

Advice for State Schools on Acceptable Use of ICT Facilities and Devices

This advice supports the [Information and Communication Technology \(ICT\) Procedure](#).

The department allows restricted access to its ICT facilities and devices which includes network, printers etc. using either departmental or personal owned devices.

If in doubt when implementing technical requirements around the management of personally owned mobile devices and access to the department's ICT facilities and devices, advice can be sought from the Service Centre on 1800 680 445. Policy advice can be sought directly from Manager, Information Policy on 3034 4313. Additionally, information is available at Service Centre Online: <https://qlddet.service-now.com/sco/>.

Personal mobile device access

The department is aware that limited personally owned mobile device access is essential for the effective running of schools. The department reserves the right to restrict access of personal mobile devices to ensure the integrity of the network and a safe working and learning environment for all network users. These mobile devices include but are not limited to laptops, tablet devices, voice recording devices (whether or not integrated with a mobile phone or MP3 player), games devices (e.g. PSPs, Game Boys), USBs, DVDs, CDs and smart phones.

School employees personal mobile device access

Principals are to ensure that school employees follow the requirements under the [Information and Communication Technology \(ICT\) Procedure's](#) bring your own (BYO) personal mobile device section.

Student personal mobile device access

The departmental position is that mass access to the network by students' wholly owned personal mobile devices could compromise the integrity of the ICT network. Principals however can determine that for educational purposes a student can have access to the ICT network. This connection is provided only if the mobile device meets the department's security requirements (see [iSecurity](#) site for details) at a minimum installing, running and updating anti-virus software. Schools wanting students to connect to the department's ICT network are required to develop procedures to ensure that such provisions are assessed against the department's security requirements (where necessary undertaking a risk assessment) and that students and their parents/guardians are provided with the necessary education and assistance to be able to meet these departmental requirements.

The procedures are to include:

- providing advice to all students and their parents on appropriate security requirements (see [iSecurity](#) site for details)
- advising teacher/supervisor as soon as any breach of security is suspected
- the right to restrict/remove student access to the intranet, internet, email or other network facilities if they do not adhere to the school's network usage and access policy, guideline or statement
- ensuring that students are aware of [occupational health and safety](#) issues when using computers and other learning devices.

Schools that are implementing or have implemented the [BYOx](#) process need to also ensure steps have been taken to provide a safe and effective learning environment for students while meeting the department's security requirements. This includes advising parents/guardians that the devices provided allows access to their home and other out of school internet services and that such services may not include any internet filtering.

Student access to the department's ICT facilities and devices

The Smart Classrooms strategy underpins the growth and improvement in innovative programs and resources in schools for teachers and students. Essential tools for providing these innovative educational programs are the intranet, internet, email and network services (such as printers, display units and interactive whiteboards) that are available through the department's/school's ICT network. These technologies are vital for the contemporary educational program provided in schools.

At all times students, while using these 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 their school. In addition 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
- ensure they have the skills to report and discontinue access to harmful information if presented via the internet or email
- be aware that:
 - access to ICT facilities and devices provides valuable learning experiences for students and supports the school's teaching and learning programs
 - ICT facilities and devices should be used appropriately as outlined in the [Code of School Behaviour](#)
 - students who use a school's ICT facilities and devices in a manner that is not appropriate may be subject to disciplinary action by the school, which could include restricting network access
 - 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.

School specific ICT responsible use procedure

The [Information Communication and Technology \(ICT\) Procedure](#) provides direction to school principals around formulating a school procedure on access to the department's/school's ICT facilities and devices for parents and/or students to understand and acknowledge. This may take the form of a procedure, policy, statement or guideline and may require consultation with the school community. Acknowledging through signing seeks to support an understanding of what is lawful, ethical and safe behaviour when using or accessing the department's network and facilities by students and their parents. Principals may seek sign-off either on enrolment of students or alternatively at the start of each school year.

The following dot points are to assist schools with the formulation of their own procedure. Further guidance on drafting this section can be sought from the [Use of ICT Facilities and Devices Guideline](#).

