CYBERSECURITY POLICY

CONTENTS

MONITORING AND REVIEW

Staff Responsible	Bursar
Reviewed by	SLT
Approved by	SLT
Frequency of Review	Annually
Date of Last Review	January 2026
Date of Next Review	January 2027

The School refers to all staff and students in St Mary's School, which includes the Early Years/Foundations Stage (EYFS), the Preparatory Department (Years 1-6), Senior House (Years 7-11) and the Sixth Form (Years 12-13).

The term 'parent' refers to those who have parental responsibility for a child.

AIMS

At St Mary's School we are committed to providing a quality education in a caring and stimulating environment. The purpose of this policy is to highlight to staff and governors of the potential risks of cyberattacks for the school, making clear what we currently have in place to prevent such events occurring, and to highlight what is regarded as the basic principles of good cyber security. Safeguarding our students and wider school community, whether in person or online, is of

paramount importance to us. This policy encompasses everything we do to minimise and mitigate risks of cyberattack.

WIDER REFERENCES

This policy operates within a wider national framework. It operates with due regard to:

- National Cyber Security Centre - https://www.ncsc.gov.uk/section/education-skills/cyber-security-schools
- Keeping Children Safe in Education (2024)

RELATED INTERNAL POLICY

This policy should be read in conjunction with:

- Data Protection Policy
- Acceptable Use Policy
- Online Safety Policy
- Examinations Policy
- Examinations Contingency Policy

ROLES AND RESPONSIBILITIES

Role	**Responsibilities**
Head of Centre	Overall responsibility for policy implementation and cyber security strategy.
IT Manager/Team	Implement technical controls, monitor systems, respond to incidents, manage access and updates.
Bursar	Ensure compliance with data protection law, advise on data handling, and oversee data breaches.
Deputy Head (Academic)	Ensure examinations policies and procedures are compliant with Cybersecurity Policy
All Staff	Follow this policy, complete annual training, report incidents or concerns promptly within the centre.
Governors	Oversee and review cyber security arrangements and policy compliance.
Students/Users	Use IT systems responsibly and report any concerns.

INTRODUCTION

A cyber-attack is an attack launched from one or more computers against another computer or network of computers. It can maliciously deactivate computers, steal data, or use a compromised computer as a launch point to further aggravate the attack. The two aims of cyber-attacks are to either disable the system, or gain illegal access to the target computer or network.

There are different types of cyber-attacks based on their specific method and intention. A cyberattack is a malicious and deliberate attempt by an individual or organisation to breach the information system of another individual or organisation. Usually, the attacker seeks some type of benefit from disrupting the victim's network. In the past few years, the National Cyber Security Centre has issued a number of alerts to schools, warning of an increase of malware attacks, in particular ransomware, targeting educational establishments. The complexity and variety of cyberattacks is ever increasing. While cybersecurity prevention measures differ for each type of attack, good security practices and basic IT hygiene are generally good at mitigating these attacks. In addition to implementing good cybersecurity practices, we are advised to keep systems and security software up to date, leverage firewalls and threat management tools and solutions, install antivirus software across systems, control access and user privileges, backup systems often, and proactively watch for breached systems.

A detailed list of common types of cybersecurity attacks affecting schools can be found in Appendix I.

Staff Training and Awareness

All staff must complete annual cyber security training and annual refresher training.

The training must include:

- the importance of creating strong, unique passwords for all accounts;
- keeping all account details strictly confidential;
- the critical role of Multi-Factor Authentication (MFA) in protecting against unauthorised access;
- how to properly set up and use MFA for both centre and awarding bodies' systems
- an awareness of all types of social engineering/phishing attempts;
- the importance of staff quickly reporting any suspicious activity, events, incidents and encouraging a safe and supportive reporting culture.

Records of cyber training must be retained for all staff and be available for inspection.

TECHNICAL SUPPORT

St Mary's School currently has a full-time IT manager and an annual Service Agreement with CST (Central Support Technologies) for third line support. The following is a list of measures that the technical support Team provide to protect our school network from cyberattacks.

Internet security and filtering

School's access to the Internet is via the Smoothwall filter. They are an Internet Watch Foundation 5 member and block access to illegal child abuse images and terrorism content at a national level.

Smoothwall Web Filtering protects our organisation by blocking access to malicious, hacked, or inappropriate websites. Web filtering is the first line of defence against web-based attacks. Malicious or hacked websites, a primary vector for initiating attacks, trigger downloads of malware, spyware, or risky content.

The Smoothwall is configured on a group basis, split between staff, students and network administrators. The DSL and IT Support receive any urgent safeguarding alerts for them to be able to action where required and log any incidents and any false positives.

