# ICT Acceptable Use Policy

## Information for Students and their Parents about Acceptable Usage

### Acceptable device use

Students must follow the school rules when using their iPad:

- Be Safe
- Be Respectful
- Be Responsible
- Be a Learner

Students must comply with the Acceptable Use of the Department's Information, Communication and Technology (ICT) Network and Systems

Communication through internet and online communication services must also comply with the department's Code of School Behaviour and the Birkdale South State School Responsible Behaviour Plan for Students available on our school website.

Examples of acceptable use includes:

- engagement in class work and on assignments set by teachers
- developing appropriate 21st Century knowledge, skills and behaviours
- authoring text, artwork, audio and visual material for publication on the Intranet or Internet for educational purposes as supervised and approved by school staff
- conducting general research for school activities and projects
- communicating or collaborating with other students, teachers, parents, caregivers or experts as part of assigned school work
- accessing online references such as dictionaries, encyclopedias, etc.
- researching and learning through the school's eLearning environment
- ensuring the device is fully charged before bringing it to school to enable continuity of learning

Students are expected to be courteous, considerate and respectful of others when using their device.

### Unacceptable device use

Examples of unacceptable use includes:

- using the device in an unlawful manner
- downloading (including using unauthorised software), distributing or publishing of offensive messages or pictures
- using obscene, inflammatory, racist, discriminatory or derogatory language
- using language and/or threats of violence that may amount to bullying and/or harassment, or even stalking
- insulting, harassing or attacking others or using obscene or abusive language
- deliberately wasting printing and Internet resources
- intentionally damaging any devices, accessories, peripherals, printers or network equipment
- committing plagiarism or violating copyright laws
- using unsupervised internet chat
- sending chain letters or spam email (junk mail)
- accessing private 3G/4G networks during the school day
- knowingly downloading viruses or any other programs capable of breaching the department's network security
- using the device's camera anywhere a normal camera would be considered inappropriate, such as in toilets
- invading someone's privacy by recording personal conversations or daily activities and/or further distributing (e.g. forwarding, texting, uploading, Bluetooth use etc.) such material

Note: students should not divulge personal information (e.g. name, parent's name, address), via the

Internet or email, to unknown entities or for reasons other than to fulfil the educational program requirements of the school.

## What is expected of schools when providing students with access to ICT facilities?

Schools will provide information in relation to student access and usage of its network and reserve the right to restrict/remove student access to the intranet, extranet, internet or network facilities if parents or students do not adhere to the school's network usage and access guideline/statement.

The school will educate students on cyber bullying, safe internet and email practices and health and safety regarding the physical use of electronic devices. Students have a responsibility to incorporate these safe practices into their daily behaviour at school.

Where possible, internet usage by students will be considered and prepared prior to class engagement, including filtering and checking sites students are directed to visit. Assessment tasks should be delivered within an appropriate timeframe, allowing students appropriate access to the internet (during schools hours and/or outside of school hours) to complete the set task.

## What awareness is expected of students and their parents?

**Students and their parents should:**

Understand the responsibility and behaviour requirements (as outlined by the school) that come with accessing the school's ICT network facilities, and ensure they have the skills to report and discontinue access to harmful information if presented via the internet or email;

Be aware that the ICT facilities should be utilised with good behaviour as stipulated under the Code of School Behaviour; and that students breaking these rules will be subject to appropriate action by the school. This may include restricted network access or loss of BYOD privilege, for a period as deemed appropriate by the school.

Be aware that access to ICT facilities provides valuable learning experiences, therefore giving the student educational benefits in line with the school's educational program;

Be aware that the internet gives access to information on and from a wide variety of organisations, subjects, people and places with origins from around the world. The school cannot control information accessed through the internet; and information may be accessed or accidentally displayed which could be illegal, dangerous or offensive, with or without the student's immediate knowledge; and

Understand that teachers will always exercise their duty of care, but protection, mitigation and discontinued access to harmful information requires responsible use by the student.

