CHILTERN LEARNING TRUST

Cyber Security Protocol

Review Date
October 2026

CHILTERN LEARNING TRUST

Contents

1. Introduction
2. Responsibilities
3. Cyber Reviews
4. Security Controls
5. Reporting Procedures
6. Bring Your Own Device (BYOD)

1.Introduction

Chiltern Learning Trust is committed to ensuring the security of its schools' digital assets, data, and information systems. This Cyber Security protocol outlines the guidelines and measures that all staff within the Trust must follow to safeguard against cyber threats and maintain compliance with the Department of Education's Cyber Security standards for schools and colleges. The primary purpose of this protocol is to offer guidance and establish a consistent approach to cyber security across all Chiltern Learning Trust schools.

This protocol applies to all employees, contractors, volunteers, and students associated with the Trust schools. It covers all devices, networks, and systems owned or operated by the Trust.

2. Cyber Security Responsibilities

The Trust IT Operations Manager alongside Headteachers and the IT Contract Provider oversees Cyber Security. The IT Service provider is responsible for managing and maintaining the overall Cyber Security infrastructure, including firewalls, intrusion detection systems, anti-malware, and other security tools in line with the requirements stipulated by the school. They are responsible for promptly addressing any security breaches and implementing necessary actions to mitigate risks.

Chiltern Learning Trust's Board of Trustees is accountable for managing the risks associated with cybercrime, including fraud, theft and irregularity and also for ensuring that proportionate controls are put in place.

2.1 Staff and Users

Staff and users must actively participate in maintaining a secure digital environment. They are responsible for:

- Using Two Factor Authentication on Google Workspace accounts
- Using Multi Factor Authentication on Cloud Software that accesses sensitive and/or confidential information including MIS Software off site
- Completing compulsory annual Cyber Security training (NCSC)
- Protecting login credentials and not sharing them with anyone
- Using strong and unique passwords for all accounts in line with the school password protocol
- Reporting any suspected security incidents to the IT service provider and SLT via the IT Support helpdesk
- Complying with the Trust ICT Acceptable Use Policy

2.2 Compulsory Training

It is compulsory for all school staff, Governors and Trustees associated with the Trust to complete annual NCSC Cyber Security training through the school platform. As part of the Cyber Security training, participants will be educated on the importance of promptly reporting any suspected security incidents or potential vulnerabilities they encounter to the designated IT contact person within the school.

2.3 Reporting

Reporting incidents and concerns is critical to enable the Trust IT provider to take appropriate measures promptly. The schools will conduct regular cyber security awareness campaigns to all staff and stakeholders. These initiatives will reinforce cyber security best practices.

Headteachers and SLT are required to follow the Cyber reporting process outlined in Business Continuity plans.

3. Cyber Reviews

To ensure the effectiveness and ongoing improvement of Cyber Security measures, the Trust will use a comprehensive Cyber Review in line with the 10 steps to Cyber Security and Cyber Essentials requirements provided by the National Cyber Security Centre (NCSC). Reviews will be conducted annually by an external provider in collaboration with school staff, governors, and other relevant stakeholders.

Following the Cyber Reviews, an Action Plan will be developed outlining the necessary steps and improvements to enhance the Cyber Security position of each school. This plan will address any identified weaknesses, gaps, or areas of concern. The outcome of the reviews and an action plan will be reported each year to our Trust Board.

The Trust IT provider, in conjunction with the IT Operations Manager and the Headteacher will work to implement the Action Plan promptly. Progress toward completion of the Action Plan will be monitored throughout the year.

4. Security Controls

4.1 Overview

There is additional detail available on technical and organisational controls from the Trust IT Provider. Below is an overview of the key security controls in place at the Trust. For consistency, the controls have been categorised in line with the same sections used for the Cyber Review assessments. Note: this is not an exhaustive list of all security controls in place.

Key Security Controls	
Component	**Security Controls**
Network Security	• Firewalls in place to control all external connections and traffic to the Trust's networks • The Trust employs anti-spoofing controls for incoming emails • The Trust has external email banners configured to alert users when emails are received from external parties • Network traffic is effectively segregated where possible through the use of VLANs and separate SSIDs for staff, students and guests • Staff remote access to the school network is disabled
Secure Configuration	• User accounts and privileges are managed and monitored centrally • Systems are configured to block brute force attacks • Staff are not assigned local admin access on their school-provided devices or network systems
User Access Control	• Password-protected accounts are required to access Trust systems • MIS, safeguarding and Finance cloud software require MFA to access data • Systems are configured to have default complexity requirements • 3rd party users (facilities, catering, guests) are provided with limited web access only
Malware Protection	• The Trust uses ESET anti-virus which is kept up to date and maintained on all school-managed devices • Only approved applications can execute on devices
Security Update Management	• The IT teams update software on a regular basis as per the patch management policy in Appendix C • The IT team actively monitor the status of devices & software for updates
Risk Management	• The Trust takes a structured approach to risk management and integrates mitigating actions to regular ICT meetings and work plans
User Engagement & Training	• The ICT Teams deliver regular communications to Trust staff regarding latest risks and best practice around cyber security • The Trust provides policy-based guidance to staff around the acceptable use of technology, particularly in regards to remote working • The Trust has a defined and structured incident management policy and procedure • This Incident Response Plan is communicated to staff as part of the wider communication and awareness approach

