



**BUNDABERG
STATE HIGH SCHOOL**

Department of Education trading as
Education Queensland International (EQI)
CRICOS Provider Code 00608A

STUDENT POLICY—JANUARY 2024

Information & Communication Technology Policy, including Acceptable Computer and Internet Use

Upon enrolment in a Queensland Government school, parental or caregiver permission is sought to give the student/s access to the Internet, based upon the policy contained within ICT-PR-004 Using the Department's Corporate ICT Network.

This policy also forms part of this Student BYOx Agreement and Charter, and the school's Acceptable Use of IT and Internet Policy. The acceptable-use conditions apply to the use of the device and Internet both on and off the school grounds.

Communication through Internet and online communication services must comply with the Responsible Behaviour Plan which is also available on the school website.

There are a few conditions that students should adhere to. Students should not:

- create, participate in or circulate content that attempts to undermine, hack into and/or bypass the hardware and/or software security mechanism that are in place.
- disable settings for virus protection, spam and/or Internet filtering that have been applied as part of the school standard.
- use unauthorised programs and internationally download unauthorised software, graphics or music
- internationally damage or disable computers, computer systems or Queensland DET networks
- use the device for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose.

Note Students' use of Internet and online communication services can be audited and traced to the account of the user. This includes social media sites such as Facebook. Any legal issues will be referred to the police.

MOBILE PHONES AND OTHER ELECTRONIC DEVICES

From the beginning of Term 1 2024, all Queensland state school students must keep their mobile phones switched off and **'away for the day'** while at school. Notifications on wearable devices, such as smartwatches, must be disabled to prevent phone calls, messages and other notifications from being sent or received during school hours.

The decision to implement a consistent, state-wide approach to putting mobile phones away during the school day is based on the advice of Ms Cheryl Vardon AO, former Queensland Family and Children's Commissioner, who completed an independent review of Queensland's approach to mobile phones. Ms Vardon's review included consultation with key education stakeholders, such as principals, school staff, students and families from each education region, as well as a review of recent research on student use of mobile phones and personal devices in schools.

'Away for the day' will support schools to maintain a strong focus on educational achievement, and student wellbeing and engagement by:

- providing optimal learning and teaching environments
- encouraging increased face-to-face social interactions between students
- promoting the health and wellbeing of students through increased social interaction and physical activity
- reducing the potential for students to be exposed to the negative impacts of the digital world, resulting from unsafe or inappropriate technology use.

For further information please refer to [Advice for state schools on acceptable use of ICT facilities and devices](#).

If students choose to bring their mobile phone to school, they must **switch it off** and keep it in their school bags or out of sight during school hours. Smartwatches and other devices can be worn; however notifications must be **switched off**. This includes during lessons and break times, as well as other school activities.

Exemptions

- an exemption may be granted for a specific individual student circumstances which must be negotiated with the Principal or delegate through written application, e.g.: a specific health requirement such as diabetics. These phones will be on silent while at school.
- use of mobile phones and wearable devices for school payments (e.g. tuckshop, uniform shop and office);
- use of mobile phone for recording evidence for assessment tasks during class time only where specified in the assessment task sheet;
- use during representative school sports, camps and excursions at specified and supervised times (in accordance with the [School excursions](#) procedure).

