtual IT director, MSP lead engineer and MSP junior technician.

CEO	
Director of Finance and Resources (DF&R)	
	MSP Virtual IT Director/CISO
	MSP Lead Engineer
	MSP Level 1 ICT Engineer

ELT – Executive Leadership Team

The leadership team must fully inform the trustees of the cyber security posture, and they must treat cyber security as a critical topic. It is responsible for setting the tone and ensuring that there is management buy in. Importance must be placed on implementation and maintenance of the cyber security framework, policies and procedures which are in place, and fostering a culture of cyber security awareness across the Trust.

The Director of Finance and Resources has oversight of the cyber security framework, how it's managed and the team's responsibilities.

The ELT approves core plans, polices and processes such as:

- The Cyber Security Framework
- Cyber Security Policy
- Incident Response Plan
- Backup, Business Continuity and Disaster Recovery Plan.
- New systems and processes, with consultation from the Virtual IT Director/CISO.

The Director of Finance and Resources performs the critical higher-level function of ensuring support and adoption of the cyber security framework, policies and processes across the Trust.

IT and Cyber Security MSP

Virtual IT Director / CISO (Cyber Security Consultant)

- Creates the cyber security methodology based on best practice
- Determines the best practice bodies used for guidance.
- Staying up to date on the latest best practice and Digital and Technology Standards.
- Audit and reviews of IT and cyber security systems and processes.
- Creation of controls and reporting for the cyber security function.

- Provides advice and support for the ELT.
- Is responsible for managing the change control process.
- In partnership with the Director of Finance and Resources, creates policies and processes that feed the cyber security framework.

MSP Lead Technical Engineer

- The Lead MSP Engineer takes responsibility for carrying out the monthly controls checklist (Cyber Security Framework Report) and submitting the results to the cyber security management team.
- Reviews logs and system alerts.
- Is responsible for the configuration, installation and updates for IT and cyber security systems.
- Provides escalation support as an expert engineer, who is trained by the security vendors.
- Responds to and mitigates security incidents.
- Regularly scans and reviews the systems for vulnerabilities and updates and patches systems to address known vulnerabilities.
- Implements and manages firewalls, end point security, Office 365 security and other cyber security systems.

MSP Level 1 ICT Engineer

- Looks after the daily ICT operations and daily cyber security tasks.
- Assists the lead technical engineer in carrying out investigations and remedial tasks.
- Assists with educating and advising staff regarding security best practice.

Staff, Students and other Stakeholders

All stakeholders are responsible for:

- Adhering to this policy.
- Following best practices for secure use of technology, including strong passwords and Multi-Factor Authentication (MFA).
- Adhering to the Trust ICT and Internet Acceptable Use Policy.
- Reporting any suspicious activity or potential security incidents to the IT department immediately.
- Ensuring that all sensitive data is securely stored, processed and transmitted.
- Staying aware of threats and using the systems in a responsible and secure way.
- Never sharing any confidential information, usernames or passwords.

Controls, Reporting and Review

Cyber security is not a one-time check; it's an ongoing process. Continuous monitoring and regular auditing to ensure that systems remain secure and compliant.

Examples of the reporting in place:

- Quarterly IT Management Report
- Monthly Cyber Security Framework Controls Report
- Police Cyber Alarm Report (threat analysis and response)

The systems and framework components are checked monthly by the MSP lead engineer, and are documented in the cyber security framework controls report.

The report is shared with the Trust and MSP management team.

This policy will be clearly communicated with all staff and form a key component of the cyber security process during new starter induction.

8. DATA PROTECTION AND PRIVACY

Data Encryption

All Windows based machines are encrypted and the information is saved on the MS365 Tenant.

