Fairfield School
Embracing Uniqueness

Cyber Security Policy

Nov 2020

Version	1.0
Date Approved by Governors:	10th Nov 2020
Review date:	10th Nov 2022
Version History	

Policy brief & purpose

Our 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 too severe security breaches. Human errors, hacker attacks and system malfunctions could cause financial and reputational damage. 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.

Scope

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

Policy Elements

1. **Confidential data** is secret and valuable. Common examples are:
    - Student, parent & staff details
    - Academic data
    - Financial information

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

2. Protect personal and school devices

When staff use their digital devices to access school emails or data, they introduce a potential security risk to our data. We advise 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.
- Choose and upgrade a complete antivirus software.
- Ensure they do not leave their devices exposed or unattended.
- Log into the school portal / systems through secure and private networks only.
- Avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.
- Follow instructions from our IT partners to protect their devices.

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 give-aways (e.g. grammar mistakes, capital letters, excessive
- number of exclamation marks.)
- If a colleague isn't sure that an email, they received is safe, they can refer to our IT partners

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, 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.)
- 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, staff should prefer the phone instead of email, and only if they personally recognise the person they are talking to.
- Change their passwords every term.

5. Transfer data securely

Transferring data introduces security risk. Staff must:

- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees to ask our IT partners for help.
- Share confidential data over school's 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 partners need to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise staff to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists. Our IT partners must investigate promptly, resolve the issue and send a school alert when necessary. They are responsible for advising employees on how to detect scam emails. We encourage our colleagues raise any questions or concerns.

6. Additional measures

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

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

We also expect our employees to comply with our acceptable use policy.

Our IT partners will:

- Install firewalls, anti-malware software and access authentication systems.

- Arrange for security training to all employees.
- Inform staff regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policy provisions as other employees do.

School will have all physical and digital shields to protect information.

7. Remote employees

Staff remotely accessing the school's portal should follow this policy's instructions too. Since they will be accessing school's 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 partners.

8. Disciplinary Action

We expect all staff 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, staff who are observed to disregard our security instructions may face disciplinary action, even if their behaviour hasn't resulted in a security breach.

Take security seriously

Everyone 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.