Purpose statement

- Information and communication technology (ICT), including access to and use of the internet and email, are essential tools for schools in the provision of innovative educational programs.
- Schools are constantly exploring new and innovative ways to incorporate safe and secure information and communication technology (ICT) use into the educational program.
- School students, only with the approval of the principal, may be permitted limited connection of personally owned mobile devices to the department's information and communication technology (ICT) network, where this benefits the student's educational program.

Authorisation and controls

The principal reserves the right to restrict student access to the school's ICT facilities and devices if access and usage requirements are not met or are breached. However restricted access will not disrupt the provision of the student's educational program. For example, a student with restricted school network access may be allocated a stand-alone computer to continue their educational program activities.

The Department of Education and Training monitors access to and usage of their ICT network. For example, email monitoring will occur to identify inappropriate use, protect system security and maintain system performance in determining compliance with state and departmental policy.

The department may conduct security audits and scans, and restrict or deny access to the department's ICT network by any personal mobile device, if there is any suspicion that the integrity of the network might be at risk.

Responsibilities for using the school's ICT facilities and devices

- Students are expected to demonstrate safe, lawful and ethical behaviour when using the school's ICT network as outlined in the [Code of School Behaviour](#).
- Students are to be aware of [occupational health and safety](#) issues when using computers and other learning devices.
- Parents/guardians are also responsible for ensuring students understand the school's ICT access and usage requirements, including the acceptable and unacceptable behaviour requirements.
- Parents/guardians are responsible for appropriate internet use by students outside the school environment when using a school owned or provided mobile device.
- The school will educate students regarding cyber bullying, safe internet and email practices, and health and safety regarding the physical use of ICT devices. Students have a responsibility to behave in line with these safe practices.
- Use of the school's ICT network is secured with a user name and password. The password must be difficult enough so as not to be guessed by other users and is to be kept private by the student and not divulged to other individuals (e.g. a student should not share their username and password with fellow students).

- Students cannot use another student or staff member's username or password to access the school network, including not trespassing in another person's files, home drive, email or accessing unauthorised network drives or systems.
- Additionally, students should not divulge personal information (e.g. name, parent's name, address, phone numbers), via the internet or email, to unknown entities or for reasons other than to fulfil the educational program requirements of the school.
- Students need to understand that 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.

Responsibilities for using a personal mobile device

- Prior to any personal mobile device being used approval is sought from the school to ensure it reflects the department's security requirements.
- Students are responsible for the security, integrity, insurance and maintenance of their personal mobile devices and their private network accounts.
- All files are to be scanned using appropriate virus software before being downloaded to the department's ICT network.
- Follow any advice provided on best security requirements e.g. password protection (see [iSecurity](#) site for details).
- Students and parents are to employ caution with the use of personal mobile devices particularly as these devices can store significant numbers of files some of which may be unacceptable at school e.g. games and 'exe' files. An 'exe' file ends with the extension '.exe' otherwise known as an *executable* file. When they are selected they can install programs which may start unwanted processes.
- Any inappropriate material or unlicensed software must be removed from personal mobile devices before bringing the devices to school and such material is not to be shared with other students.
- Unacceptable use will lead to the mobile device being confiscated by school employees, with its collection/return to occur at the end of the school day where the mobile device is not required for further investigation.

Acceptable/appropriate use/behaviour by a student

It is acceptable for students while at school to:

- use mobile devices for
 - assigned class work and assignments set by teachers
 - developing appropriate literacy, communication and information skills
 - authoring text, artwork, audio and visual material for publication on the intranet or internet 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 dictionaries, encyclopaedias, etc.
 - researching and learning through the department's eLearning environment
- be courteous, considerate and respectful of others when using a mobile device
- switch off and place out of sight the mobile device during classes, where these devices are not being used in a teacher directed activity to enhance learning
- use personal mobile device for private use before or after school, or during recess and lunch breaks
- seek teacher's approval where they wish to use a mobile device under special circumstances.

