Cyber Security Policy

Person Responsible	Fiona Richards
Approved by Directors	
First Written	August 2023

For Review	Reviewed	Signature
July 2024	Completed	Fiona Richards
July 2025	Completed	Fiona Richards
July 2026		
July 2027		
July 2028		
July 2029		

All policies are renewed annually. If no change then just signed.
If an amendment or full change is required, this is recorded.

Contents

Cyber Security at Acorn Education Trust

Definition – Cyber security is the protection of devices, services, networks and information on them from theft or damage via electronic means. (NCSC 2019)

Academy handbook – 6.16 *"Academy Trusts must be aware of the risk of cyber-crime, put in place proportionate controls and take action where a cyber security incident has occurred"*.

Targets:

1. Strengthen our cyber security awareness:
    a. Ensure we have strong structures and partnerships internally and externally
    b. Enhance and expand the skills of our staff at every level
2. Continue to build and maintain a resilient and prosperous digital system:
    a. Improve our understanding of cyber risk at every level
    b. Prevent and resist cyber attacks by improving the management of risk
3. Develop resilience in the organisation to prepare for, respond to and recover from a cyber-attack:
    a. Stay up to date on technologies vital to maintain cyber security
    b. Ensure we have the resources to act on science and technology development
    c. Provide the resources to keep IT equipment up to date

Scope of the Policy

This policy applies to all settings and staff within Acorn Education Trust who handle, process, or have access to the Trust's data and information assets. This includes all staff, governors, Trustees, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware. The policy applies to all staff whether they are working in a setting or remotely.

The policy should be read in conjunction with the:

- Acorn Education Trust Data Breach Policy
- Acorn Education Trust Information Security Policy
- Acorn Education Trust Acceptable Use of IT policy

Introduction

The purpose of this policy is to highlight to the Trustees and all staff of the potential risks of cyber-attacks for the school, and to present a consistent approach to prevent such events occurring, and the procedures that need to be followed in the event of a cyber incident.

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. 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. A number of schools have been forced to pay ransomware so that they can recover their data.

The complexity and variety of cyber-attacks 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.

This cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure. The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human error, hacker attacks and system malfunctions could cause great damage and may jeopardise our school's reputation or threaten our finances.

For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

It is important to remember that not all incidents are the result of malicious acts and some outcomes may look like a cyber attack but are not. For example, the loss of internet to a school might be a malicious act or might be due to an outage in the local area. Because of this, we will refer to cyber incidents and consider them to be potential threats. We will respond to any cyber incident assuming it could be malicious in order to protect the systems in the Trust.

Risks

There are many risks associated with a cyber incident. These include:

- Financial risks, for example, ransoms demanded, costs of the recovery of data, costs for the replacement of hardware, compensation and fines around any loss of data.
- Reputational. We are trusted with the security of data of staff and our students. We hold highly sensitive safeguarding, medical, personal and educational information.
- Data breach. Some incidents can lead to a GDPR data breach.
- Permanent loss of data. We could lose access to data, both personal and educational (eg. Coursework for external assessments).
- Operational. We are heavily reliant on computer systems and any attack would create a disruption to everyday running of the settings.
- Safeguarding. If we lose access to systems in the day, we would lose access to information about the students.
- Exposure of minors to inappropriate content and contact.
- Accuracy of data. Hackers could change data in the school.

Roles and Responsibilities

Trustees and the CEO	Quality assure the response to cyber security via the A&R committee.
Head of Acorn IT	Responsible for ensuring that there are technical defences in place. Responsible for responses to any possible attack.
Head teachers	To ensure that all staff are trained and that the policy is followed. To ensure that breaches are reported to Acorn IT.
All staff – including contractors and volunteers	Comply with this policy, follow established security protocols, and actively participate in cyber security awareness and training. To report any incidents to the setting's cyber security officer. For particulars see below.
IT team	Responsible for managing and implementing cyber security measures, including ensuring that software is up to date. Responsible for ensuring that the Trust's IT solution meets the DFE standards and any other published applicable standards. Ensure that antivirus, firewall, filtering and other digital security software is installed and is regularly updated. To review and audit the Trust's IT solution annually. In some schools IT is provided via a third party.
Computing curriculum leads	To raise awareness with students about cyber security and how to prevent incidents.

Where might a threat originate?

- **Online Criminals** Some criminals are good at identifying what can be monetised, for example stealing and selling sensitive data, or holding systems and information to ransom.
- **Hackers** Individuals with varying levels of expertise, often operating in an untargeted way, to disrupt just for the sake of it.
- **Malicious** Insiders use the access they have to conduct malicious activity.
- **Honest mistakes** Sometimes staff will just make an honest mistake, and this can leave the Trust vulnerable to a cyber attack.
- **Students** Some students might enjoy the challenge of putting their IT skills to the test. In addition, they can, like staff, make honest mistakes which leave the Trust vulnerable to an attack.

A list of the different types of threats is in Appendix B.

