Harbour Schools Partnership

A guiding light for education

Cyber Security Policy

Date Adopted: December 2025

Reviewed on:

Author/owner: Board of Trustees

Anticipated Review: September 2026

NB. 'Trustees' means the Directors referred to in the Trust's Articles of Association.

Introduction

History of most recent policy changes

Version	Date	Page	Change	Origin of Change e.g. TU request, Change in legislation
1.0	03/12/25			New THSP policy

Links to other Trust Policies

E-Safety & Acceptable Use Policies
Data Protection Policy

Table of Contents

History of most recent policy changes 2
Links to other Trust Policies 2
1.0 Introduction 4
2.0 Purpose Statement 4
3.0 Scope 4
4.0 Roles & Responsibilities 4
5.0 Common Cybersecurity Threats 5
6.0 Users 5
7.0 Risk Management 6
8.0 Device and Network security 6
9.0 Password Security Policy 6
9.1 Password Requirements 7
9.2 Multi-Factor Authentication (MFA) 7
9.3 Student/Pupil Passwords 7
9.4 Password Protection & User Responsibilities 7
9.5 Training & Awareness 8
10.0 Cloud Systems and Software Providers 8
11.0 Working remotely 8
12.0 User Education & Awareness 8
13.0 Monitoring, Preventative Action, Reporting & Incident Management 9
13.1 Monitoring 9
13.2 Preventative Action 9
13.3 Reporting 9
13.4 Cyber Response Plan 9
14.0 Disciplinary Action 10

1.0 Introduction

Cyber-crime and cyber security present major risks such as data theft, scams, and security breaches that could seriously harm the Trust's operations. Effectively managing these threats is essential to safeguard the Trust's resources, prevent financial losses, maintain business continuity, and uphold its reputation.

Cyber security involves protecting our devices and online services from theft, damage, and unauthorized access to personal data, whether stored on devices or in the cloud. This policy should be read alongside the schools' e-safety, acceptable use and data protection policies.

2.0 Purpose Statement

This policy aims to minimise cyber-crime risks to THSP by:

- Promoting collective understanding of cyber security's role in achieving organisational goals.
- Implementing appropriate risk and asset management.
- Fostering a positive cyber security culture through training and engagement.
- Protecting systems and data throughout their lifecycle.
- Preventing unauthorised data access.
- Monitoring, reporting, and managing incidents effectively.
- Embedding cyber security compliance within procurement and the supply chain.
- Meeting regulatory requirements.
- Preparing a Cyber Response Plan.

3.0 Scope

THSP uses information and communication technology (ICT) to improve teaching, learning, and its administrative operations. All staff members, trainees, pupils, volunteers, and visitors may access the Trust's IT systems as needed for their professional or educational tasks.

This policy applies to all current Trust employees, pupils, volunteers, and workers.

It covers every aspect of the Trust's IT systems, including local networks, trust-wide networks, cloud software, and any devices—personal or otherwise—used to access these networks or services, whether on-site or when representing THSP from any location.

4.0 Roles & Responsibilities

Trustees hold ultimate accountability for managing cyber security risks. They monitor this responsibility through the Strategic Risk Register, as well as reports from external auditors and the Trust Data Protection Officer (DPO).

The Chief Operations Officer and Head of IT oversee the IT strategy to protect against cyber threats, stay informed on risks, and share updates.
The Information Governance Leader ensures supply chain compliance and maintains oversight of all aspects of information security.

Head Teachers are responsible for ensuring that all staff receive Cyber Security Awareness training at induction, in addition to annual updates thereafter.

5.0 Common Cybersecurity Threats

All schools face cybersecurity risks, typically through emails, websites, or removable devices.

The Trust prohibits USBs and other removable devices unless specifically allowed, making email and unsecured websites the main cybersecurity threats.

Microsoft 365 incorporates various security features designed to filter out most spam, spoofing, and phishing emails, but some may still reach inboxes. Users should recognize and promptly delete or report suspicious emails—especially those with attachments, links, or requests for information—as they may lead to fraud or IT damage.

Spam comes as unsolicited offers and should be deleted. Spoofing and phishing pretend to be legitimate sources, often requesting payment or urgent information, and may have unusual email addresses or errors. Report these by forwarding to report@phishing.gov.uk, then delete without opening.
If unsure about an email's authenticity, do not open or click it; contact the sender using their published contact details.

Accidental opening of malicious emails should be reported immediately to Senior Leadership and IT Support.

Be careful on external sites—check for a padlock icon and the correct URL. Do not follow browser pop-ups or email links unless you're certain of their origin. Validate credentials only when expected via official company websites.

If you access a fraudulent link or submit info to an unknown party, record details and report to leadership so security can be improved and data breaches prevented.

