FORWARD AS ONE CE ACADEMY TRUST

Digital/Cyber Security Policy

Approved by:	Trust Board	**Date:** 19.07.24
Last reviewed on:	19.07.24	
Next review due by:	31.08.25	

Updates and amendments

Date	Policy section	What's changed?	Why?
January 2025		Cyber Security Link Trustee appointed	

Table of Contents

1. Policy brief and purpose

The Forward As One cyber security policy outlines the 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 financial damage and may jeopardize our organisations' reputation.

For this reason, the Trust has implemented several security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

Our Cyber Security link trustee is Michael Crossley (crossleym@fa1.uk)

2. Scope

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

3. Policy elements

3.1 Confidential data

Confidential data is secret and valuable. Common examples are:

- Unpublished financial information
- Data of pupils'/staff/ parents/outside agencies / service providers
- Patents, formulas or new technologies
- Pupil lists (existing and prospective)

All employees are obliged to protect this data. In this policy, we will give our employees instructions on how to avoid security breaches.

3.2 Protect personal and company devices

When employees use their digital devices to access Forward As One emails or accounts, they introduce security risk to our data. We advise our employees to keep both their personal and company-issued computer, tablet and mobile phone secure. They can do this if they:

- Keep all devices password protected.
- Choose and upgrade a complete antivirus software.
- Ensure they do not leave their devices exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into Forward As One systems through secure and private networks only.

We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

When new employees receive Trust / school issued equipment they will receive instructions for:

- [*Disk encryption setup*]
- [*Password management tool setup*]
- [*Installation of antivirus/ anti-malware software*]

They should follow instructions to protect their devices and refer to our IT Network Support, Computeam, if they have any questions.

3.3 Keep emails safe

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct employees 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 giveaways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If an employee isn't sure that an email, they received is safe, they can refer to our IT Specialist, Computeam

3.4 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, Forward As One advise our employees 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.)
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Exchange credentials only when absolutely necessary. When exchanging them in person isn't possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- Change their passwords every three months.

3.5 Transfer data securely

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g. pupil information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees to ask Computeam for help. In most instances such transfer will take place as CTF, be password protected / WinZip Folders – encrypted.
- Share confidential data over the Trust/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.
- Report scams, privacy breaches and hacking attempts

Our IT provider, Computeam, need to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists. Our IT Provider must investigate promptly, resolve the issue and send a Trust wide alert when necessary.

Our IT provider is responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to them with any questions or concerns.

3.6 Additional measures

To reduce the likelihood of security breaches, we also instruct **our employees to**:

- Turn off their screens and lock their devices when leaving their desks/ classrooms
- Report stolen or damaged equipment as soon as possible to the Headteacher

- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in Forward As One systems.
- Refrain from downloading suspicious, unauthorized or illegal software on their company equipment.
- Avoid accessing suspicious websites.

We also expect our employees to comply with the social media and internet usage policy.

Our IT Network Providers should:

- Install firewalls, anti-malware software and access authentication systems.
- Arrange for security training to all employees.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policies provisions as other employees do.

Forward As One will have all physical and digital shields to protect information.

4. Remote working

When working remotely all employees must follow this policy's instructions. Since they will be accessing Forward As One systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure. We encourage them to seek advice from our IT Network Providers when and where appropriate.

5. Disciplinary Action

We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: We may issue a verbal warning and train the employee on security.
- Intentional, repeated or large-scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination.

  We will examine each incident on a case-by-case basis.

Additionally, employees who are observed to disregard our security instructions will face progressive discipline even if their behaviour hasn't resulted in a security breach.

6. Take security seriously

Everyone, from our children and parents to our employees 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.