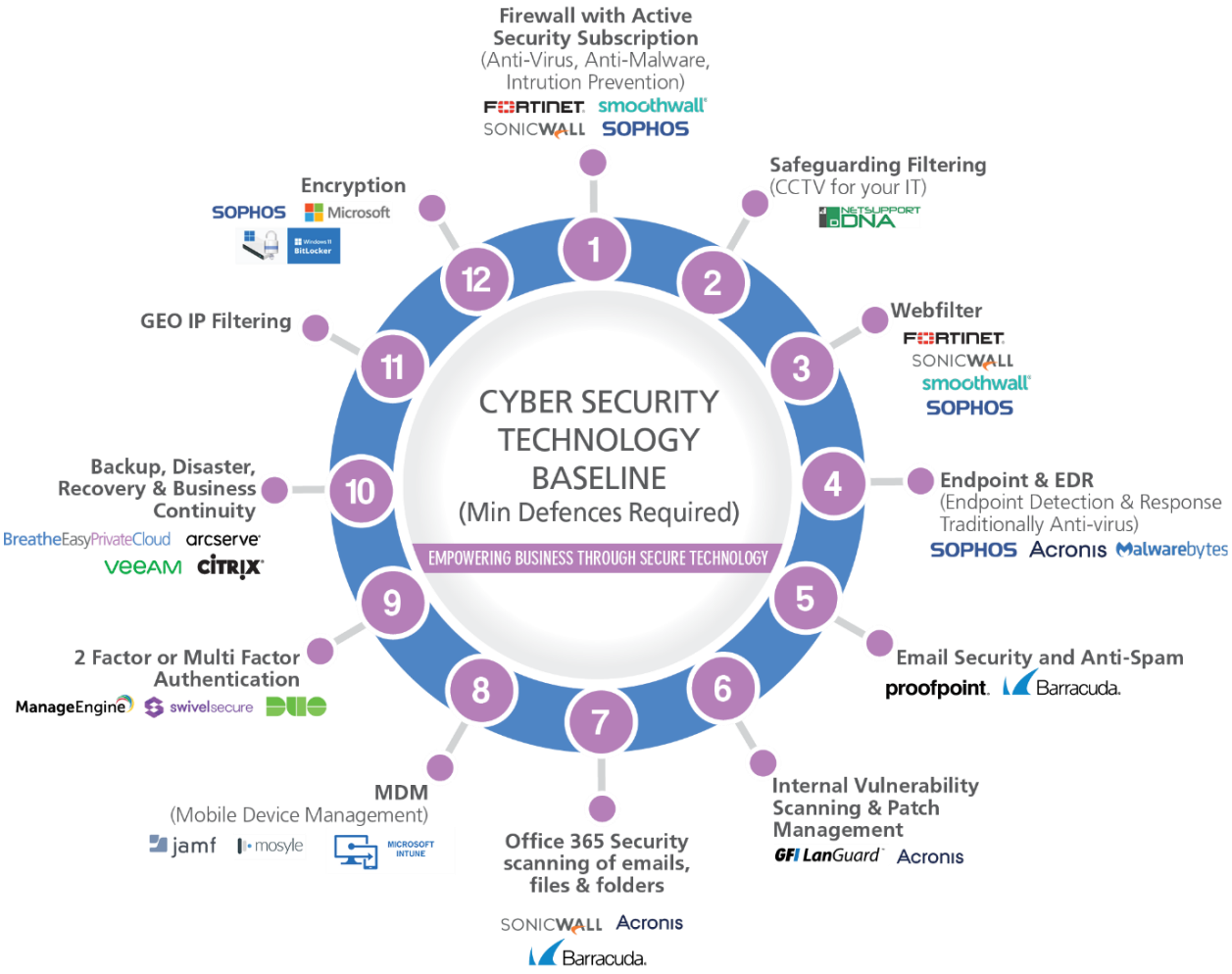
Backup data that is sent to the offsite/ offline backup is encrypted in transit and at rest.

Regular use of USB memory sticks is discouraged, but in the event that these are used for a specific purpose, then data must be encrypted.

When sending any confidential information via email, staff should use the built-in encryption functionality in Microsoft Outlook. Please refer to our Data Protection Policy for further information.

9. INFRASTRUCTURE SECURITY

Cyber Security Baseline Technologies



The cyber security baseline technologies are a set of technology categories that are defined in the cyber security framework as the minimum layer of defences that the Trust requires. This list is by no means exhaustive and is likely to expand as new threats arise.

All cyber security technologies used by the Trust must have an active subscription for updates and security definitions. Vendor support and warranty is essential.

The following technology categories are in place:

Firewalls and Intrusion Detection

All schools within the Trust have network perimeter protection in place via firewalls with an active security subscription that includes:

- Real-Time Malware and Virus Protection
- Intrusion Detection and Prevention (IPS/IDS)
- Access to a regularly updated malware and virus global database

- Secure inspection of SSL encrypted traffic

Safeguarding Filtering

A safeguarding filtering system is implemented at all schools across the Trust. This system can monitor user activity and identify safeguarding risks across applications used on trust-managed devices. For example, the system can detect concerning phrases typed into emails or Microsoft Teams chats.

Web Filtering

Web content filtering is in place at the network perimeter of each school and on all student devices. The solution includes reporting and alerting capabilities. The MSP support team collaborates closely with each school's safeguarding lead.