6.0 Users

Staff are the first line of defence against cyber threats, making their awareness and caution crucial for safeguarding the school's data and IT systems.

The Trust aims to create an open, positive culture around cyber awareness, removing barriers to incident reporting and information sharing.
We achieve this by:

- Developing policies for safe IT use, including guidance on acceptable use, data protection, and information security
- Providing annual training and awareness sessions for staff
- Offering consistent IT support across the Trust's systems
- Sharing updates about emerging cyber threats

All users are strongly encouraged to report any suspected malicious cyber activity through the appropriate channels.

While many of the Trust's cybersecurity features operate in the background unnoticed, some directly affect daily work. The Trust strives to balance robust security with user needs. Those with access to sensitive data or administrative controls may experience stricter security measures.

Though these controls can sometimes feel inconvenient, they are essential to defend against cyber threats and prevent data breaches. If a user finds that a security measure hinders their work, they should discuss it with their Head Teacher and IT support.

Any agreed changes will only be made if overall IT system safety is not compromised.

By signing the Trust's Acceptable Use of IT Policy, users commit to safe IT practices and accept responsibility for managing and reporting cybersecurity incidents.

7.0 Risk Management

Cyber security incidents will be documented within the Trust's Risk Register as part of the broader risk management process. These risks will be assessed and reviewed annually, following any changes to IT systems, or immediately after an incident.

8.0 Device and Network security

The Trust's IT strategy is structured to activate essential security measures that safeguard data and protect the network from cyber threats. These features are intentionally designed to be complex enough for strong protection, but not so restrictive that they create obstacles leading users to devise weaker systems.
Security measures include:

- Firewall protection for the Trust's network
- Role-based device compliance and user permissions
- Limited admin privileges through Intune role controls
- Automated onboarding/offboarding with Intune and Azure AD
- Anti-virus management through Intune
- Windows and software updates delivered by Intune update rings
- Cloud service updates
- Password complexity and multi-factor authentication enforced by Azure AD/Intune
- Microsoft Edge password manager usage
- Asset management
- Standardised device configurations through Intune
- USB/external drive restrictions
- Secure device disposal protocols
- Guest Wi-Fi access

Even with these precautions, cyber risks cannot be completely eliminated. The Trust relies on users to remain vigilant and help maintain robust protection.
Users should:

- Avoid sharing specific information about the school or their job on social media
- Use distinct passwords for work and personal accounts
- Create strong passwords for work accounts
- Refrain from sharing passwords or writing them down; if written, store securely in a locked cabinet or safe inside a signed and sealed envelope
- Use Microsoft Edge Password Manager when required
- Not use work email addresses for personal sites or services
- Always lock their screens when stepping away
- Ensure personal devices used for work have current operating systems and anti-virus protection
- Download software only from official sources
- Seek assistance if they feel compromised or pressured to disclose sensitive details
- Promptly report clicking on malicious links to the Senior Leadership Team and IT Support
- Discuss security measures with Senior Leadership or IT Support if guidance poses barriers to effective work

Visitors needing IT access will sign an acceptable use policy upon joining the network. They should not use removable devices for accessing documents; instead, they can log into their cloud storage or email documents to themselves, or, in exceptional situations, contact a designated person at the school.

9.0 Password Security Policy

To protect the Trust’s data and IT systems, all users must follow robust password management practices. This section outlines the requirements for password creation, management, and protection

9.1 Password Requirements

Minimum Length & Complexity:
Staff passwords must be at least twelve characters long and include at least three of the following: lowercase letter, uppercase letter, number, and special character (e.g., !, #, $, %, @, etc.). Passwords must not include personal information or proper names.

Three Random Words:
Where possible, use the “three random words” method, then add complexity by mixing in numbers, upper/lower case, and special characters.

Account Lockout:
Accounts will be locked after six unsuccessful login attempts for ten minutes.

Password Changes:
Temporary passwords must be changed at first login. Passwords should not be reused for six months and must be significantly different from previous passwords. A password blacklist is used to prevent common or easily guessed passwords.

Session Timeout:
Users must re-authenticate after 60 minutes of inactivity.

System Defaults:
Default system passwords must be changed or disabled during setup.

9.2 Multi-Factor Authentication (MFA)

MFA is required for all staff accessing sensitive data, communication systems (such as email), and cloud-based solutions accessible from any location. MFA may not be required at trusted locations, such as Trust schools.

9.3 Student/Pupil Passwords

Primary (EYFS, KS1, KS2):
Minimum six characters, including at least one letter and one number. Passwords cannot be changed by students.
Secondary (KS3+):
Minimum ten characters, including lowercase, uppercase, number, and special character. Passwords can be changed by students.