Staff Responsibilities

All Acorn education staff including Trustees, governors, contractors and volunteers who have access to Acorn Education hardware and data must adhere to the following measures to mitigate cyber security risks: -

- If a member of staff leaves their workspace they must use screen lock (*windows button + L*). Screens should be locked when unattended even for short periods, such as toilet breaks.
- Staff must not allow students to use their devices, unless the student has logged into their own account.
- The use of external hardware should be limited and any extra risks considered carefully.
- Management of computers and/or networks is controlled via the Acorn IT department.
- Users shall not install software onto any school IT system, for any purpose, unless authorised to do so by the IT Department. Administrator privileges are required in order to install any software.
- Passwords should never be shared with any other person.
- Disposal of equipment is allowed only by authorised personnel.

Business continuity is assured by continually reviewing our information systems, in particular:

- That information shall be available to properly authorised personnel as and when it is required.
- Relevant information security awareness and training is regularly available and accessible to staff.
- All cyber incidents, actual or suspected, are recorded, reported and investigated and mitigating measures put into place to prevent a re-occurrence Potential or Actual Security Breaches.
- All staff within the Trust are responsible for ensuring that no potential or actual security incidents occur as a result of their actions.

Simple measures to avoid cyber incidents

Protect personal and school devices
In general, staff should try to only use Trust-issued devices to access school emails, accounts or folders. We advise our staff to keep both their personal and school-issued computer, tablet and mobile phone secure. They can do this if they:

- Keep all devices password protected.
- Ensure that the school-installed antivirus software (ESET) is installed on their school-owned computer and that they have anti-virus software installed on home computers/devices.
- Ensure they do not leave their devices exposed or unattended.
- Log into school accounts and systems through secure and private networks only. We also advise our staff to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.
- Antivirus / anti -malware software is installed on all Trust owned devices and we advise all staff to have antivirus software installed on their own devices.

Keep emails safe
Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct staff to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing.")
- Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- Check email and names of people they received a message from to ensure they are legitimate.

- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)
- If a member of staff isn't sure that an email they received is safe, they can refer to the IT department.

See the section in the Acceptable Use of ICT Policy for further details on email etiquette and email security.

Manage passwords properly
Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, we advise our staff to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays). General guidance on creating a password is to take three random words. To meet the criteria for many passwords you will also need to capitalise a letter and add a number and a special character – e.g. DinosaurStarRose14%. This is considered best practice by the National Cyber Security Centre.
- Consider using a password manager. This will allow you access sites across the devices you use. You will need to remember the password for the password manager.
- Remember that companies will not ask for your passwords.
- In addition to good password management, Acorn Education Trust will be requiring its employees to use two factor or mutli-factor authentication (MFA) when logging into email accounts, Arbor or other data, unless on a school site.

Transfer data securely
Transferring data introduces security risk. Staff must:

- Avoid transferring sensitive data (e.g. customer information, staff records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request staff to ask our IT department for help.
- Share confidential data over the school network/ system and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies.
- Ensure that data is sent to the correct email addresses/contacts and take particular care when sending mass emails (eg. via BCC facility). When contacting parents use the Arbor facility wherever possible and ensure that any attachments do not contain any personal information about anyone other than the recipient or their children.

Additional measures
To reduce the likelihood of security breaches, we also instruct staff to:

- Turn off screens and lock devices when leaving desks.
- Report stolen or damaged equipment as soon as possible to IT
- Change all account passwords at once if a device is stolen.
- Refrain from downloading suspicious, unauthorised or illegal software on school equipment.
- Avoid accessing suspicious websites.

Procedures in the event of a cyber incident

Phishing attack	If a member of staff receives a suspicious email then they should not open any attachment or click on any links. InformRob Knott (Head of IT) rkk@acorneducationtrust.com (For an indication of how to look out for Phishing emails see Appendix A)
Unusual activity	If a member of staff sees anything unusual then they should contact IT. If this follows an event such as a phishing email they should contact the CSO as soon as possible. Examples of unusual activity include: - • The device running very slowly. • Pop up adds. • New files / folders appearing.
Password	If a member of school staff suspects that their password is known to anyone else, then: - 1. It should be reported to central IT as soon as possible via IT help desk or rkk@acorneducationtrust.com 2. IT will change the password with immediate effect.
Disruption to IT / internet	Report to IT If there is any doubt as to the origin of the disruption this should also be reported to the cyber security team.
Ransomware	If a member of staff receives a demand for data / systems being ransomed they must: - 1. Report it to the Rob Knott (Head of IT) immedidately – rkk@acorneducationtrust.com 2. No contact should be made with cyber criminals. 3. The Trust IT lead will inform the Trustees / CEO.
Data breach	If any cyber incident or mistake leads to personal data being disclosed, then staff must follow the Data Breach policy and contact Fiona /Jo Ronxin.

Training and Awareness

The Trust will ensure annual training for all staff. This will be delivered via each setting's headteacher or delegated member of staff.