Filtering systems must be:

- Approved by 360 Degree Safe and the Internet Watch Foundation
- Compliant with the most recent Keeping Children Safe in Education (KCSIE) guidelines

End Point Protection

All trust-owned servers and workstations are protected by an endpoint protection solution with an active subscription, which features in the Gartner Magic Quadrant. This ensures consistent protection from malware, viruses, and other endpoint threats.

Email Security

Emails are hosted via Microsoft 365, which is considered a significant threat vector. Therefore, the Trust email systems are protected with a security solution that can provide the following:

- **Threat Protection:** Emails are scanned for SPAM, phishing, social engineering, malware, and other forms of attack.
- **Email Authentication**: To protect against email spoofing and to ensure email authenticity, the Trust has implemented DMARC, DKIM and account takeover protection.

Office 365 Security

The growing use of Microsoft 365 applications (SharePoint, OneDrive, Teams) increases the risk of unauthorised data access via the internet. To mitigate this, cloud security scanning has been implemented on the Trust Microsoft tenant to scan all data for malware and suspicious code, as well as monitor account activity for potential account takeover incidents. Additionally conditional access policies have been implemented to restrict access from unmanaged devices as well as limit tenant access to the UK only.

Vulnerability Scanning and Patch Management

- Patch management is done through cloud management tools where Trust devices are enrolled.
- Trust and school systems must be checked for known vulnerabilities and have identified vulnerabilities remediated; where a vulnerability cannot be reasonably remediated, it should be added to the Trust IT risk register.

Mobile Device Management

MDM is used to manage, secure, and monitor mobile devices such as laptops and desktops.

Multi-Factor Authentication (MFA)

MFA adds a critical layer of protection for accessing accounts, and sensitive services. MFA must be implemented wherever available, especially for systems storing sensitive information (e.g., M365, MIS, financial systems, student data).

Systems not owned by the Trust but holding Trust data, such as cloud hosted services, must also support MFA.

Backup, Business Continuity and Disaster Recovery

The Trust has a comprehensive strategy in place that meets the NCSC guidelines and DfE standards.

Additional Considerations

Wireless Network Security

Wireless networks are encrypted using WPA3 or a similarly secure standard. Access to the wireless network is restricted to authorised users only, and guests can access the internet using a segregated guest Wi-Fi.

Remote Access

Remote access to the locally hosted school systems is restricted to the IT MSP support team and is performed via the provided remote management tool.

Web Application Firewall (WAF)

The Trust websites are hosted by the MSP in a cloud datacentre and are protected by a Web Application Firewall (WAF).

10. AUTHENTICATION AND ACCESS CONTROL

Password Management

All accounts must be protected with strong passwords that meet the following criteria:

- 6 previous passwords are remembered and can't be re-used
- Complexity requirements:
  - Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
  - Be at least eight characters in length for general users and twelve characters in length for accounts with administrator privileges
  - Contain characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example, !, $, #, %)
- Complexity requirements are enforced when passwords are changed or created.
- Passwords must be changed under the following conditions:
    - After a known/suspected security breach
    - If the password has been written down
    - If it is known/suspected that the password has been shared with an unauthorised individual

Role-Based Access Control and Conditional Access

The Trust makes use of Role-Based Access Control (RBAC), which is a security strategy that applies tailored access controls to users based on their roles and responsibilities within the Trust. It leverages conditional access policies to enforce different authentication and access requirements depending on a user's job function, ensuring both security and usability.

11. MONITORING AND ALERTING

By implementing comprehensive monitoring and alerting, the Trust can significantly reduce cyber security risks, detect issues early, and maintain a safe IT environment.

The following monitoring and alerting measures have been setup for the Trust and MSP to receive and, if required, immediately respond to:

- Endpoint Security Monitoring

- User Activity Monitoring
- Email Security Monitoring
- Cloud and Application Security Monitoring
- Cyber Threat Intelligence
- Safeguarding Monitoring (Classroom management)

Monthly, the MSP lead engineer checks all systems to ensure that monitoring and alerting is functioning correctly and analyses system reports and logs. This standardised process is captured in the Trust Cyber Security Framework Controls document, and the report is then provided to the ELT and the MSP Team.

12. CYBERSECURITY TRAINING AND AWARENESS

Training

All staff, trustees, governors and members must complete cyber security training upon commencement of employment and annually thereafter. The training will cover topics such as:

- Identifying phishing attempts.
- Best practices for password management.
- Safe use of school devices and networks.
- Reporting security incidents.

As part of this training, staff must complete the NCSC (or equivalent) training for schools.