## Internet Use at School

At school, students must agree to follow the Acceptable Use of the Department's Information, Communication and Technology (ICT) Network and Systems in relation to Internet Use. Internet access is provided by Education Queensland's Managed Internet Service (MIS) and provides students with Content-filtered Internet access and Virus-filtered email.

MIS provides the means to filter students' access to web pages from a global level; controlled by Education Queensland and from a school level when appropriate.

## Email Use

While at BSSS, students have access to a Department of Education, Training and Employment email account, which they can access from home and school for the purposes of learning. Email traffic is monitored for inappropriate use, content and language.

## Digital citizenship

Students should be conscious creators of the content and behaviours they exhibit online and take active responsibility for building a positive online reputation. They should be conscious of the way they portray themselves, and the way they treat others online.

Students should be mindful that the content and behaviours they have online are easily searchable and accessible. This content may form a permanent online record into the future.

Interactions within digital communities and environments should mirror normal interpersonal expectations and behavioural guidelines, such as when in a class or the broader community.

Parents are requested to ensure that their child understands this responsibility and expectation. The school's Responsible Behaviour Plan also supports students by providing school related expectations, guidelines and consequences.

## Cyber Safety

If a student believes they have received a computer virus, spam (unsolicited email), or they have received a message or other online content that is inappropriate or makes them feel uncomfortable, they must inform their teacher, parent or caregiver as soon as is possible.

Students must never initiate or knowingly forward emails, or other online content, 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, post or publish:

- inappropriate or unlawful content which is offensive, abusive or discriminatory
- threats, bullying or harassment of another person
- sexually explicit or sexually suggestive content or correspondence
- false or defamatory information about a person or organisation.

Parents, caregivers and students are encouraged to read the department's Cybersafety and Cyberbullying guide for parents and caregivers.

## Web filtering

The internet has become a powerful tool for teaching and learning, however students need to be careful and vigilant regarding some web content. At all times students, while using ICT facilities and devices, will be required to act in line with the requirements of the *Code of School Behaviour* and any specific rules of the school. To help protect students (and staff) from malicious web activity and inappropriate websites, the school operates a comprehensive web filtering system. Any device connected to the internet through the school network will have filtering applied.

The filtering system provides a layer of protection to staff and students against inappropriate web pages, spyware and malware, peer-to-peer sessions, scams and identity theft.

This purpose-built web filtering solution takes a precautionary approach to blocking websites including those that do not disclose information about their purpose and content. The school's filtering approach represents global best-practice in internet protection measures. However, despite internal departmental controls to manage content on the internet, illegal, dangerous or offensive information may be accessed or accidentally displayed. Teachers will always exercise their duty of care, but avoiding or reducing access to harmful information also requires responsible use by the student.

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 network must also be reported to the school.

The personally-owned devices have access to home and other out of school internet services and those services may not include any internet filtering. Parents/caregivers are responsible for appropriate internet use by their child outside the school.
Parents, caregivers and students are also encouraged to visit the Australian Communications and Media Authority's CyberSmart website for resources and practical advice to help young people safely enjoy the online world.

## Privacy and confidentiality

Students must not use another student or staff member's username or password to access the school network or another student's device, and must not trespass in another person's files, home drive, email or access unauthorised network drives or systems.

Additionally, students should not divulge personal information via the internet or email, to unknown entities or for reasons other than to fulfil the educational program requirements of the school. 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. Students should also not reveal personal information including names, addresses, photographs, credit card details or telephone numbers of themselves or others. They should ensure that privacy and confidentiality is always maintained.

## Intellectual property and copyright

Students should never plagiarise information and should observe appropriate copyright clearance, including acknowledging the original author or source of any information, images, audio etc. 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.

Copying of software, information, graphics or other data files may violate copyright laws without warning and be subject to prosecution from agencies to enforce such copyrights.

## 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, the school may be required to provide the authorities with access to the device and personal holdings associated with its use.

## 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 school reserves the right to restrict/remove access of personally owned mobile devices to the intranet, internet, email or other network facilities to ensure the integrity and security of the network and to provide a safe working and learning environment for all network users. The misuse of personally owned mobile devices may result in disciplinary action which includes, but is not limited to, the withdrawal of access to school supplied services.