



Acceptable Use of Information & Communication Technologies

SCHOOL ICT POLICIES
• FOR PARENTS & CARERS •

Page | 1

This Acceptable Use of Information and Communication Technology (ICT) Policy outlines the expectations, responsibilities, and conditions for the safe, respectful, and lawful use of school-provided and approved ICT resources at Hervey Bay State High School.

The policy applies to all Students and sets out acceptable and unacceptable use, digital citizenship expectations, online safety requirements, security and privacy obligations, monitoring practices, use of Internet, email, devices, and storage media, as well as consequences for policy breaches. Parents and Carers are expected to support Students in understanding and complying with this policy.

Continued access to ICT resources is conditional upon compliance with this policy and all related school and Department of Education requirements.

1. Policy Statement

Upon enrolment at HBSHS, Students and their Parents or Carers are required to read, understand, and agree to comply with the conditions of this policy. Acknowledgement is recorded via the **Student Enrolment Checklist** or other applicable agreement forms.

A digital version of this policy is available on the school website at herveybayshs.eq.edu.au. Printed copies are available upon request.

Acceptance of this policy constitutes a binding agreement to comply with its terms as a condition of being issued ICT accounts, credentials, or access to school ICT resources.

This policy may be redistributed or updated following audits, reviews, or legislative changes. Continued use of school ICT services constitutes acceptance of any updated versions of this policy.

2. Glossary of Terms

Devices

Includes all:

1. Bring Your Own (BYO) devices
2. School Hire-to-Buy devices
3. Intermediary school program devices
4. School-hosted, shared, and managed devices

This includes Windows desktops and laptops, Apple MacBook laptops, and Apple iPad tablets.

Devices incompatible due to failure to follow published school requirements are excluded.

Account / Account Credentials

Refers to the Department of Education (DoE) hosted single sign-on service providing Students with access to education-related systems via a unique username and password.

3. General Conditions of Use

Students using HBSHS ICT facilities and services must:

- a. access ICT resources only using their own unique account credentials;
- b. keep usernames and passwords secure and confidential;



- c. accept responsibility for all activity conducted using their account;
- d. store school-related files only in approved locations (e.g. H drive, OneDrive);
- e. use provided storage and email services strictly for educational purposes;
- f. not store executable files, games, music, videos, malicious software, or large non-educational files on DoE or school systems.

4. Student and Parent Awareness

Students and Parents or Carers must understand that:

- a. ICT facilities must be used in accordance with this policy and all school rules;
- b. breaches may result in restricted or removed ICT access;
- c. ICT access is provided to support educational outcomes;
- d. the school cannot control all content available via the Internet;
- e. Students may inadvertently encounter inappropriate material;
- f. Teachers exercise duty of care, however responsible use by Students is essential.

5. Monitoring and Management of ICT Use

Use of school ICT systems is monitored and logged.

HBSHS reserves the right to:

- a. filter and moderate Internet and intranet access;
- b. monitor and record ICT usage;
- c. audit, archive, or delete Student files to manage storage and compliance;
- d. remove inappropriate or non-educational material;
- e. take disciplinary action where breaches occur.

ICT resources are provided for educational purposes only unless otherwise authorised.

6. Digital Citizenship and Online Conduct

Students are expected to demonstrate responsible digital citizenship and ethical online behaviour.

This includes:

- a. respectful communication in all digital environments;
- b. awareness of the long-term impact of digital actions;
- c. responsible creation and sharing of digital content;
- d. understanding that online behaviour can have real-world consequences.

7. Acceptable Use

Students may use ICT resources for:

- a. teacher-directed class work and assessment;
- b. developing literacy, communication, and information skills;
- c. creating approved digital content for educational purposes;
- d. conducting research for school projects;
- e. collaborating with Students, Teachers, Parents, or approved experts;
- f. accessing approved DoE digital environments and references.



Students must immediately report any ICT malfunction, damage, or security concern to a Teacher or ICT Technical Officer. Students must not attempt to investigate or exploit security vulnerabilities.