Annually, a simulated phishing attack is carried out by the MSP, using real world tools. This attack is not communicated to staff before it is performed. However, the results are communicated after. This helps to create awareness and a culture of vigilance encouraging everyone to stay alert, report concerns, and act responsibly to prevent security or data breaches.

Training for Students

Students will receive age-appropriate cybersecurity education in alignment with the Trust's Online Safety Policy that at a minimum covers:

- The risks of sharing personal information online.
- How to recognise and avoid phishing emails and scams.
- The importance of maintaining strong, private passwords.

13. INCIDENT RESPONSE PLAN

All staff and students are required to report any security incidents, including suspicious emails, potential breaches, or system vulnerabilities, to the trust MSP Support Team immediately. All incidents are logged via the helpdesk system. Where required the DPO will inform the ICO.

Incident Response

An incident response plan is in place and should be reviewed in conjunction with this document. The IT MSP will follow a defined incident response protocol will:

- Assess the nature and scope of the incident.
- Contain and mitigate the impact of the incident.
- Investigate the cause of the incident.
- Notify affected parties, including students, staff, and parents, as necessary.

Post-Incident Review

After a cyber security incident, a post-incident review will be conducted to evaluate the response and identify areas for improvement.

14. CHANGE MANAGEMENT

The IT MSP Team uses a change management process to govern all changes that meet specific criteria:

- Changes that affect multiple users
- Changes that affect the cyber security systems or processes
- Changes that have a financial impact or requirement
- Changes to the system architecture or design
- Changes that require down time or cause disruption with the IT systems

The sign off process includes the same stakeholders as the cyber security management team.

15. ACCEPTABLE USE OF TECHNOLOGY

The ICT and Internet Acceptable Use Policy is in place and should be viewed in conjunction with this policy.

General Use

Students, staff, trustees and members are expected to use Trust and school technology responsibly and for educational or administrative purposes only. The following behaviours are prohibited:

- Accessing, downloading, or distributing inappropriate or illegal content.
- Unauthorised use or sharing of other people's accounts or data.
- Circumventing security controls or attempting unauthorised access to systems.
- Allowing remote connections onto the trust network via personal devices

Personal Devices (BYOD)

With very few exceptions, the use of personal devices to access Trust data is not permitted. Where an exception is granted by ELT, devices must be secured with complex passwords or other complicated forms of authentication such as PIN od at least six digits or biometric authentication. All personal devices accessing Trust systems can be subject to monitoring.

16. COMPLIANCE AND REGULATORY REQUIREMENTS

The Trust will comply with all applicable cyber security laws, regulations, and industry standards, including:

Requirement	Key Actions
DfE Digital & Technology Standards	The minimum standards that schools need to achieve in IT, safeguarding and cyber security
GDPR	Data encryption, access controls, appoint a DPO, breach reporting.
Cyber Essentials	Firewalls, secure configurations, malware protection, patching.
KCSIE	Online monitoring, content filtering, safeguarding policies.
NCSC Guidelines	MFA, backups, training, endpoint protection, response planning.
Prevent Duty	Monitor extremist content, train staff to recognize risks.
Incident Response	Develop and test incident response and disaster recovery plans.

17. CYBER SECURITY INSURANCE

Each school must have cyber security insurance in place, either from their general insurance provider or via the DfE's Risk Protection Arrangement (RPA).

Cyber security insurance, provides critical financial and operational support to schools in the event of a cyber incident:

- Covers incident costs such as data recovery and system restoration
- Legal and regulatory costs
- Ransom payments where applicable

18. POLICY AND FRAMEWORK REVIEW AND UPDATES

This policy will be reviewed annually and updated as necessary to reflect changes in technology, legal requirements, and cyber security best practices.

19. CO-OPERATION BETWEEN FUNCTIONS

Cyber security is a trust wide responsibility that requires co-operation between departments.

This includes:

HR

- Staff employment checks and onboarding/offboarding.
- Maintaining a schedule of staff that have completed the cyber security training

Governance

- Approval of policies
- Approval changes and new systems

DPO

- GDPR related policies and processes that affect data

Facilities and Estates

- Responsible for physical security, access and alarm systems including the server room and communications rooms.

20. ENFORCEMENT AND DISCIPLINARY ACTIONS

Failure to comply with this policy may result in disciplinary actions, including revocation of access to Trust systems, suspension, or termination of employment or enrolment, depending on the severity of the violation.

21. LINKS WITH OTHER POLICIES

This cyber security policy is linked to the:

- AI Policy
- CCTV Policy
- Data Protection Policy
- ICT and Internet Acceptable Use Policy
- Online Safety Policy