The King's (The Cathedral) School
Cyber Security Policy

Responsibility:	IT Network Manager
Ratified By:	Governing Body
Date Reviewed:	March 2025
Next Review Date:	March 2026

Table of Contents

1. Objective & Scope of the Policy

1.1 Purpose

This Cyber Security Policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure. The more that we rely on technology, the more vulnerable we become to severe security breaches especially in a world where there is increased sophistication of cyber-attacks. For this reason, we have implemented a number of security measures which are outlined in this policy.

1.2 Scope

This policy applies to all our staff, governors, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

1.3 Roles and Responsibilities

Our Risk Register has identified a cyber-attack as a significant concern for the effective running of the School. The Headteacher has ultimate responsibility to ensure that the policy and practices within this policy are embedded and monitored.

The scrutiny of this policy will be completed by our Finance Committee who may wish to receive regular updates on the implementation and the School's evaluation of security against nationally recommended benchmarking tools. Where appropriate, they may wish to engage with third party experts to provide additional scrutiny and risk level.

Our IT Manager is responsible for ensuring that the safeguards identified within this policy (and the Cyber Response Plan) are in place and that any possible risks to the organisation are discussed and shared with the Headteacher.

Our Data Protection Officer, supported by external consultants, will ensure that our responsibilities towards effective handling of data are completed in line with our Data Protection Policy.

Our IT teaching staff will play a specific role in ensuring that students are aware of their own role in keeping the School and themselves safe from cyber-attacks.

All staff including governors should ensure their own practice is in line with those measures identified here, within our IT code of conduct and as updated by the Headmaster or ICT Manager should the need arise.

Jointly with respective departments we should ensure that any purchases of hardware or software are reviewed in line with government and industry-wide best practice.

1.4 Types of Cyber Threat

A threat is any breach or action that if left unchecked could disrupt the day-to-day operation of the School, the delivery of education and the protection of sensitive information.

Specific types of threats are likely to include:

a) Cybercrime: generally done for financially gain, most commonly for the purposes of fraud or exploitation. Methods typically include Malware, Ransomware or Phishing attacks;
b) Hacktivism: taking over a website or social media account in order to highlight a particular cause;
c) Denial of Service attack: use of large bot nets to attack our external connections or services hosted by third parties, causing loss of service;
d) Internal malicious actions: actions of internal actors to disrupt services and operations of the School;

e) Age-Related Threats and Product Retirement Planning: as technology evolves, older hardware and software can become vulnerable to security risks due to outdated features and lack of support. It is crucial to regularly assess the age and condition of our IT assets to identify potential vulnerabilities. This includes planning for the retirement and replacement of obsolete products to ensure continued protection against cyber threats. By proactively managing the lifecycle of our technology, we can mitigate risks associated with aging systems and maintain a robust security posture.

2. Steps taken to increase Cyber Security

The School takes guidance from a number of relevant organisations in order to keep its IT systems as safe as possible. These include:

a) **Back Up**

i. Our current backup solution is installed according to industry standards. The configuration details are stored in hard copy for review, as necessary
ii. We follow a 3.2.1 rule of backups and ensure that we have air-gapped offline copies. We also ensure our Microsoft systems are backed up to another third-party immutable backup
iii. The cloud-based systems that the School uses are backed up. We are relying on the provider of that third party system to configure and handle their backups in accordance with their own terms and conditions of contract

b) **2 Factor Authentication**: to ensure that our systems and data are protected while users are away from the School campus, we will enforce the use of the Microsoft security products via the use of 2FA, conditional access rules and other settings as allowed by the level subscription
c) Reviewing national and supplier best practice guidance
d) Patch and update management
e) Reviewing cyber warning information on zero-day bugs
f) Reviewing and monitoring age of hardware assets against vulnerability and age-related failure.

Many of these steps taken require staff and governors to take specific precautions. Specifically, these are:

a) Keeping all passwords secure;
b) Ensuring devices are not left exposed or unattended;
c) Not trying and turn off or bypass any antivirus or anti-malware software installed on School devices.
d) Not trying to bypass internet and email filtering platforms used by the School;
e) Being diligent regarding the threat of phishing attacks, especially through the use of emails. Staff are explicitly instructed not to open attachments from links they are unfamiliar with, avoiding suspicious pop-ups or equivalents, and being vigilant for inconsistencies or give aways, e.g. wrong spellings of names;
f) Not using removable media (e.g. memory sticks) without the express permission and support of the IT Network Manager;
g) Completing the necessary annual training and responding to any cyber updates.

To support colleagues our IT procedures have been created to ensure that:

a) Passwords must be of a pre-defined security level and colleagues must currently update them every 180 days. To ensure the security of our systems, all passwords must adhere to the following standards:

i. Length: Passwords must be at least 12 characters long
ii. Complexity: Passwords must include a combination of:

- Uppercase letters (A-Z)
- Lowercase letters (a-z)
- Numbers (0-9)
- Special characters (e.g. ! @ # $ % ^ & *)

iii. Uniqueness: Passwords must not be reused across different accounts or systems
iv. Avoid Common Patterns: Passwords should not contain easily guessable information such as names, birthdays, or common words

b) Multi-Factor Authentication is required for accessing services on the Microsoft Office 365 Platform when outside of the King's School network;
c) A firewall has been created to provide security around the network. The firewall firmware is updated and kept to within current version and last good version;
d) All devices issued by the School including laptops and mobile devices are configured securely. Our Microsoft Platforms (Intune, SCCM, Azure AD, supported by Microsoft Endpoint Security) allows our IT team to monitor all devices individually. We follow a number of principles for secure configuration, which include:

i. Adhering to benchmarks for device and system configuration,
ii. Anti-virus software pre-installed on all machines.
iii. Automatic security patch updating
iv. Device encryption
v. Monitoring end to end actions of cyber event that might happen.

e) Limit access control to only those where it is required. For example:

i. Limit the number of colleagues with admin access to a very small group of IT Technicians with MFA challenge on as many systems as capable;
ii. Regular review of access privileges;
iii. Ensure that SharePoint sharing permissions are understood by site owners, SLT and staff;
iv. Ensure automatic systems for creating, removing and updating users, SharePoint and other systems are functioning correctly.

f) Anti-malware software is loaded on the network and automatically updated. The system has automatic monitoring of malware and suspicious activity, with alarm warnings being sent to relevant teams as deemed necessary.

3. Reporting Incidents or Abuse

Any security breaches or attempts, loss of equipment or any unauthorised use or suspected misuse of IT equipment must be reported immediately to the Headteacher.

We expect all our staff to follow this policy and those who cause security breaches may face disciplinary action.

Students should also be made aware that loss of their personal devices, or malicious account access should be reported to School staff for review.

4. Cyber Security Response

The School has created a Cyber Security Response Plan that outlines the roles and duties of those colleagues responsible in the event of cyber-attack. This is a live document.