PRENTON HIGH SCHOOL FOR GIRLS

Making a positive difference today to achieve a better tomorrow

PRENTON HIGH SCHOOL FOR GIRLS

CYBER SECURITY POLICY

INTRODUCTION

The Prenton High School 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 attack, system malfunction and insider threat (I.e. a malicious act from an employee) could cause great financial damage and may jeopardize the reputation of the school.

Although Prenton High School has invested in technical measures to combat cyber security, we cannot solely be reliant upon this. It is recognised that we all need to be vigilant and it is the responsibility of everyone to protect our data and IT systems.

SCOPE

This policy applies to all our Staff, Students, Governors, and anyone who has permanent or temporary access to our systems and hardware.

POLICY ELEMENTS

Confidential data

Confidential data is secret and valuable, and should only be visible/accessible by persons it is intended for, Common examples are:

- Unpublished financial information.
- Data of staff, Students, and/or Governors.
- Emails / online data
- Any data school deems confidential and/or sensitive.

Everyone is obliged to protect this data as listed in this policy.

Protect personal and school devices

Prenton High School expect all staff, students, Governors, and anyone who has permanent or temporary access to our systems and hardware to keep both their personal and school-issued computers, tablets and mobile phones secure. They can do this if they:

- Keep all devices password protected.
- Do not share or allow access to login details supplied to them
- Do not leave devices unprotected and exposed.
- Do not allow others to use their personally owned device within school.
- Do not allow others to use a device loaned directly to them.
- Do not use or transport data on removable devices unless they are encrypted and password protected.
- Lock their computers/devices when leaving the desk/room
- Only log into school accounts and systems through secure and private networks only.
- There should be no interference with school devices in their automatic anti-virus and security updates.
- Personal owned devices should be kept updated with the most recent security and antivirus updates if used within the school.
- Users can only access data to which they have the right to access

- Do not allow any third-party company or person remote access without prior authorisation from the IT department.

Working from Home.

- Devices are directly loaned to staff or students for the sole use of the person.
- Devices are not to be shared with family or friends.
- Devices must not be prevented from updating pre-loaded security software.
- Do not install/uninstall applications without authorisation from the IT department.
- Do not make changes to the accounts or features on the device.
- Follow the same guidance as above to protect school devices.

In the event of loss or a stolen device, the IT Strategic Manager must be informed immediately to help prevent data loss or theft.

Keep emails safe

Emails often host scams and malicious software, 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.
- Be suspicious of clickbait titles (e.g., offering prizes, advice).
- Check the email and names of recipients to ensure they are legitimate.
- Look for inconsistencies or giveaways (e.g., grammatical errors such as, capital letters, an excessive number of exclamation marks).

If staff are unsure about an email they have received, they should seek advice from the IT team.

Managing passwords

Password leaks are dangerous since they can compromise the 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 everyone to:

- Choose a password with at least seven 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 you need to write a password, you are obliged to keep the paper or digital document confidential and destroy it when the work is done.
- There should be no exchange of credentials.
- Change the password every three months.
- For password complexity, an alpha numerical system is in use with special characters and a mix of MFA (Multi-Form-Authentication). This is governed by the IT security and is subject to change, these changes will be relayed by the Strategic ICT Manager.

Remembering a large number of passwords can be daunting. The IT team will use a password management tool which generates and stores passwords, these are frequently changed as part of its Disaster Recovery practices. Staff are obligated to create a secure password for their use following the abovementioned advice.

Secure transfer of data

Transferring data introduces security risks. Staff must:

- Avoid transferring sensitive data (e.g., customer information, staff or Students' records) to other devices or accounts unless necessary. When the mass transfer of such data is needed, Staff must ask the IT Department for help.
- The IT department has systems to monitor the transfer of files.
- 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.
- Report scams and hacking attempt promptly to the Strategic ICT Manager for action.

The IT department must be informed of scams and malware so they can continue to protect the infrastructure. For this reason, it is advised to report all perceived attacks, suspicious emails, or phishing attempts as soon as possible to the Strategic ICT Manager.

The IT department will investigate promptly, resolve the issue, and send a schoolwide alert where necessary.

The Strategic ICT Manager is responsible for advising staff and governors on detecting scam emails. Whilst students will follow guidance from the E-Safety Teacher.

Additional measures

To reduce the likelihood of security breaches, staff are instructed to:

- Turn off screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to the IT Department who will lock, repair or trace the device.
- 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 school equipment in line with the Staff Acceptable Use Policy and Information and Communication policy
- Avoid accessing suspicious websites.

The Strategic ICT Manager will:

- Install firewalls, anti-malware software and access authentication systems.
- Ensure onsite and offsite backups are in place.
- Arrange for security training for all staff annually.
- Inform staff regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow the policy provisions as other staff do.

Prenton High School will ensure that all physical and digital shields are in place to protect the integrity of the data.

Remote Staff working

Staff working remotely must continue to follow this policy. Accessing school accounts and systems from a distance, requires staff to follow all data encryption, protection standards and settings, and ensure their private network is secure.

Staff must seek advice from the Strategic ICT Manager if unsure of the expectation.

DISCIPLINARY ACTION

Staff are expected to follow this policy at all times.

Staff who are observed to disregard the security instructions and those who knowingly cause a security breach may be dealt with under the disciplinary policy.