8. Unacceptable Use

It is unacceptable for Students to:

- a. use ICT resources unlawfully, including harassment, intimidation, theft, or vandalism;
- b. access, create, store, or distribute offensive or inappropriate content;
- c. engage in cyberbullying, harassment, impersonation, or image-based abuse;
- d. download, install, copy, or share unauthorised software or applications;
- e. deliberately waste printing, bandwidth, or ICT resources;
- f. tamper with or damage ICT equipment or infrastructure;
- g. commit plagiarism or breach copyright laws;
- h. access social media or unauthorised email services during school hours;
- i. use VPNs, torrent software, malware, or other tools to bypass security controls.

Any attempt to breach ICT security may result in disciplinary action and referral to external authorities.

9. Usernames and Passwords

Students must:

- a. use only their own DoE-issued credentials;
- b. never share usernames or passwords;
- c. never access another person's account, files, or emails.

Suspected compromise must be reported immediately. Failure to report may result in the Student being held accountable for subsequent misuse.

10. Internet, Email, and Online Services

- a. Internet and email access is for educational purposes only.
- b. Use during class time requires Teacher authorisation.
- c. Students must use only their DoE-provided email account.
- d. Emails are filtered and scanned for inappropriate content.
- e. Students must not disclose personal or sensitive information online.
- f. Inappropriate websites or emails must be reported immediately.

Use of school ICT systems to denigrate the school or its community, including outside school hours, is prohibited where it impacts the school environment, safety, or reputation.

11. Artificial Intelligence and Emerging Technologies

Students must not use artificial intelligence tools or automated content generation services to complete assessment tasks unless explicitly authorised by a Teacher. Presenting AI-generated content as original Student work may constitute plagiarism or academic misconduct.



12. Bring Your Own Devices (BYO)

Students may connect approved BYO devices (Windows laptops, Apple MacBooks, Apple iPads only).

- a. Device specifications are published on the school website.
- b. Only compatible devices are supported.
- c. Connection instructions must be followed precisely.
- d. The school may refuse support for incompatible devices.

13. USB and External Storage Devices

USB storage devices may be used for educational purposes only.

- a. Devices are scanned for malware.
- b. Infected files may be quarantined or deleted.
- c. Non-educational or prohibited material is not permitted.

14. Printing

Students receive a \$5 print credit each semester.

- a. Additional credit requires approval from an ICT Technical Officer.
- b. Charges may apply via Student Services.
- c. Credit lost due to verified technical faults may be reimbursed.

15. Copyright and Plagiarism

Students must:

- a. obtain permission before copying another person's work;
- b. acknowledge sources appropriately;
- c. comply with copyright laws.

Unauthorised copying may result in disciplinary or legal action.

16. Accessibility and Reasonable Adjustments

Reasonable adjustments to ICT access or requirements may be made for Students with approved learning, accessibility, or medical needs, in consultation with relevant school staff.

17. Breaches of Policy

Breaches may result in:

- a. suspension or removal of ICT access;
- b. school disciplinary action;
- c. referral to the Department of Education or external authorities.

Investigations may involve school leadership, DoE Cyber Security teams, or law enforcement agencies.



19. Confidentiality of Reports

Reports of ICT misuse or security concerns will be handled confidentially where appropriate and in accordance with legislative and departmental requirements.

20. Release of Liability

HBSHS provides ICT services without warranty and accepts no responsibility for loss of data, service interruptions, or damages arising from ICT use.

Use of Internet-based information is at the Student's own risk. Students are responsible for evaluating the accuracy and reliability of online information.

Approved by Hervey Bay State High School

Reviewed in accordance with Queensland Department of Education requirements

CONTACT INFORMATION AND URLS:

Call: (07) 4194 3777 | Email: enquiry@herveybayshs.eq.edu.au

Policies - School Website: <https://herveybayshs.eq.edu.au/our-school/rules-and-policies>

ICT Services - School Website: <https://herveybayshs.eq.edu.au/facilities/computers-and-technology>