Scholars

SCHOLARS ACADEMY TRUST

Fulfilling every child's potential

Cybercrime and IT Security Policy

Written / reviewed: September 2021

Next review: April 2023

Signed: ....

Trustee: S. Richards.

Date: ....4../..11../..21.................

Introduction

Scholars Academy Trust is committed to working to minimise the risks posed by Cybercrime and Cyberterrorism. The more we rely on technology to collect, store and manage information and data, the more vulnerable we become to severe security breaches. Scholars Trust has therefore implemented a number of security measures to mitigate against the risk, and these are summarised in this policy.

This policy applies to all staff, trustees, governors, volunteers and any other individuals with access to the Trust's electronic systems, information, software and/or hardware.

The following Trust policies are linked to this document:

- Risk Management Policy
- GDPR Policy
- Safeguarding Policy
- Debit / Credit Card Policy

Responsibilities

Trustees:

- Setting the trust policy and reviewing compliance and breaches through the Audit and Risk Committee.

Senior Leaders:

- Informing all staff of the responsibilities covered in this policy and their individual responsibilities for IT and data security;
- Reporting related breaches to the Audit and Risk Committee and any associated action taken.

IT Manager:

- Managing access levels in accordance with instructions from senior leaders;
- Keeping firewalls and anti-virus software up to date;
- Reporting to senior leaders on compliance and breaches;
- Ensure there is a register of all IT equipment issued to staff, pupils and volunteers, including desktops, laptops, tablets and mobiles.

Staff and volunteers:

- Adherence to password requirements;
- Awareness of Spam / Phishing techniques used by scammers;
- Keeping data secure;
- Transferring data securely;
- Reporting breaches to line manager and/or IT manager.

Cybercrime

In accordance with the Academy Trust Handbook, no cyber ransom demand will be paid without the express permission from ESFA.

Cyberattacks are anticipated to come from:

- Email interception;
- Ransom Ware (e.g. phishing)
- Creating fake offices;
- Phone calls from banks / suppliers;
- Hacking of accounting systems.

The trust will actively reduce the risk of cybercrime by:

- Giving staff appropriate and regular training and updates on cybercrime;
- Using firewall and antivirus software;
- Reminding staff to use strong passwords and to change them regularly;
- Use encryption to protect information contained in emails or stored on laptops or other portable devices;
- Destroy old computers, backup drives, memory sticks using specialist applications or a reputable contractor;
- Routinely back up data and devices;
- Raising awareness amongst staff of email hacking;
- Teaching staff how to identify phishing messages and how best to check authenticity;
- Ensuring staff know how to minimise the risk of downloading malware;
- Reminding staff of the risks of using public Wi-Fi.

Trust staff will be trained to ensure that they:

- Understand the need for strong and unique passwords;
- Never disclose passwords on phone / by email;
- Understand how to keep data secure when storing and transferring it;
- Know how to report a potential breach of IT security.

We will prepare a response plan covering the internal procedures the Trust will put in place following a potential cyberattack, which will provide a contingency process for managing the business.

Access to network and data

The Trust will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that:

- Firewall and antivirus software is up to date and installed on all trust issued devices;
- A register is kept of all IT equipment issued by the trust;
- Users can only access confidential data to which they have a right of access;
- Access to personal data is securely controlled in line with the school's personal data procedures;
- Logs are maintained of access by users and of their actions while users of the system;
- There are regular reviews and audits of the safety and security of school computer systems;
- There is an oversight from senior leaders and these have impact on policy and practice.

Technical Security

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.

- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.

- All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the Technical Staff (or other person) and will be reviewed, at least annually by a Senior Leader.

- Users are responsible for the security of their username and password, they must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security to their line manager or senior leader.

Password summary
A safe and secure username/password system is essential and will apply to all school technical systems, including networks and email.

- All school networks and systems will be protected by secure passwords that are regularly changed (at least once every 90 days);
- The "master/administrator" passwords for the school's systems, used by the technical staff must also be available to the Headteacher or other nominated senior leader and kept in a secure place i.e. school safe;
- Usernames for new users will be allocated by the IT technicians and kept on a master list. Passwords are only known by the user;
- All users (adults and children) will have responsibility for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security;
- Lost passwords are reported to technician who will reset the account;
- All documents emailed containing personal details will be password protected or sent through an encrypted email service.

Password security
The following minimum standards apply to passwords used for trust business:

- Should be a minimum of 8 characters long and must include uppercase character, lowercase characters, numbers and special characters;
- The account should be "locked out" following six successive incorrect log-on attempts, the IT technician will then reset the account;
- Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on;
- When entering passwords, the characters shall not be displayed on screen;
- Should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school;
- Should not be re-used and be significantly different from the previous password.

Pupil Passwords

- All pupils will be provided with an individual username and password;
- Pupils will be taught the importance of password security;
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.

Training / Awareness
Senior Leaders are responsible for providing training and awareness to staff on IT security and Cybercrime, and will do this through:

- This policy;
- At induction;
- Through the Acceptable Use Agreement;
- Through regular updates from the trust IT manager.

Pupils will be made aware of the school's password policy through:

- Lessons;
- The Acceptable Use Agreement.

Monitoring
This policy will be reviewed on a biannual basis or sooner if monitoring or other information comes to light