Policy reviewed and updated	08/05/2025
Date of next review	08/05/2026
This policy will be subject to ongoing review and may be amended prior to the scheduled date of the next review in order to reflect changes in legislation where appropriate	

Policy brief & purpose

Harefield School has created this cyber security policy that outlines our guidelines and provisions for preserving the security of school 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 errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardise the school's reputation.

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

Scope

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

Policy elements

Confidential data

Confidential data is secret and valuable. Common examples are:

- Unpublished financial information
- Data of customers/partners/vendors
- Patents, formulas or new technologies
- Customer lists (existing and prospective)

All employees are obliged to protect this data. In this policy, instructions are given on how to avoid security breaches.

Protect personal and company devices

When staff use their digital devices to access school emails or accounts, they introduce security risks to our data. Staff are advised to keep both their personal and school-issued device secure. They can do this if they:

- Keep all devices password protected.
- Choose and upgrade antivirus software.
- Ensure devices are not left exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into school accounts and systems through secure and private networks only.

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

Devices allocated for new staff are set up with antivirus software. They should follow instructions to protect their devices and refer to our IT Support team if they have any questions.

Keep emails safe

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, staff are instructed 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 any member of staff isn't sure that an email they received is safe, they can email our IT manger or visit the IT office.

Manage passwords properly

Password leaks are dangerous since they can compromise the school 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 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 staff 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 recognize the person they are talking to.
- Change their passwords every three months.

Transfer data securely

Transferring data introduces security risk. Employees 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 IT for help.
- Share confidential data over the school network/ system and not over public Wi-Fi.
- 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.

IT need to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise all staff to report perceived attacks, suspicious emails or phishing attempts as soon as possible to the IT Manager. IT must investigate promptly, resolve the issue and send a whole-school alert when necessary. Staff are encouraged to contact IT with any questions or concerns, as they are responsible for advising everyone how to detect scam emails.

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 to IT.
- 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 staff to comply with our social media and internet usage policy.

Our Network Admins should:

- Install firewalls, antivirus software and access authentication systems.
- Arrange for security training for all employees.

- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policy's provisions as other employees do.

Remote working

This policy also applies to anyone working remotely. Since they will be accessing our company's accounts and systems offsite, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.
Staff can speak to IT for help with this if they require assistance.

Disciplinary Action

We expect 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 will face progressive discipline, even if their behaviour hasn't resulted in a security breach.

Take security seriously

Everyone, from staff, pupils, 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 at the forefront of our working routines.