Applecroft School

Cyber Security Policy

Review Cycle:	Annually
Committee to Review:	Finance & Premises
Reviewed Date:	November 2024
Next Review Date:	November 2025

Cyber Security Policy

School Vision:

'To be a positive and inspiring community that nurtures each individual and empowers leaders for life.'

School Mission Statement:

'Nurturing Potential, Inspiring Minds, Changing Lives'

School Values:

- Ambition and Leadership
- Kindness and Supportiveness
- Respect and Honesty
- Determination and Resilience

What is the Policy For?

Applecroft School ("the Trust") is obliged to ensure that all its Information Technology (IT) Systems are secure and not subject to improper use. This policy describes the responsibilities for all users, including those of privately owned devices that connect to Trust systems.

Purpose and Scope

The purpose of this policy is to establish systems and controls to protect the School from cyber criminals and associated cyber security risks, as well as to set out an action plan should the School fall victim to cyber-crime.

Cyber-attacks can lead to systems becoming unavailable, data loss, financial loss and reputational damage, Implementation of this this policy reduces the likelihood of these effects.

This policy encompasses guidance from internal audit recommendations, the National Cyber Security as well as the Academy Trust Handbook 2024.

This policy should be read in conjunction with our

- Data Retention Policy
- Data Security Policy
- Data Breach Policy
- Data Privacy Notices

Who is the Policy For?

This policy is for the attention of anyone who is employed by, provides a service to, or volunteers to work at Applecroft School and uses its IT systems either on a Trust owned device or a personally owned device. This includes trustees and members.

What is Cyber-Crime?

Cyber-crime is simply a criminal activity carried out using computers or the internet and includes but is not limited to: hacking, phishing, malware, viruses or ransom attacks.

The following are all potential consequences of cyber-crime which could affect an individual and/or individuals:

- cost;
- confidentiality and data protection;
- potential for regulatory breach;
- reputational damage;
- business interruption; and
- structural and financial instability.

Types of Cyber-Attack

Common types of cyber-attack include:

- ***Malware*** - Malware is a term used to describe malicious software, including spyware, ransomware, viruses, and worms. Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software. Once inside the system, malware can do the following:
    - Block access to key components of the network (ransomware) o Installs malware or additional harmful software.
    - Covertly obtains information by transmitting data from the hard drive (spyware)
    - Disrupt certain components and renders the system inoperable.
- ***Phishing*** - Phishing is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email. The goal is to steal sensitive data like credit card and login information or to install malware on the victim's machine. Phishing is an increasingly common cyberthreat. A Cyberattack made via text message or SMS is known as Smishing.
- ***Man-in-the-middle attack*** - Man-in-the-middle (MitM) attacks, also known as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data. Two common points of entry for MitM attacks are:

1. On unsecure public Wi-Fi, attackers can insert themselves between a visitor's device and the network. Without knowing, the visitor passes all information through the attacker.
2. Once malware has breached a device, an attacker can install software to process all the victim's information.

- ***Denial-of-service attack*** - A denial-of-service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfill legitimate requests. Attackers can also use multiple compromised devices to launch this attack.
- ***SQL Injection*** - A Structured Query Language (SQL) injection occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not. An attacker could carry out a SQL injection simply by submitting malicious code into a vulnerable website search box.
- ***Zero-day exploit*** - A zero-day exploit hits after a network vulnerability is announced but before a patch or solution is implemented. Attackers target the disclosed vulnerability during this window of time.

Phishing (and Smishing)

Whilst cyber-attacks can come in many forms, the number one cause of cyber security breaches is Phishing or Multi-Layered Phishing (Social Engineering).

Phishing emails are designed to trick an individual into divulging sensitive information or will include a malicious link or attachment which if clicked on or opened will download Malware on to your computer and/or network.

Whilst some Phishing emails may contain obvious spelling or grammar mistakes, Cyber Criminals are becoming more sophisticated and may include personal information to give their appearance validity.

Phishing emails will often include 'urgency' and 'authority' cues to pressure you to act quickly and without thinking, for example, your payment has been declined, 'click here to avoid further action', or claim to be from a person in authority, for example a CEO.

Applecroft School employees are expected to be familiar with the organisation's policies and procedures and to double check the validity of an email or instruction if something seems unusual. This checking must **not** be undertaken by responding to the email rather they should telephone a trusted contact.

'Phishers' will use publicly available information to make their emails more convincing so employees should consider reviewing privacy settings on social media settings.

Employees are not permitted to post online about any Company or organisational activity which is not already in the public domain or provided or approved by the Company.

Spotting scam emails is tricky, but things to look out for include:

- official-sounding messages about 'resetting passwords,' 'receiving compensation', 'scanning devices' or 'missed deliveries'.
- emails full of 'tech speak', designed to sound more convincing.
- being urged to act immediately or within a limited time. The message will often claim to be from an authority figure (like a bank, or power company).

Remember, your bank (or any other official organisation) will **never** ask you to supply personal information.