Firewalls

Firewall services are provided by a Smoothwall S9 appliance. The S9 identifies thousands of applications inside network traffic for deep inspection and granular policy enforcement. It protects against malware, exploits, and malicious websites in both encrypted and non-encrypted traffic. It detects and prevents against known and unknown attacks using continuous threat intelligence from AI-powered Smoothwall security services. Delivers industry's best threat protection performance and ultra-low latency using purpose-built security processor (SPU) technology. Provides industry-leading performance and protection for SSL encrypted traffic.

Anti-virus

School devices are protected by Sophos. By using advanced AI learning, Sophos stops. It also protects against malware, online banking and shopping threats and much more.

USB pens

The School's policy is that USBs storage devices should not be used by staff or students, with the exception of exams administrators, invigilators and system admins. In the event of a USB being used by staff or students, it is scanned by Sophos antivirus (on any school owned device) and any malicious or harmful files are identified and removed.

Schools Technical Support personnel

CST Staff (when needed in school) are subject to DBS checks as required. Continuous Professional Development and relevant training is provided to ensure the correct security policies are applied to all ICT systems. Internal policies dictate that when staff leave, they are deleted from team email accounts and critical passwords are changed.

Emails

Microsoft Office 365 is used for all of our emails. Microsoft email is encrypted using Transport Layer Security (TLS). This is a protocol that securely encrypts and delivers inbound and outbound mail while disabling eavesdropping between mail servers. Most major email providers use TLS but it is important to keep in mind that both the sender and receiver must use a TLS supported mail server to encrypt messages.

Passwords

For security purposes, staff are requested to use a strong password and the use of 2-Factor Authentication is compulsory for accessing the network remotely.

Backup

The school has an agreement with CST who host Acronis Backup cloud that is run every hour for all onsite servers. Information is kept for 30 Days and then gets re written. This solution ensures we have an offsite backup of the school data. Microsoft offers data retention for one drive for any files deleted for up to 30 days and also has file versioning enabled should there need to be any file restores from one drive.

Acceptable Use and Device Care

Staff and students sign an AUP at the start of every academic year, agreeing appropriate use of school systems.

REQUESTING ADMIN RIGHTS

Only the IT Manager (and 3rd line support) hold admin rights to school systems. If a member of staff requires additional software to be installed on their school device, they must liaise with the IT team and allow a week's notice in order for the team to be able to do due diligence checks.

SIGNING UP TO THIRD-PARTY APPLICATIONS AND WEBSITES

The downloading of apps and programmes onto school devices, or student BYOD devices, should only take place after the IT department have approved the app or programme. Please follow the procedure below;

- Identify the website you wish to use and contact the IT Department **at least 2 weeks prior** to rollout date, detailing the specific educational reason why you need it and whether there are any costs associated.
- In your request, clarify whether you can support the students in signing up during lesson time, or whether you need assistance from IT support. If it is the latter, this needs to be factored into the rollout timeline.
- If students are installing an app/programme onto their device, a letter **must** go home from you, the class teacher detailing the educational purpose and the date in which it will take place as well as any costings. Please follow appropriate protocol for letter writing – it must go via the main school office.
- If students are accessing a new website, please check the age requirement. Anything that is not age appropriate should not be used. In the case of students needing to access a website with different maturity ratings, please inform the IT department before requesting a signature from home.

DISPOSAL OF REDUNDANT SCHOOL ICT EQUIPMENT

St Mary's School currently dispose of redundant ICT equipment via a company called Enviro Electronics. The recognised standards are: PCI DSS (Payment Card Industry) Data Security Standard HIPAA (Health Information Portability and Accountability Act) 7 PIPEDA (Personal Information Protection and Electronic Documents Act) Data protection Act 1998.

NATIONAL CYBER SECURITY – Practical Tips

The National Cyber Security Centre has issued practical tips for everyone working in education. Cyber security is about protecting the devices we use in school and the services we access on line, both at home and work, from theft or damage. It is also about preventing unauthorised access to the vast amounts of personal information we store on the devices and on line

As a school we hold lots of sensitive information, for example staff bank details, medical information about students and safeguarding records. All of this has to be kept safe and confidential. Cyber criminals understand that a school's information is sufficiently important that they might be prepared to pay a ransom to get it back.

Powerful Passwords

When implemented correctly, passwords are a free, easy and effective way of helping to prevent unauthorised users accessing devices or networks in school. Here's how to use them well:

- Have a different password for each account / service. If this isn't possible then make sure your most sensitive accounts (e.g. access to student records) have a unique password.
- If you must write down your passwords, store them securely and away from your device.
- On the advice of the IT team, two factor authentication should be considered in specific circumstances.
- Always lock your account when you step away or stop using your device, even if it's just for a minute. This applies in school or when working from home.

A good way of creating a strong and memorable password is to use three random words. Passwords should be easy for you to remember but hard for somebody else to guess.

We strongly recommend that you **don't** include the following:

- Partner's name
- Child's name
- Pet's name
- Place of birth
- Favourite holiday
- Something related to your favourite sports team
- A list of numbers (e.g. 123456) or words like 'password' or 'qwerty'.