Asset Management	• The ICT teams maintain an asset log of all school-owned devices and infrastructure within their schools
Proactive Monitoring	• The ICT teams use in-built tools to carry out configurational vulnerability scans on Google which are used to identify high priority risks related poorly configured features • The ICT teams receive and review alerts via Google regarding suspicious access activity • The Trust uses Active Directory Event Viewer to monitor the network and automated alerts are created based on any "suspicious" activity
Data Security	• The Trust utilises cloud backup systems to backup important data • Backup restore testing is carried out to a set schedule • The Trust encrypts user devices • All software suppliers are risk assessed for security protocols using a DPIA form, by schools, before engaging

4.2 Multi-Factor Authentication

It is a requirement at Chiltern Learning Trust that all staff Google Workspace accounts, safeguarding and MIS software has Two/Multi-Factor Authentication enabled. This requirement is essential to mitigate the increasing risks posed by unauthorised access attempts, phishing attacks and credential theft.

All cloud software accessing the schools Management Information Systems must have Multi Factor Authentication enabled.

4.3 Remote Network Access

In addition to the implementation of Multi-Factor Authentication (MFA) remote local network access is strictly prohibited within schools. By disabling remote access, the organisation ensures that sensitive data and systems remain within the controlled confines of the internal network infrastructure.

5. Reporting Procedure

While there are significant technical controls in place to identify, prevent and manage cyber incidents, there is no substitute for the role of people in the incident response plan. It is crucial that all staff (and students) take responsibility for reporting incidents when they are identified. Examples of reportable incidents include:

- Receipt of an email suspected to be a phishing attempt
- A user who has concerns they may have clicked on a fraudulent link, or submitted their credentials on a fraudulent website
- Receipt of any kind of notice/alert/demand of malware or ransomware
- Notice of any unusual activity on your email or Office365/Google Account

On the identification of any of the above, users should immediately notify **their school IT team (via ticket, email or phone)**, providing as much information as possible about the potential incident.

Relevant information may include:

- Details of what has triggered the alert (received an email, noticed something suspicious on a device etc.)
- Relevant details to timeline (when first noticed, when links were clicked etc.)
- Any knowledge as to the extent of data which might have been compromised
- Any details of other users who may be affected
- Mark the email as spam

6. Bring Your Own Device (BYOD)

The Trust supplies staff and trainees with school owned devices to enable them to complete their role effectively. Staff are not permitted to use a personal laptop, ipad or chromebook to carry out work on the school site due to GDPR considerations.

These controls are intended to protect the security and integrity of CLT's data and technology infrastructure. Users must comply with this requirement and agree to the terms and conditions set below.

- Any device used to access school systems (including cloud-based software) must be lockable and password protected in line with the Trust's password policy
- Staff accessing web-based software outside of the school site to view/edit documents must not download school files/documents onto their personal devices
- Staff accessing cloud based school software outside of the school site on a personal device must continue to abide by the Trust's Acceptable Use Policy and Data Protection Policy
- Staff accessing school cloud based systems outside of school on a personal device must ensure Multi Factor Authentication is enabled/prompted and alert the school DPO if this is not the case. This includes Apps used to access school software
- Files and documents must not be transferred directly onto personal devices or portable storage devices as they may contain confidential information
- If using a shared device, applications should be logged out after use and credentials should not be stored on the device/browser password management system
- Rooted or Jailbroken mobile devices are not permitted to connect to the Trust's network or school systems
- Staff and trainees are not permitted to connect personal devices to the school wifi due to safeguarding requirements*
- IT Teams are not permitted to connect staff personal devices to the school network or WiFi for day to day working*
- Users are responsible for maintaining good security practices while using personal devices and retain liability for protection of school data accessed using these devices. Breach of Trust policies through this use may result in disciplinary action.

- Staff are responsible for deleting all school/Trust data from their personal devices if they leave their employment and also in line with Trust data retention policies

*Visitor WiFi is available on request when visiting school sites. The Visitor passwords are automatically updated regularly.

The Cyber Security Protocol aims to create a secure and resilient digital environment across all schools within the Trust. By adhering to these guidelines and complying with the Department of Education's Cyber Security standards, we can collectively safeguard our data, information systems, and digital assets from cyber threats.

Associated Documents & Roles		
Document Name	**Description**	**Owner(s)**
Data Protection Policy	Outlines how data management and protection is conducted	Trust Data Protection Officer
Keeping Children Safe in Education Policy	Outlines safeguarding practices	Trust Director of Safeguarding
Acceptable Use Policy	Outlines acceptable use of technology in school	Trust HR Manager
Business Continuity Plan	Outlines the measures in place to maintain service and access to systems/data in the event of potential incidents.	CFO
Trust AI Policy	This AI policy outlines the guidelines and measures that all schools and staff within the Trust must follow to establish a consistent approach to AI.	Trust Tech4Learning Lead