Acceptable Use of Information & Communication Technologies

Use of the Internet, email, and other ICT resources is essential for schools in delivering educational programs and services. While using these facilities, Students must adhere to all school policies and rules. It is the responsibility of Parents and Carers to ensure that Students understand and follow the expected standards of behaviour when using ICT resources. Schools reserve the right to restrict access to these facilities if Students breach any policies or rules.

1. Purpose

Hervey Bay State High School (HBSHS) offers well maintained ICT resources which includes software, hardware, Internet and email access to facilitate and support Student learning. Having access to these resources provides opportunities with responsibilities. To participate and maintain access, Students must accept and be familiar with this policy and its guidelines – also known as the **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 applicable parties have read, understand and agree to comply with all conditions of this policy. A digital online version is available to read 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 or any other ICT resources provided. This policy may be re-distributed whenever major changes or updates take place following audits or reviews.

Accounts and passwords or other ICT resources may only be issued to Students who have indicated their acceptance of this policy and their agreement to comply with its terms, by signing in acknowledgement within the **Student Enrolment Checklist** (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 program, and (**4**) school hosted, shared and managed: Windows desktop and laptop computers, Apple MacBook laptop computers, and Apple iPad tablets. The scope of "devices" does not include digital resources that have been purchased by Parents/Carers for BYO use that are incompatible, generally resulting from not consulting the school or its available documentation 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 utilizing HBSHS ICT facilities and services will:

- only access these resources using unique account credentials assigned to them individually;
- 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 and conduct while using their unique account;
- save their files (classwork, assignments, etc) on their H drive, OneDrive or other instructed 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, malicious software or large files or files that take up unreasonable 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 that:

- 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 restricting some or all ICT access for a period as deemed appropriate at the time;
- 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 exercise their duty of care - nevertheless protection against, mitigation of 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 filtering of websites;
- monitor and record the use of its ICT facilities, including Internet services;
- regularly filter storage devices for inappropriate/non-education files and if found, remove them;
- cull/archive Student files to remove unnecessary data and/or to regain server disk 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 with ICT Tech Officers.

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 account's credentials with any other Student. 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 and/or password is being used by another person, it is their responsibility to inform a Class Teacher and arrange for their password to be changed immediately. Failure to do so shows the Student liable for any breaches including unauthorised or illegal activities conducted without their knowledge.

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 filtering systems which scan emails and their attachments for words that the department has determined 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 appropriate actions when breaches of expected behaviour occur – the school's email services are to be used for educational purposes only.

6.5 Students must 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 or in person with anybody.

6.6 Filtering of websites is in place however 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

It is acceptable for Students to use USB storage devices to fulfil their educational program requirements (e.g. bring assessment items to school as opposed to emailing or downloading files from OneDrive).

8.1 Antivirus and malware software automatically scans files stored on the network, and files contained within USB storage devices when plugged into a school hosted and managed desktop or laptop, or Hire to Buy laptop.

8.2 USB storage devices must not be plugged into a school hosted and managed desktop or laptop, unless they contain educational materials and are being used for class work and 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 team monitor the access and usage of school ICT services. Security monitoring services and processes in place identify and protect against inappropriate use, they 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 start of each semester, all Student print credit balances are reset to $5. Students are responsible for maintaining their own printing. 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 for the applicable amount of credit lost.

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

12.2 Alleged breaches of this policy will be investigated by appropriate Staff, not limited to the Principal, other school staff, or appropriate external parties such as the department's Cyber Security teams or Police Officers.

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 expressed or implied for digital services it provides. 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 Network, Internet or email services or use thereof by any other person.

This includes loss of data resulting from delays, no-deliveries, mis-deliveries, service interruptions, or 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 school's ICT resources, services and facilities. Use of any information obtained via the Internet is at the user's own risk.

Hervey Bay State High School denies any responsibility for the accuracy and quality of Internet or other online digital information obtained by students via the school's ICT resources, services and facilities. Students should carefully consider their sources of online information and how accurate and valid that data may be.

CONTACT AND REFERENCE INFORMATION:
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