

PRENTON HIGH SCHOOL FOR GIRLS POLICY

STUDENT ACCEPTABLE USE POLICY

Reviewed:	Summer 2026
Ratified:	Summer 2026
Next Review:	Summer 2027

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

STUDENT INTERNET ACCEPTABLE USE POLICY

PURPOSE

This Student Internet Acceptable Use Policy is aimed at encouraging responsible behaviour and good practice. It has been created with the view to:

Ensure compliance and enforcement of relevant legislation which include but is not limited to the Computer Misuse Act and the Data Protection Act; • Ensure the safety and integrity of students, staff and others;

- Prevent damage to the school and its physical property.

POLICY STATEMENT

- Prenton High School reserves the right to amend this Acceptable Use Policy, at any time, without notice. It is the student's responsibility to ensure that they are up to date with such changes.
- This Acceptable Use Policy replaces and supersedes all previous versions.
- A copy of the most recent Acceptable User policy will be held on the school's website.

ELECTRONIC MAIL (E-MAIL) AND REMOTE ACCESS

All students will be provided with email services for school-related communication.

- This email account is to be used only for school-related emails.
- Students can email any valid email address.
- While Prenton High School respects the privacy of students, where there is a reason for concern, the school reserves the right to monitor and intercept e-mail communication.
- Any e-mail communication made must not bring the School into disrepute; this includes anything libellous, defamatory or criminal.
- This pertains to all external cloud services, e.g. cloud-based email, document storage, inclusive of Google Drive, OneDrive or other "cloud-based" storage solutions utilised by Prenton High School, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (Paas), are also considered for school-only use and are subject to the same reserves for monitoring and review.
- Any data stored within school accessible storage that relates to an associated school email address or accessible via school school-hosted system must be solely for school use; any data that contravenes any Act mentioned therein would be subject to review.
- Student email addresses must not be used to sign up for any subscriptions, social media, streaming services, or other platforms not authorised by Prenton High School or approved academic learning platforms. This includes, but is not limited to, media services such as Netflix, Prime, YouTube, and social media platforms like Facebook, Instagram, Snapchat, WhatsApp, TikTok, WeChat, Messenger, Telegram, LinkedIn, Twitter (X), Reddit, Pinterest, Discord, and Tumblr.
- Student email addresses must not be used for any online shopping.

INTERNET ACCESS

- By logging onto Prenton High School network, students are agreeing to the Acceptable Use Policies that are located on the School Website for review.
- All Internet access is logged to maintain standards of security and acceptable use.
- Attempts to access inappropriate websites or websites which attempt to bypass filtering systems constitute a breach of this Acceptable Use Policy.
- Inappropriate websites, but are not limited to any site which contains:
 - Pornographic Material (of either a legal or illegal nature);
 - Material which incites hatred or discrimination;
 - Material which promotes illegal activity;
 - Material which is in breach of the Copyright Designs and Patents Act 1988;
 - Material which is degrading to people or groups of people.
- Students are required to report any website that they become aware of, which is not filtered, that is deemed inappropriate as per the criteria stated above.
- Students should refrain from downloading large files during school hours, as this may affect the quality of service for other users.
- While Prenton High School implements appropriate filtering and monitoring systems and takes reasonable steps to minimise the risk of users accessing harmful or inappropriate content, no filtering solution can provide complete protection or guarantee that all unsuitable material will be blocked. The school regularly reviews and updates its filtering and monitoring arrangements in line with statutory guidance and identified risks. Any concerns relating to inappropriate content or online activity should be reported immediately in accordance with the school's safeguarding procedures.

NETWORK ACCESS

- Student logins must only be used by the student to whom they are issued. Liability remains with the logged-in user.
- Allowing another person to use your login is a severe breach of this Acceptable Use Policy and contravenes legislation.
- Passwords must never be divulged to anyone at any time.
- If it is suspected that a password has been compromised, it must be changed immediately.
- Students will not attempt to download or install software onto the network or IT Equipment.
- It is prohibited to copy any software or inappropriate material onto the network.
- Students understand that the right is reserved to remotely monitor and intercept network activity.

AI TECHNOLOGIES

Prenton High School for Girls recognises the potential of AI technologies to enhance learning and creativity. However, students must use these technologies responsibly and ethically, and they are not permitted to be used to replace or enhance their work.

- Unauthorised use of AI technologies for educational purposes is prohibited unless under the supervision of staff.
- Students must ensure that AI technologies are used in a manner that respects the rights and privacy of others.
- AI-generated content must not be used to deceive, mislead, or harm others.
- Students must not input personal or sensitive information into AI systems.
- AI technologies must not be used to plagiarise or cheat.
- All AI-assisted work must be properly attributed and documented.
- School emails are not permitted to be used in any AI platform that is not authorised by Prenton High School for Girls.

MONITORING AND COMPLIANCE:

- Prenton High School for Girls reserves the right to monitor the use of AI technologies to ensure compliance with this policy.
- Any misuse of AI technologies will be subject to review and disciplinary action.

AI Technologies that are prohibited without authorisation include (but are not limited to) the examples below:

- Chatbots and virtual assistants (Google Assistant, Siri, Amazon Alexa)
- AI-based research tools (Chatgpt, Grok, Claude, Llama, Gemini, DeepSeek)
- Machine learning applications (TensorFlow, Keras, Scikit-learn)
- AI for creative projects (DALL-E, DeepArt, AIVA)
- AI for communication (Grammarly, QuillBot, Hemingway Editor)

LEGISLATION

- All network users are bound by current relevant legislation. The applicable laws (as amended) include, but are not limited to:
 - Computer Misuse Act 1990
 - Copyright, Designs and Patents Act 1988
 - Criminal Justice Act 1988
 - Defamation Act 2013
 - Freedom of Information Act 2000
 - Human Rights Act 1998
 - Obscene Publications Acts 1959 and 1964
 - Protection of Children Act 1978
 - Protection from Harassment Act 1997
 - Public Order Act 1986
 - Telecommunications Act 1984
 - Malicious Communications Act 1988
 - Communications Act 2003

- Regulation of Investigatory Powers Act (RIPA) 2000
 - Investigatory Powers Act 2016
 - Equality Act 2010
 - Data Protection Act 2018
 - UK General Data Protection Regulation (UK GDPR)
- Students should understand that any attempt to bypass the School or other network security systems, including the introduction of viruses or applications of a destructive nature, could lead to prosecution.
 - Where it is believed that a student is in breach of legislation, appropriate action will be taken.

ICT EQUIPMENT AND SUITES

- Students may not move any ICT equipment without prior consent or instruction.
- Students are not allowed to use the ICT suites or classroom systems without suitable supervision by a member of staff.

ADDITIONAL SYSTEMS

- Students may have access to additional systems which include, but are not limited to: The school's Learning Platform, Student Email, Exam software, and Remote Applications.
- These systems may require additional passwords. It is the responsibility of the students to ensure that their password meets the complexity set out by the school and that their password is only known to them.

SANCTIONS

In the event that this Acceptable Use Policy is breached, Students will be subject to sanctions which may include, but are not limited to:

- Disciplinary procedures;
- Temporary or permanent restriction of network access;
- Temporary or permanent revocation of network rights;
- Restriction to or denial of access to ICT Suites;
- Investigation in accordance with the Data Protection Act 2018, including the Investigatory Powers Act 2016 and Regulation of Investigatory Powers Act 2000).
- Temporary or permanent restrictions of Internet access;
- Temporary or permanent restrictions of Wireless access.