If you have any doubts:

- contact the organisation directly using their official website or social media channels. Do not use the links or contact details in any messages you have been sent.
- Hover over the recipient to see the full originating email address; an email address can be set to appear as something like "Lloyds Bank" in the settings, but if you hover over this name, it could be from 'clicktogetphished@scammer.com'.
- If a suspicious email arrives which is from someone within your organisation, call them to check.

Cyber-Crime Prevention

Given the seriousness of the consequences noted above, it is important for the School to take preventative measures and for staff to follow the guidance within this policy.

This cyber-crime policy sets out the systems we have in place to mitigate the risk of cyber-crime as well as mitigating the risk of falling victim to cyber-crime. These include controls and guidance, cyber security measures, and ultimately a cyber-security incident management plan.

Controls and guidance

The following controls are suitable for all users and provides a non-technical explanation of the key elements of cyber security.

1. Passwords

Passwords are an effective security countermeasure if they are strong and kept confidential. Passwords are a means of validating a user's identity to access a computer

resource, to ensure the security of that resource and to maintain the confidentiality of information held on that resource.

All users must:

- choose strong passwords:
  - Avoid the most common passwords that criminals can easily guess, for example 'passw0rd'.
  - Be made of up of 3 random words – these must not be words which are easily guessed (like a pet's name or anything which is linked to the school, your hobbies, or your children). Numbers and symbols can be included if you need to, for example, 'OrangeToasterExtension5!'
  - Use 2 Factor Authentication (where applicable/available)
  - Not be duplicated/used for multiple accounts

- Keep passwords secret:
  - Not be written down and kept near to your computer. If passwords are written down, they must be kept securely, out of sight.
  - Passwords can be stored in your browser when prompted as this is more convenient and safer than re-using the same password.

- Never allow any other person to access the school's systems using your login details.

2. Firewalls, antivirus software, web filtering, encryption, automatic updates and patches

Firewalls
A firewall is a device or software program that is located between your computer and the internet. It manages data flowing to and from your device, allowing legitimate connections and blocking malicious ones.

Endpoint Protection
Endpoint Protection or Antivirus software when Installed on a computer, scans for malicious software such as computer viruses, malware or ransomware. This protects your computer and data from malicious damage or theft.

Updates and Patches
Security vulnerabilities that enable malicious activity on computer systems are discovered frequently, software companies release security updates and patches on a regular basis. These must be installed to ensure devices have the latest protection. Out of date software increases vulnerability to cyber threats.

All users must:

- not turn off or attempt to circumvent any security measures that the IT team have installed on their computer, phone or network or the School IT systems;
- report if they suspect a firewall is not working or incorrectly blocking a service;
- if they encounter a message that a device is infected with a virus or they suspect it is, turn it off and contact IT immediately;
- not install software onto your School computer or phone. All software requests should be made to the Headteacher.
- avoid clicking on links to unknown websites, downloading large files, or accessing inappropriate content using School equipment and/or networks.
- only access work systems using computers or phones that the School owns. Staff may only connect personal devices with the authority of the school.

3. Remote Working

Remote working relates to accessing Trust systems from external locations. This could be from home, another school or a public place.

All users must:

- only work remotely through the secure methods provided by the IT department such as Remote Desktop (LARA).
- only work on data where it is stored, on secure Trust systems rather than downloading it to your device for editing.
- be aware of your surroundings when working on sensitive data or entering passwords and beware of 'shoulder surfers'.

4. Cyber Security Incidents

A cyber Security Incident is a breach of a system's security in order to affect its integrity or availability, the unauthorized access to or attempted use of a system; or a breach of Trust IT Policies or procedures.

There are a number of forms of cyber incident:

- it could be a virus infection,

- someone having access to data that they should not be able to access,
- a phishing attempt,
- or a complex cyber-attack that causes a system to be unavailable. All users have a responsibility to report cyber incidents.

If you become aware of a cyber-incident or a situation that you suspect could be an incident you should report this immediately to the school Finance & Business Manager. If your concern relates to a data breach you must follow the schools Data Breach Policy.

Cyber Security Measures

The School have implemented the following technical measures to protect against cyber-crime:

(i) firewalls;

(ii) anti-virus software;

(iii) anti-spam software;

(iv) auto or real-time updates on our systems and applications;

(v) URL filtering;

(vi) secure data backup;

(vii) encryption;

(viii) deleting or disabling unused/unnecessary user accounts;

(ix) deleting or disabling unused/unnecessary software;

(x) using strong passwords; and

(xi) disabling auto-run features.

Cyber-security Incident Management Plan

The incident management plan consists of four main stages:

(i) **Containment and recovery:** To include investigating the breach, utilising appropriate staff to mitigate damage and where possible, to recover any data lost.

(ii) **Assessment of the ongoing risk:** To include confirming what happened, what data has been affected and whether the relevant data was protected. The nature and sensitivity of the data should also be confirmed, and any consequences of the breach/attack identified.

(iii) **Notification:** To consider whether the cyber-attack needs to be reported to regulators (for example, the ICO and National Crime Agency) and/or colleagues/parents as appropriate.

(iv) **Evaluation and response**: To evaluate future threats to data security and to consider any improvements that can be made.

Where it is apparent that a cyber-security incident involves a personal data breach, the School will invoke their Data Breach Policy rather than follow out the process above.