Acceptable Use of Information & Communication Technologies

SCHOOL ICT POLICIES
• FOR PARENTS & CARERS •

Essential for schools in providing education programs and resources, is the use of the Internet, email and other ICT facilities and services. At all times while using school ICT facilities and services, students are required to conduct themselves according to the requirements of all school policies and rules. Responsibility for conveying and ensuring students understand and follow behaviour standards when using ICT facilities and services, also falls upon parents and carers. Schools reserve the right to restrict access to ICT facilities and services if breaches by students occur.

1. Purpose

Hervey Bay State High School (HBSHS) offers a large host of ICT services which allows students to access a wide range of curriculum specific software, hardware and Internet related services to facilitate learning. With this opportunity comes responsibility. To be able to access these services, all students must be familiar with the guidelines stated in the school's Acceptable Use of Information and Communication Technologies Policy (AUP).

2. Policy

When students enrol at HBSHS, they and their parents/carers fill in and sign the Student Enrolment Checklist, which on page 24 requires that all parties have read, understand and agree to comply with all conditions of this policy. A digital online version of this policy is located at: https://herveybayshs.eq.edu.au/our-school/rules-and-policies Physical copies are available on request. Signatures on the Student Enrolment Checklist or any other agreement form by a student subject to this policy and any parent or carer shall constitute a binding agreement to comply with its terms in consideration of an account and password being issued. This policy will be re-distributed whenever major changes or updates occur.

Accounts and passwords will only be issued to those students who have indicated their acceptance of this policy and their agreement to comply with its terms by signing an agreement within the enrolment package form (including signature by a parent or carer where required).

Glossary of Terms:

The term "devices" in this document incorporates all (**1**) Bring Your Own (BYO), (**2**) school Hire to Buy program, (**3**) intermediary school programs, and (**4**) school hosted and managed: Windows desktop and laptop computers, Apple MacBook laptop computers, and Apple iPad tablets. The scope of "Devices" does not include devices that have been purchased by parents/carers for BYO use that are incompatible, resulting from them not consulting the school or its documentation – which is either provided to them by the school directly or is available on the school website.

The terms "account", "account credentials", "computer account", "username", "login credentials" refer to a Department of Education hosted single sign-on service for students to gain access to resources hosted for education purposes, such as the Internet and emails via a username and password, or email address and password.

Students using HBSHS ICT facilities and services will:

- only access these resources using their unique account credentials assigned to them;
- not divulge their account's credentials (username and/or password) to any other individuals or group;
- be accountable for all ICT services or device usage conducted while using their unique account;
- save their files (classwork, assignments, etc) on their H drive, OneDrive or other assigned repositories;
- be provided with network storage space and a school email account, to be used for school purposes only;
- not store executable files, music, games, videos, large amounts of images and other similar files on the Department of Education's school network or Internet hosted services.

Students and their parents must be aware:

- ICT facilities are utilised with good behaviour under this policy, and where stipulated under all of the school's other related policies and rules for students;
- students breaking these policies and rules will be subject to appropriate action by the school which may include restricted some or all ICT access for a period as deemed appropriate by the school;
- access to ICT facilities provides valuable learning experiences, therefore giving the student educational benefits are in focus with the school's educational program;
- the school cannot claim to control information accessed through the internet;
- information may be accessed or accidentally displayed which could be illegal, dangerous or offensive, with or without the student's immediate knowledge;
- teachers will always exercise their duty of care, but protection, mitigation and discontinued access to harmful information requires responsible use by the student.

Network use, including use of the internet, intranet and email is monitored and recorded. HBSHS reserves the right to:

- moderate access to Internet and Intranet services, including the filter of websites;
- monitor and record usage of its ICT facilities, including Internet services;
- regularly filter storage for inappropriate/non-education files and if found, delete these automatically;
- cull/archive student files to remove unnecessary data and/or to regain disc space;
- take disciplinary action when breaches of expected behaviour occur – the school's ICT facilities are to be used for educational purposes only, unless otherwise arranged.

3. Acceptable Use

Students will use ICT devices, the school network, Internet, intranet, email and other digital local or online services only for educational purposes related to their studies.