Unacceptable/inappropriate use/behaviour by a student

It is unacceptable for students while at school to:

- use the mobile device in an unlawful manner
- download, distribute or publish offensive messages or pictures

- use of obscene, inflammatory, racist, discriminatory or derogatory language
- use language and/or threats of violence that may amount to bullying and/or harassment, or even stalking
- insult, harass or attack others or use obscene or abusive language
- deliberately waste printing and internet resources
- damage computers, printers or network equipment
- commit plagiarism or violate copyright laws
- ignore teacher directions for the use of social media, online email and internet chat
- send chain letters or spam email (junk mail)
- knowingly download viruses or any other programs capable of breaching the department's networks security
- use in-phone cameras anywhere a normal camera would be considered inappropriate, such as in change rooms or toilets
- invade someone's privacy by recording personal conversations or daily activities and/or the further distribution (e.g. forwarding, texting, uploading, Bluetooth use etc.) of such material
- use the mobile phone (including those with Bluetooth functionality) to cheat during exams or assessments
- take into or use mobile devices at exams or during class assessment unless expressly permitted by school employees.

Note: The Australian Mobile Telecommunications Association (<http://www.amta.org.au/>) has published materials which may be of use to schools including a [template](#) which can assist in creating an acceptable use policy.

Web filtering - Removing online content

The following information is provided as a guide to state schools when seeking to remove and report the uploading of inappropriate images/ footage to websites, particularly where school employees and/or students are involved, or if the school is in some way associated.

Incident awareness

The incident may come to your attention through employees, students, parents, community members, the media etc.

Step 1: Incident investigation

Principal or their delegate undertakes immediate investigation of the incident by reviewing the web content of concern.

Website is accessible

Assessing the website of concern to review content to determine if further action is required.

Website is inaccessible

If the website is blocked contact the Service Centre by phone on 1800 680 445 to discuss options for available or escalate to the Cybersafety & Reputation Management Team for further investigation.

Step 2: Where employees, students or any school community members have been threatened, or are in danger as a result of the incident, the principal should take the school's usual emergency response process or report the incident to the regional director.

Step 3: Requesting removal of content from a website

If the student responsible refuses to delete the inappropriate or offensive content or the identity of the person who posted the material is not known, then the principal, delegate, or victim should report the content to the site's service provider and ask to have it removed.

Where the website provides contact information

Coordinate with those directly involved for removal of information. Alternatively, where possible, directly request the website to remove the content.

For assistance in removing content seek advice from the Cybersafety & Reputation Management Team on (07) 3034 5035, Cybersafety.ReputationManagement@deta.qld.gov.au or [Regional Technology Manager](#).

Step 4: Minimising access to offensive content

The principal should assess whether the website housing the offensive content requires blocking through the school and departmental network.

Website does not require blocking

No further action is required.

Request blocking of a website

School level: Request to block a website through school's [Regional Technology Manager](#).

Departmental level: Request to block website through the Service Centre on 1800 680 445.

Step 5: Reporting incidents

For employee misconduct contact the Ethical Standards Unit, email: ethicalstandards@deta.qld.gov.au or phone: (07) 3234 1514

For further information about the removal of inappropriate images/footage on websites, contact:
Cybersafety & Reputation Management Team
Learning Technologies
Phone: (07) 3034 5035
Email: Cybersafety.ReputationManagement@det.qld.gov.au

Assistance on removing content from the internet can also be sought from your [Regional Technology Manager](#).

Security and licence

This document has an information security classification of public.

© The State of Queensland (Department of Education and Training) 2013

Unless otherwise noted below, materials included in this paper are licensed under a Creative Commons Attribution 3.0 Australia licence. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/3.0/au/>



Last review date: 7 April 2014 Final TRIM Ref: 14/33001

Uncontrolled copy. Refer to the Department of Education and Training Policy and Procedure Register at <http://ppr.det.qld.gov.au> to ensure you have the most current version of this document.