Cyber Security Policy

LINKS: Data Protection Policy, Emergency and Business Continuity Policy

DATE: May 2025

POSTHOLDER RESPONSIBLE: Trust ICT Manager

TRUSTEES/GOVERNORS COMMITTEE: Finance, Operations & Audit

AUDIENCE: All schools, employees and volunteers within the QET

STATUS: Approved

DATE RATIFIED: May 2025

DATE OF NEXT REVIEW: This Policy will be reviewed annually

STATUTORY/NON-STATUTORY: Non statutory

Data Protection Office: dposchools@somerset.gov.uk

Contents

Introduction 3

About this policy 3

1. Roles and Responsibilities 3
2. Scope 3
3. Complying with Regulations 3
4. Cyber Security best Practice 4
5. Account management best practice 4
6. Training 4
7. National Cyber Security Centre (NCSC) training and guidance 5

Introduction

This cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

This cyber security Policy is designed to protect the integrity, confidentiality, and availability of all trust school's information systems and data. The policy applies to all students, faculty, staff, and visitors who use each school's network, digital resources, and devices. The goal is to ensure the safe and secure use of technology in a way that promotes an effective learning environment while safeguarding against cybersecurity threats.

About this policy

The purpose of this policy is to:

Establish guidelines for secure use of each school's information technology resources. Protect the personal and academic data of students, faculty, and staff. Minimize the risks of cyberattacks and unauthorized access to each school's network. Promote a culture of cyber security awareness among all students and staff.

This policy details the measures that should be taken to mitigate the risk of cyber threats under the following sections and in compliance with the National Cyber Security Centre's guidance in section 7.

1. Roles and Responsibilities

The trust's senior leadership team (SLT) recognises the need for all staff to be involved in the conducting of Cyber Security and is critical to protecting each school's systems and Data. This is an important aspect of strategic leadership within the trust, the SLT, Headteachers and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

2. Scope

All trust schools will comply with all applicable cybersecurity regulations and standards, including those related to data protection.

This policy applies to all devices and systems owned or operated by all schools within the trust, including:

- School computers, tablets, and smartphones.
- Email systems and web applications.
- Network infrastructure (e.g., Wi-Fi, LAN).
- Cloud-based services and digital storage solutions
- All users, including students, faculty, staff, administrators, and visitors

3. **Complying with Regulations**

This Policy has due regard to regulations including, but not limited to the following:

- Data Protection Act 2018 (DPA 2018)
- Network and Information Systems (NIS) Regulations (2018)

- The UK NIS Regulations are designed to improve the overall cybersecurity posture of essential services and digital service providers, aligning with the EU NIS Directive.
- Cybersecurity Essentials (Cyber Essentials)
- The Computer Misuse Act 1990
- ISO/IEC 27001
- Information Commissioner's Office (ICO)
- National Cyber Security Centre (NCSC)

4. Cyber Security best Practice

All schools will ensure that all faculty, staff and Governors are educated on how to identify phishing attempts, use secure devices and how to protect systems and data.

Best practice, advice and guidance from the National Cyber Security Centre is observed for all IT systems, particularly those where learner information, learner work or assessment records are held.

National Cyber Security Centre (NCSC) training and guidance includes:

- Establishing robust password and account management controls
- Enabling multi-factor authentication (MFA)
- Keeping software and systems up to date
- Implementing network security measures
- Conducting regular data backups
- Educating employees on security awareness
- Develop a Cyber response plan
- Regularly assess and audit of security controls

By adopting industry standard cyber security best practices, the SLT, Headteachers and Governors significantly reduce the risk of cyber-attacks and protect valuable data and assets within all Schools.

If a cyber-attack which impacts any School data, assessment records or learner work is experienced, the senior leadership team/will contact the relevant awarding body/bodies immediately for advice and support as detailed in the QET Cyber response plan.

5. Account management best practice

Implementing best practices in account management helps minimize the risk of unauthorised access, data breaches, and identity theft. Using Strong password policies and two factor authentication significantly reduces the risks and prevents attackers from repeatedly guessing passwords, greatly reducing successful brute-force attacks.

Avoid Shared Access Issues: By avoiding shared accounts, you ensure that access is properly tracked to individual users, making it easier to identify and respond to suspicious behaviour.

6. Training

Staff training in cybersecurity is crucial because human error is often the biggest risk in an organization's security posture. Even with the best technology in place, an untrained employee can inadvertently compromise systems or data

7. National Cyber Security Centre (NCSC) training and guidance

Password Management

- All Users are informed that password length is a more valuable defence than complexity and instructed to use a password creation approach such as three random words to generate suitably secure passwords
- All users will not use easily guessable information such as birthdays, singular names or common words for a password
- For every account, users are instructed to use a strong unique password, and that the same password is not used across any other account(s)
- Passwords must not be shared with others. If a password is suspected to have been compromised, it should be changed immediately.
- Passwords should be changed every 3 months, to ensure greater protection is maintained.

Multi-Factor Authentication (MFA)

- All users should use two-step verification or multi-factor authentication (MFA) wherever available/requested. Staff should be aware of the purpose of MFA, which includes:
    - Adding a layer of account security
    - Helps to protect users if the extra steps/factors are protected

Keeping software and systems up to date

Keeping software and systems up to date is one of the most essential practices in cyber security. It helps mitigate risks associated with vulnerabilities, exploits, and emerging threats

- Patches and Vulnerability Fixes

Software vendors regularly release updates to fix security vulnerabilities in their products. If these updates aren't applied, hackers can exploit those unpatched vulnerabilities to gain unauthorized access to systems, steal data, or disrupt services.