It is acceptable that students use HBSHS ICT services for:

- assigned class work and assignments set by teachers;
- developing appropriate and respective literacy, communication and information skills;
- authoring text, artwork, audio and visual material for publication on digital local or online services for educational purposes as supervised and approved by the school;
- conducting general research for school activities and projects;
- communicating or collaborating with other students, teachers, parents or experts in relation to school work;
- accessing online references such as the school intranet, dictionaries, encyclopaedias, etc.;
- researching and learning through the Department of Education's digital environments.

Students must report any problems, damages or vandalism to their class teacher as soon as it is observed. Students will immediately notify the school's ICT Technical Officers if they have identified a potential ICT related security problem. They will not seek out security problems as those acts may be construed as illegal attempts to gain access.

4. Unacceptable Use

It is unacceptable for students to:

- use ICT resources in and for an unlawful manner (libels, slander, vandalism, harassment, theft, etc);
- download, distribute or publish offensive messages or pictures;

- download, install, copy, or share unauthorised and prohibited software/applications;
- insult, harass or attack others, use obscene or abusive language in or via digital form;
- deliberately waste printing and Internet resources;
- tamper with or damage ICT devices (computers, iPads, CCTV cameras, network equipment, etc);
- commit plagiarism or violate copyright laws;
- use social media services during school hours at school on any device;
- use unauthorised online email services (e.g. Gmail) during school hours on any device, send or forward chain emails, send or forward spam emails, send or forward plagiarised materials via email and send or forward emails that include inappropriate language;
- knowingly download, store, install or forward on: torrent software, VPN software, malware, viruses, infected emails by or via any technological means capable of breaching ICT security.

Hacking or the intention to breach or circumvent school security, breach copyright, pirate and upload or transfer unauthorized software via USB media, or any other storage devices onto any Department of Education ICT services or devices is a breach of the Acceptable Use of Information and Communications Technology Policy and will result in actions being taken, and possibly legal actions by the appropriate authorities if investigated for criminal offense.

5. Usernames and Passwords

5.1 Students are only permitted to access devices, the network, Internet, intranet, emails etc. using their personal DOE credentials: username, email address and password. Under no circumstances, are students permitted to share their sign in (login) credentials with any other student in any way. Students may not and are prohibited from using another student or staff member's username or password to access the school's ICT devices and infrastructure, not limited to the network, another person's files, H Drive, OneDrive or emails.

5.2 If a student suspects their username/password is being used by another person, it is their responsibility to inform their class teacher and arrange for their password to be changed immediately. Failure to do so will mean the student is then held liable for any breaches, unauthorised or illegal activities within their account.

6. Internet and Email Use

The use of the Department of Education and school's hosted Internet and emails are for education purposes only.

6.1 Internet and email access during class time, is only to occur with a teacher's instructions.

6.2 Student email use must be conducted through the email account provided by the school. Use of other email services while at school during class time is not permitted.

6.3 Sites designed for personal use such as personal web spaces, chats, forums, social media, non-educational websites and online services are not to be accessed at school. General "web surfing" may only be performed offsite.

6.4 Electronic communications via department hosted email services are scanned and filtered. When DOE emails are sent, they pass through the Department's mailing system which scans both the attachment/s and the subject/body of emails for words that the department has classified as inappropriate or offensive. The blocked word filter list includes terms associated with profanity, bullying, adult content, and drug references. ICT Technical Officers are alerted and take corresponding actions when breaches of expected behaviour occur – the school's email services are to be used for educational purposes only.

6.5 Students will not divulge any personal contact information about themselves or other people such as their name, parent's name, address, phone numbers, school address, work address, etc. online.

6.6 Filtering of websites does occur but any accidental access to inappropriate internet sites must be reported by students to their Teacher, Case Manager or an ICT Technical Officer.

6.7 If students receive inappropriate emails from anyone, they must report it to their Teacher, Case Manager or an ICT Technical Officer.

6.8 Students will not use any physical means or digital service to denigrate the school or any members of its community at any time, including out of school hours.

6.9 Students are required to only use their DOE email account to send emails to teachers or other staff.

7. Bring Your Own Devices (BYO)

Students are permitted to connect (onboard) their privately owned devices (Windows Laptop, Apple MacBook, Apple iPad only) to the school network.