'If in doubt, call it out'. Always ask for advice if you're not sure if the link or email is legitimate.

If you feel you may have compromised your security, report this to the Assistant Head or the IT Manager as soon as possible so they can try to minimise any damage.

Working from Home

Staff are responsible for keeping work information safe when accessing it at home. These tips can help to minimise the chances of any cyber security incident transferring from home devices to the school network or vice versa:

- Use up-to-date anti-virus software on your own devices
- Download all software updates as soon as they are offered
- Ensure all your devices have passcodes. (Even if you only use your laptop for work, for example, this may be synched to your phone or tablet)
- Change any default passwords on devices or software - including your home Wi-Fi

SUMMARY

Following good data protection practices and methods will ensure if ever there is an attempted cyber-attack, the school's assets and intellectual property are secure. It will also ensure the downtime is minimal and the systems are restored at the earliest. As well as taking the appropriate

steps to reduce the impact of any potential Cyber Security attack, all staff are asked to sign an Acceptable Use Policy. This tells staff what is acceptable in the use technology and communications (including social media). The school has disciplinary measures in place, should staff not adhere to the guidance.

APPENDIX I: RISK - COMMON TYPES OF CYBERSECURITY ATTACKS AFFECTING SCHOOLS

Phishing

Phishing is a technique used to deceive a target into taking harmful action such as downloading malware disguised as an important document. A targeted phishing attack could be used to gain access to a user's account that has important information (such as a member of the Senior Leadership Team) or a user with administrative privileges to the network. Phishing is usually in the form of an email sent to either a list of users or targeted at single user. The attacker would craft an email and disguise it to be seemingly normal, with malware attached that looks like it could be a normal document. The email could also include a link that goes to a website designed to look like a familiar website and trick the user into entering their credentials. To prevent phishing attacks, it is recommended the email system should have an effective filter, which SMS has on 365 platforms. All staff should be trained on how to identify potential spam emails before clicking on any links or documents attached.

Some phishing emails are more sophisticated than others, but it helps to be aware of some of the more obvious clues. These include:

- Does it contain poor quality images of logos?
- Are there spelling or grammatical errors?
- Does it address you as 'dear friend' rather than by name?
- Is it asking you to act urgently?
- Does it refer to a previous message you don't remember seeing?

Ransomware

Ransomware encrypts the target files on the system so the user cannot access them. The attacker then demands payment to restore access to the files. A ransomware attack usually happens when a user opens a malware file or link on a network connected computer. The malware file has specific scripts to identify and encrypt the files in the target area. Ransomware could be used to encrypt a school's financial and contact data so that the school would not be able to access it. To prevent ransomware attacks, it is a good practice to have On-access scanning enabled on all user devices to scan for viruses before accessing files. Firewalls should be enabled on host devices and anti-virus software should be updated with the latest security patches (Sophos).

Password attack

Password attack is an attempt to gain access to systems by cracking the user's password. Once the user password is cracked, the attacker can gain access to either confidential data or an administrative account allowing access to all data or make significant changes to the network. A targeted password attack usually involves the attacker finding out details about the user and then attempting to use that information to determine the correct password. Passwords that have been leaked or hacked from organisations are sold on the dark web by criminal gangs. A good practice to follow is not using the same password twice. The use of complex passwords with a mixture of words, numbers, and special characters is strongly advised by cybersecurity experts. This is a must for all of the staff of St Mary's School. Password policies are in place, staff and students are prompted to

change their passwords every 90 days. Another way of preventing password attack is to enable multi-level authentication on systems that support it which we have for MiS and 365 platforms.

Brute force

Brute force is an attempt to gain access to systems by trying different passwords to eventually guess the correct one. Similar to a password attack, the attacker could gain access to privileged user accounts. Malware that is installed on the network with direct access to a systems login screen can be used to secretly attempt to guess a user's password. One of the prevention tactics is to configure locking the accounts. Accounts should lockout if there are too many failed attempts at logging in. Audit logs should also be configured and regularly reviewed by the system administrator for any abnormal use of accounts.

Denial of Service (DDoS)

This is created by sending so much traffic to a computer or network such that its resources are overwhelmed and they are made unavailable to anyone. When affected by a Denial of Service attack, the school would be unable to access and use the affected systems. An attacker compromises a computer or multiple computers using malware that instructs them to send traffic to a single target. In the case of multiple computers, it is called a distributed denial of service attack. Systems should be built and configured around the concept of redundancy and the ability to fail-over to a secondary system if the first is unavailable. Systems should also be designed with the ability to deal with increased load over the average normal usage. SMS systems are mostly linked to the cloud, meaning that in the event of overload or outage, we can continue from another cloud location. Some shared files (e.g. staff resources) are currently hosted on school server, meaning if a DDOS attack took place, these files could only be accessed locally rather than remotely. We encourage staff to use OneDrive as much as possible in order to mitigate this.