- Improved Features and Security Enhancements

Updates often include enhancements to the security architecture, such as better encryption, stronger authentication, and the adoption of new technologies to defend against evolving threats.

- Reducing Exposure to Malware and Ransomware

Ransomware attacks and other malware are often able to exploit outdated systems and software. Keeping systems up to date significantly reduces the likelihood of these attacks.

- Maintain Inventory

Keep track of all software versions and hardware that is use within an organization to ensure

everything is properly updated, this includes but not limited to, PCs, Laptops, Tablets, Chrome-books, Printers, Servers, Networks and Wi-Fi devices

Implementing network security measures

Implementing network security measures is essential to protect data, systems, and networks from potential threats, attacks, and unauthorized access.

- Firewalls

Firewalls monitor and control incoming and outgoing network traffic based on redetermined security rules.

- Web filtering

Filtering is an essential part of cybersecurity to prevent access to malicious or inappropriate websites, reducing the risk of phishing and improving network performance. It helps to protect users from online threats

- Antivirus

Ensure antivirus software is used and kept up to date, it helps protect computers, servers, and mobile devices from malware, viruses, and other forms of malicious software.

Antivirus programs detect, block, and remove harmful software, providing a layer of defence against cyber threats.

- Network Segmentation (VLANs)

Dividing the network into smaller, isolated segments to limit access and reduce the spread of potential threats.

Segment critical network resources (e.g., servers, databases) and restrict access between segments based on the principle of least privilege.

Conducting regular data backups

All Trust schools, regardless of size, will take regular, full backups of their data so that they can recover from a cyber security or business continuity incident.

A backup may also be a condition of your school's cyber insurance cover to aid in the recovery of your school's services, you will need to refer to your insurance documents for further advice on this.

General guidelines for effective cybersecurity backups:

Follow the 3-2-1 Rule

- 3 Copies of Data: Have at least three copies of your data: the original and two backups.

- 2 Different Media: Store backups on two different types of media (e.g., an external drive, cloud storage, or network-attached storage).
- 1 Offsite Backup: Keep at least one copy offsite, which helps protect your data in case of physical disasters (like fire or flooding) or local cyberattacks (such as ransomware).

Encrypt Backups

- Encrypt your backup files, especially if they contain sensitive information. This adds an extra layer of protection in case they are compromised.
- Use strong encryption algorithms (AES-256) to ensure that even if an attacker gain access to the backups, they cannot easily access the data.

Automate Regular Backups

- Schedule regular automated backups (daily, weekly, etc.) to ensure that you don't miss critical updates.
- Automating backups reduces the risk of human error and ensures your backup is always up to date.

Use Versioning

- Implement version control for your backups. This means you can revert to previous versions of files in case of accidental changes or if malware corrupts the current version.
- Cloud services often provide versioning by default, so check that your service supports this feature.

Test Backups Regularly

- It's crucial to test your backups to ensure they are functioning properly. Restore files from backup on a regular basis to verify that the process works smoothly.
- Testing helps to identify issues before they become a critical problem.

Keep Backup Locations Secure

- If using physical backup devices (external hard drives, USB drives), store them in a safe, secure location.
- For cloud backups, choose a provider that offers strong security measures, such as end-to-end encryption and data redundancy.

Educating employees on security awareness

All users must complete annual cybersecurity awareness training, which includes topics such as phishing prevention, safe internet practices, and data protection.

- Staff must check first with a senior leader/line manager/ IT Department/Support if they are unsure or have a wariness of anyone or anything they are not expecting.

- Staff must take care if unsolicited or unexpected emails, instant messages, or phone calls are received asking for account credentials or personal or confidential information

- Staff will never approve or authenticate a login request that they did not initiate
- Staff will not click on suspicious links, download attachments or scan QR codes from unknown sources
- Staff will verify the authenticity of any communication by contacting the organization directly through official known channels
- Staff will report any phishing attempts to senior leader/line manager/ IT Department or IT Support immediately

Developing a Cyber incident response plan

All Schools should complete a Cyber response plan and refer to the RPA website where schools have Cyber insurance.

Schools can also refer to the QET Cyber response plan.

Completion of this plan will aid the school's ability to recover from a Cyber-attack as quickly as possible and to ensure that school staff will have a clear understanding of who should be contacted, and the actions necessary to minimize disruption.

Regularly assessing and auditing security controls

Conduct regular reviews of your measures.

Cyber attackers adapt and evolve, and your security needs to do likewise so testing the effectiveness of your security controls is important.

Schools can review defensive measures against suitable frameworks such as Cyber Assessment Framework (CAF), or certification schemes such as Cyber Essentials.

Schools should rehearse how your they can respond to cyber-attacks by using the NCSC's Exercise in a Box resource, which provides a safe environment for schools to assess its resilience.

In addition, it's good practice to test schools systems and security processes by emulating an attacker hacking into secure systems or data by 'red teaming'.

A 'red team' can be an externally contracted group of penetration testers or a team within your own organisation, tasked to hack your environment using real world techniques in order to test a wide variety of cyber-attacks, breach scenarios.