7.1 Device requirements are available to parents and carers on the school website. Only compatible devices are permitted. Parents/carers are expected to know compatibility requirements. The school reserves the right to not provide a service if a device is brought in that is incompatible and does not meet BYO requirements.

7.2 Instructions to connect are available for parents, carers and students on the school website. A print-out of these instructions may be obtained by students from an ICT Technical Officer during school hours.

7.4 The instructions provided must be adhered correctly to for the service to function. Students are responsible for adhering to any instructions provided by school staff to assist them.

8. USB Flash Drives / Other USB Storage Devices

While USB storage falls under the definition of private devices, it is acceptable for students to use such devices to fulfil their educational program requirements (e.g. bring assessment items to school as opposed to emailing).

8.1 Virus scanning occurs on all files downloaded/stored on the network, including files contained within USB storage devices when plugged into a school hosted and managed desktop or laptop, or Hire to Buy laptop.

8.2 No USB storage devices are to be plugged into a school hosted and managed desktop or laptop, unless they contain educational materials and are being used for the purposes of class work and/or assignments. The same applies to Hire to Buy laptops while the device is with student at school.

8.3 When detected by virus and malware scans, malicious files stored on USB storage devices when plugged into school hosted and managed desktops or laptops, or Hire to Buy laptops are automatically deleted.

9. School Monitoring

The school's technicians and Department of Education's cyber security personnel monitor the access and usage of school ICT services. Security monitoring services and processes are in place to identify and protect against inappropriate use, to maintain performance, determine compliance with State and departmental policies and determine compliance with State and federal legislation and regulations.

The school reserves the right to restrict student access to ICT services if access and usage requirements are not met or breached.

10. Printing

At the beginning of each semester, each student's print credit is reset to $5 balance. Students are responsible for maintaining their printing balance. If students require additional credit after their balance runs out, they must visit an ICT Technical Officer first to evaluate credit usage. They may be instructed to pay a nominal amount at Student Services to obtain more credit, then take the receipt back to the ICT Technical Officer who will adjust the printing balance accordingly.

If the student has been found to have experienced problems with printing and has lost credit due to proven unavoidable technical problems involving school ICT services, they may be reimbursed some of their credit without having to pay for more. Each occurrence is actioned appropriately to assist students.

11. Copyright & Plagiarism

11.1 Students must obtain permission before copying data or works from another individual. Copying data or works belonging to another individual without their expressed permission may constitute plagiarism and/or theft.

11.2 The unauthorised copying of software, information, graphics or other intellectual properties and digital assets may violate copyright laws, and may be subject to prosecution from agencies to enforce such copyrights.

12. Breaches of the Policy

12.1 Alleged breaches of this policy will be investigated by appropriate staff, not limited to the Principal, Deputies, Heads of Department, Teachers, Business Manager, ICT Technical Officers and Administration Officers.

12.2 If students are found to have breached the Acceptable Use of Information and Communications Technology Policy, consequences will apply.

12.3 Breaches of the Acceptable Use of Information and Communications Technology Policy may result in immediate suspension of students' ICT privileges, and may result in further actions being taken by Hervey Bay State High School, the Department of Education, State or Federal authorities.

13. Release of Liability

Hervey Bay State High School makes no warranties of any kind, whether express or implied, for the service it is providing. Hervey Bay State High School will not be responsible for any damages a user suffers as a result of their use of the Department of Education's or HBSHS's ICT services or use thereof by any other person.

This includes loss of data resulting from delays, no-deliveries, mis-deliveries, service interruptions, or the Hervey Bay State High School's negligence or by the user's errors or omissions or by the actions of any other user of the HBSHS network. Use of any information obtained via the Internet is at the user's own risk.

Hervey Bay State High School specifically denies any responsibility for the accuracy or quality of information obtained through its services. All users need to consider the source of any information they obtain and consider how valid that information may be.

CONTACT AND REFERENCE INFORMATION:
Call: (07) 4194 3777 | Email: enquiry@herveybayshs.eq.edu.au
School Website (Policies): https://herveybayshs.eq.edu.au/our-school/rules-and-policies
School Website (ICT Services): https://herveybayshs.eq.edu.au/facilities/computers-and-technology