	Response	Action	
MINOR	1st Breach	<ul style="list-style-type: none"> ○ Students hand phone to the Hub for the day and receive a receipt ○ Warning and rule reminder. Mobile phones are <i>away for the day</i>. Mobile phones must be off and out of sight (including headphones/pods). ○ Smartwatch/wearable notifications are off ○ SMS home to parents/carers 	Failure to follow staff instructions may result in further disciplinary action.
	2nd Breach	<ul style="list-style-type: none"> ○ Students hand phone to the Hub for the day and receive a receipt ○ Rule reminder. Mobile phones are <i>away for the day</i>. Mobile phones must be off and out of sight (including headphones/pods). ○ Smartwatch/wearable notifications are off ○ Hub Detention at 1st break (or following day if breach after break 1) ○ Student must complete <i>responsible technology use</i> booklet ○ SMS home to parents/carers 	
	3rd Breach	<ul style="list-style-type: none"> ○ As per 2nd Breach response and ○ Parent/carer to collect phone from the Hub or negotiate with school staff 	
MAJOR	4th Breach	<ul style="list-style-type: none"> ○ Suspension may result due to continued technology violation/non-compliance with school expectations ○ Parent/carer contact/meeting to address behaviour and establish a plan to prevent continuation 	
	Any further breach	<ul style="list-style-type: none"> ○ Individual student management via Hub HOD/Deputy Principal/Principal ○ Repeated behaviour will result in phone remaining at home or Hub on a long-term basis (determined by Hub Head of Department/Deputy Principal) ○ Daily check-in with Hub/Exec staff ○ Parent/carer contact/meeting ○ Individual support processes/plan 	

- The process refreshes each Semester.

Note The school does not accept responsibility for loss, theft or damage of such items.

PASSWORDS

Passwords must not be obvious or easily guessed; they must be kept confidential, and changed when prompted or when known by another user. Personal accounts cannot be shared. Students should not allow others to use their personal account for any reason. Students should log off at the end of each session to secure no one else can use their account or laptop.

CYBERSAFETY

At any time, if a student believes they have received a computer virus or spam (unsolicited email), or they have received a message that is inappropriate or makes them feel uncomfortable, they must inform their teacher, parent and/or caregiver as soon as is possible. Students are encouraged to explore and use the ‘Cybersafety Help’ Queensland Government website to talk, report and learn about a range of cybersafety issues. Students must seek advice if another user seeks personal information, asks to be telephoned, offers gifts by email or asks to meet a student.

Students must never initiate or knowingly forward emails, or other messages, containing:

- a message sent to them in confidence.
- a computer virus or attachment that is capable of damaging the recipients' computer.
- Chain letters or hoax emails.
- spam (such as unsolicited advertising Students must never send or publish.
- unacceptable or unlawful material or remarks, including offensive or discriminatory comments.
- threats, bullying or harassment of another person.
- sexually explicit or sexually suggestive material or correspondence.
- false or defamatory information about a person or organisation.

PRIVACY AND CONFIDENTIALITY

It is important that students do not publish or disclose the email address of a staff member or student without that person's explicit permission. The student should not reveal personal information including names, addresses, photographs, credit card details or telephone numbers of themselves or of others. It should also be ensured that privacy and confidentiality is maintained by not disclosing or using any information in a way that is contrary to any individual's interests.

INTELLECTUAL PROPERTY AND COPYRIGHT

Students should never plagiarise information and shall observe appropriate copyright clearance, including acknowledging the original author or source of any information used. It is also important that the student obtain all appropriate permissions before electronically publishing other people's works or drawings. The creator or author of any material published should always be acknowledged. Material being published on the Internet or intranet must have the approval of the Principal or their delegate and have appropriate copyright clearance.

MISUSE AND BREACHES OF ACCEPTABLE USAGE

Students should be aware that they are held responsible for their actions while using the Internet and online communication services. Students will be held responsible for any breaches caused by other person/s) knowingly using their account to access Internet and online communication services.

The **misuse** of Internet and online communication services **may result in disciplinary action** which includes, but is not limited to, the withdrawal of access to services and/or device.

MONITORING AND REPORTING

Students should be aware that all use of Internet and online communication services can be audited and traced to the account of the user. All material on the device is subject to audit by authorised school staff. If at any stage there is a police request, DET may be required to provide the authorities with access to the device and personal holdings associated with its use.

STUDENTS' REPORTING REQUIREMENTS

Students are required to report any Internet site accessed that is considered inappropriate. Any suspected security breach involving students, users from other schools, or from outside the Queensland DET must also be reported to the school.