9.4 Password Protection & User Responsibilities

- Never share passwords or write them down in unsecured locations.
- Do not use dictionary words, family names, or easily guessed information.
- Change your password immediately and report to IT if you suspect compromise.
- Be vigilant when entering passwords to avoid “shoulder surfing.”
- All passwords must be encrypted in storage.

9.5 Training & Awareness

All staff, trustees, and governors are informed of the password policy at induction, through the Acceptable Use Agreement, and via ongoing training.
Students are taught password security as part of the Computing curriculum and through the Acceptable Use Agreement.

10.0 Cloud Systems and Software Providers

The Trust works with various IT providers whose reliability and risk levels differ. For business-critical services like email, MIS, and course delivery, providers must demonstrate cyber threat protection through Cyber Essentials compliance and, for sensitive data, ISO9001/27001 accreditation.

Key systems containing highly sensitive information, such as MIS, Finance, and Safeguarding software, should be sourced from approved government digital marketplaces or National Frameworks. DPIA assessments are required during procurement.

Software as a Service use is increasing, especially platforms hosting sensitive Trust data. Users must follow password complexity guidance and maintain privacy practices, including screen locking when unattended.

Data must stay within these systems and only be transferred between schools using secure, built-in file transfer protocols or the DfE system.

IT data protection considerations are mandatory in procurement.

11.0 Working remotely

Pupils and staff require remote access to school systems for learning and administrative tasks.

Using staff devices at home can risk unauthorized access to sensitive data, so all files should be stored in the cloud—never on removable or local drives—to prevent loss if a device is lost or stolen.

Staff must practise secure remote work by only using their work devices, not allowing others to use them, and ensuring password entry is always required (no auto-login).

Work accounts or devices should not connect to unsecured networks. Staff may access work accounts via personal mobile phones if they are password-protected (minimum 6 characters or biometric ID) and have antivirus software enabled; these personal devices must not be shared.

Remote access to school on-premise systems is strictly prohibited. Staff and pupils must not attempt to connect to internal servers, desktops, or other on-site IT infrastructure from outside the school environment under any circumstances. This measure is in place to safeguard sensitive data and protect the integrity of the Trust's network from external threats.

12.0 User Education & Awareness

Training is necessary so all users know their cybersecurity roles:

- IT Support and Network Managers will stay updated on cybersecurity and receive technical training regularly.
- Senior Management will complete yearly training (e.g., from NCSC), meet with IT, and share updates with staff.
- All staff will receive Cyber Security Awareness training per this policy.

Active management and reporting of cyber activity by all users strengthen internet safety and support students' ongoing education.

13.0 Monitoring, Preventative Action, Reporting & Incident Management

The Trust promotes a positive cyber security culture where users can report issues without fear of punishment. Early reporting helps identify risks and protect systems from data loss or breaches. Most threats are handled promptly through user vigilance and good practices, reducing the need for incident management.

13.1 Monitoring

The Trust's IT systems actively monitor user activity. The internet filtering system identifies attempts to access websites or materials deemed potentially harmful and can detect repeated attempts to access user accounts.

The Trust may share IT monitoring reports with external agencies to facilitate the identification of inappropriate use, address safeguarding concerns, or support investigations into cyber-crime incidents.

13.2 Preventative Action

If you believe you've received malicious IT communications:

- For spam emails, simply delete them without opening.
- For spoofing or phishing emails, do not open them; instead, forward them to report@phishing.gov.uk and then delete without sharing them further.
- If you receive a hijacked email from a trusted source, notify the sender, report it to itsupport@thsp.org.uk, and delete the message.

13.3 Reporting

The Trust understands users may accidentally open emails or links that introduce malicious software into the IT system, risking data loss or system failure.
If this occurs, users must:

- Immediately isolate the device by disconnecting it from LAN or/and Wi-Fi (if possible). **Only** power off the device if removal form network is not possible, as this could hinder data recovery.
- Record relevant information about the incident.
- Report the incident straight away to IT Support and a Senior Leadership Team member, including user account details.
- Wait for approval before reconnecting the device or logging in from any device.
- Cooperate with any follow-up investigations.
- Comply with any recommended security improvements.

13.4 Cyber Response Plan

The school's Cyber Response Plan must be followed for all incidents, with procedures adapted according to the severity and risk involved.

Any decision to involve the Trust's cyber insurers will be made by the Executive Leadership Team. No action should be taken without guidance from the insurers once they are engaged.

14.0 Disciplinary Action

The Trust encourages all users to take an open and proactive approach to managing cyber security risks and does not punish staff for reporting incidents. All reported cases will be reviewed fairly, and their findings will be used to help staff prevent similar incidents in the future.

However, users are still responsible for their actions—disciplinary measures may apply if someone intentionally causes harm or deliberately ignores this policy, especially when such neglect hinders efforts to limit system damage after a cyber incident.