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

Information for Students and Parents On School ICT Network Usage

Why are schools providing student access to Information Communication and Technology (ICT) facilities?

To ensure young Queenslanders are well equipped to contribute fully to the information economy, the education sector is responding to the innovation directions of the *Smart State Strategy* through *Smart Classrooms*.

This 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. These technologies are vital for the contemporary educational program provided in schools. At all times students will act in line with the requirements of the Code of School behaviour and the specific rules of their school

What is acceptable/appropriate use/behaviour by a student?

It is acceptable for students to use school computers and network infrastructure 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 e-learning environment.

What is unacceptable/inappropriate use/behaviour by a student?

It is unacceptable for students to:

- use the IT resources in an unlawful manner
- download, distribute or publish offensive messages or pictures;
- insult, harass or attack others or use obscene or abusive language;
- deliberately waste printing and Internet resources;
- damage computers, printers or the network equipment;
- commit plagiarism or violate copyright laws;
- use unsupervised internet chat;
- use online email services (e.g. hotmail), send chain letters or Spam e-mail (junk mail)
- knowingly download viruses or any other programs capable of breaching the Department's networks security.

Usernames and passwords are to be kept private by the student and not divulged to any other individual (e.g. a student should not share their username and password with fellow students).

Students can not use another student or staff member's username or password to access the school's network, including not trespassing in another person's files, home drive or e-mail.

Additionally, students should not divulge personal information (e.g. name, parent's name, address, phone numbers), via the internet or e-mail, to unknown entities or for reasons other than to fulfil the educational program requirements of the school.

Students and parents are to employ caution with the use of mobile devices e.g. USBs, particularly as these devices can store significant numbers and sizes of files some of which may be unacceptable at school e.g. games and "exe" files which may contain viruses.

Please note that personal files on USBs may be deleted by the Department's malware protection.

What is expected of schools when providing student's with access to ICT facilities?

Schools will provide information in relation to student access to and use of the network and reserve 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 guideline/statement.

Schools will prepare students for the possibility of unanticipated access to harmful information, materials or approaches from unknown persons via the internet or email.

Schools will ensure 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 1 to1 Learning Program need to ensure all steps have been taken to provide a safe and effective learning environment for students while meeting the Department's standards for network usage and access security.

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;
- ensure they have the skills to report and discontinue access to harmful information if presented via the internet or e-mail;
- be aware that:
    - access to ICT facilities provides valuable learning experiences for students and supports the school's teaching and learning programs;
    - ICT facilities should be used appropriately as outlined in the Code of School Behaviour;
    - the Principal may determine that student privately owned devices may not be used at the school;
    - students who use a school's ICT facilities in a manner which is not appropriate may be subject to disciplinary action by the school, including restricting network access;
    - despite departmental systems to manage all access to information 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.