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 ICT Device Charter. The acceptable-use conditions apply to the use of the device and internet.

Communication through internet and online communication services must comply with the schools policies and procedures with the Student Code of Conduct 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 mechanisms 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 intentionally download unauthorised software, graphics or music
- intentionally damage or disable computers, computer systems or Queensland DoE networks
- use the device for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose.
- All email communication between students and staff are through departmental email account only.

Note: Students' use of internet and online communication services may be audited at the request of appropriate authorities for investigative purposes surrounding inappropriate use.

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.

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 as soon as is possible.

Students are encouraged to explore and use the 'Cybersafety Help' button 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).

ACCEPTABLE COMPUTER AND INTERNET USE

Students must never send or publish:

- Unacceptable or unlawful material or remarks, including offensive, abusive 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.

WEB FILTERING

An internet filtering solution provides DoE with the ability to restrict access to inappropriate material on DoE's ICT network.

Content filtering is active 100% of the time on the Computer for Student (CFS) devices. The filtering system is installed on each device.

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.

DAMAGE OR LOSS OF EQUIPMENT

All devices and batteries are covered by a manufacturer's warranty which covers manufacturing defects through normal usage. In addition, devices are covered by an insurance policy which protects against accidental damage. There is no cover for negligence, abuse or malicious damage.

Costs incurred by the school for the repair or replacement of devices may be charged by the school as an excess to parents. In the event of non-compliance of agreed responsibilities, schools may review the student's continued participation.

Any software or hardware issues, vandalism or damage to the device must be reported immediately to the teacher/school.

ACCEPTABLE COMPUTER AND INTERNET USE continued

WILFUL AND MALICIOUS DAMAGE

Where a device is intentionally damaged, parents will be notified of the event, followed by an investigation. Where the school determines that damage has been intentionally caused to a device or a student has disrespected school property, parents will be invoiced according to the following:

- Lost case $10
- Missing keys on keyboard $30
- Broken screen $100
- Broken device and not working $100

SOFTWARE

The software loaded on the device is licensed to the DoE or the school.

Devices may be audited by a school. Devices may be rebuilt at any time for numerous reasons without consultation with students or parents and all local data may be lost in this process.

To stop any malicious software or virus's entering the DoE network, Miles State High School prohibits the installation of any software or program onto any school device that is licensed to the school of DoE.

Parent/Carers will receive, sign and return to school the annual online services consent form which will outline the software that students access at school during engagement in curricular and extracurricular activities.

STORING, MONITORING AND REPORTING ON SCHOOL NETWORKS

Students should be aware that all use of internet and online communication services can be audited and traced to the account of the user.

1. Students will be provided with a school USB to store files.
2. All material on the device is subject to audit by authorised school staff. If at any stage there is a police request, DoE may be required to provide the authorities with access to the device and personal holdings associated with its use.
3. Students are not to store school files or use USBs on school devices that are not the property of Miles State High School.

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 Queensland DoE must also be reported to the school.