In addition, the team will arrange adhoc training where there are updates and changes to threats and / or procedures.

Training will be provided to any member of staff who accidentally puts the Trust at risk of a cyber security incident. (E.g., if a member of staff clicks on a link in a phishing email).

Review and Compliance

Policy Review This cybersecurity policy shall be reviewed and updated periodically to reflect changes in technology, regulations, and organizational requirements. Amendments may be made as necessary.

Summary

Everyone, from our parents, students, staff, visitors and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.

Cybercriminals use a variety of methods based on their motive to attack school systems. Schools should have robust IT infrastructure and data protection policies to deter possible cyber-attacks. 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.

Guidance

- The National Cyber Security Centre (NCSC) www.ncsc.gov.uk
- The National Security Strategy 2016 – 2021 www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021
- The Information Commissioner's Office (ICO) https://ico.org.uk/
- HSCIC now NHS Digital https://digital.nhs.uk/
- Cyber Aware www.cyberaware.gov.uk
- Cyber Essentials (CE) www.cyberessentials.ncsc.gov.uk
- Get Safe Online www.getsafeonline.org
- Action Fraud www.actionfraud.police.uk
- ISO/IEC 27001 – Information Security Standard www.iso.org/isoiec-27001-information-security.html
- ISO/IEC 27002 - Security techniques - Code of practice for information security controls https://www.iso.org/standard/75652.html
- ISO/IEC 27005 - Information Security Risk Management https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27005:ed-4:v1:en
- ISO/IEC 22301 – Business Continuity Standard www.bsigroup.com/en-GB/iso-22301-business-continuity/
- ISO/IEC 22313 - Business Continuity Management Systems — Guidance www.bsigroup.com/en-GB/Cyber-Security/Cyber-security-for-SMEs/Managing-your-IT-and-cyber-security-incidents/Standards-for-managing-IT-security-incidents/
- Strong Password Generator https://strongpasswordgenerator.com/

Appendix A Watch out for phish!

In a typical phishing attack, scammers send fake emails to thousands of people asking for sensitive information (such as bank details) or containing links to bad websites. They do this to steal your details to sell or perhaps to access your organisation's information. Reducing phishing emails needs to happen at different levels.

• '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 Head Teacher or IT team as soon as possible so they can try to minimise any damage.

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

- Phishing flags 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?

Appendix B Threats

A threat if left unchecked, could disrupt the day-to-day operations of the school, the delivery of education and ultimately has the potential to compromise local and national security.

Cybercriminals and Cybercrime

Cybercriminals are generally working for financial gain. Most commonly, for the purposes of fraud: either selling illegally gained information to a third party, or using directly for criminal means. Key tools and methods used by cybercriminals include:

- **Malware** – malicious software that includes viruses, Trojans, worms or any code or content that could have an adverse impact on organisations or individuals.

- **Ransomware** – a kind of malware that locks victims out of their data or systems and only allows access once money is paid 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.

- **Phishing attack**
  A phishing attack comes in the form of emails purporting to come from a public agency with the sole intention of extracting sensitive information from members of the public. They might appear to come from another member of the school community or an organisation that the school works with.

  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.

- **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 are also sold on the dark web by criminal gangs that have been leaked or

hacked from organisations. A good practice to follow is not using the same password twice.

- **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)**
  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.

Hacktivism
Hacktivists will generally take over public websites or social media accounts to raise the profile of a particular cause. When targeted against local government or school websites and networks, these attacks can cause reputational damage locally. If online services are regularly disrupted by cyber-attacks this could lead to the erosion of public confidence in using such services. Hacktivist groups have successfully used distributed denial of service (DDoS – when a system, service or network is burdened to such an extent by an electronic attack that it becomes unavailable) attacks to disrupt the websites of a number of councils already.

Insiders
Staff may intentionally or unintentionally release sensitive information or data into the public domain. This may be for the purpose of sabotage or to sell to another party, but more often than not is due to simple human error or a lack of awareness about the particular risks involved.

Zero-day threats
A zero-day exploit is a cyber-attack that occurs on the same day a weakness is discovered in software. At that point, it's exploited before a fix becomes available from its creator. It is an attack that exploits a previously unknown security vulnerability. This poses a risk to any computer or system that has not had the relevant patch applied, or updated its antivirus software.

Physical threats
The increasing reliance on digital services brings with it an increased vulnerability in the event of a fire, flood, power cut or other disaster, natural or otherwise, that impacts upon our IT systems.

Terrorists
Some terrorist groups demonstrate intent to conduct cyber-attacks, but fortunately have limited technical capability. Terrorist groups could obtain improved capability in a number of ways, namely through the sharing of expertise in online forums providing a significant opportunity for terrorists to escalate their capability.

Espionage
Several of the most sophisticated and hostile foreign intelligence agencies target UK government and public sector networks to steal sensitive information. This could ultimately disadvantage the UK in diplomatic or trade negotiations, or militarily.