BUNDABERG STATE HIGH SCHOOL

STUDENT POLICY — DECEMBER 2018

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 available on the school website or in the student planner.
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 mechanisms that are in place within the school grounds
- disable settings for virus protection, spam and/or Internet filtering that have been applied as part of the school standard
- use unauthorised programs and intentionally download unauthorised software, graphics or music
- intentionally 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

Bundaberg State High School has an obligation to ensure that our school provides a safe and supported teaching and learning environment. In a move to further protect our young people from the harms of cyberbullying and the disruption that inappropriate use of mobile phones* can have on teaching and learning, mobile phones and accessories (e.g. headphones) cannot be used during school hours (8:30 am – 2:35 pm) by Junior Secondary students, unless a teacher has given permission for educational purposes.
Under these conditions the mobile phone:

- must be switched to silent
- cannot be used as a communication device unless communicating with a teacher via a school approved email or app when directed to do so by the teacher
- cannot be used to record images or video of other people
- cannot be charged at school
- cannot be used for listening to music or gaming (unless directed by the teacher for educational purposes)
- cannot be used during lunch breaks within the school grounds
- students who breach the policy will have to hand in their phone at the relevant Hub for the remainder of the school day. For repeated breaches of the policy, students will be dealt with through level 2 or 3 behaviour consequences outlined in the Bundaberg State High School Responsible Behaviour Plan for Students.

Electronic devices such as mobile phones and iPods can be expensive – they should be carried on the person (pocket) and not left in bags. The school does not accept responsibility for loss or theft of such items.

*or other electronic devices which capture images/text/recordings

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 ensure no one else can use their account or laptop.

Cyber Safety

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 'Cyber safety Help' Queensland Government website to talk, report and learn about a range of cyber safety 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 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 interest.

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.