MIDDLE SENIOR SCHOOLS STUDENT ICT NETWORK ACCESS AND USAGE POLICY

Information and Communication Technologies (ICTs) are valuable tools which enhance the college educational program. The college ICT infrastructure is part of the Department of Education and Training's statewide network which is a managed operating environment. Further information about the services provided by DET can be found in the Smart Classrooms site and the 2014-17 Digital Strategy at http://education.qld.gov.au/smartclassrooms/index.html and http://deta.qld.gov.au/publications/strategic/pdf/dete-digital-strategy-2014-17.pdf

At all times students will act in line with the requirements of the Code of School behavior and the specific rules of the college.

It is an expectation of enrolment that Year 7–11 students participate in the college Bring Your Own Device (BYOx) Program and bring a laptop (which meets minimum specifications) to school each day. Families experiencing financial hardship may apply to join the College Equity Program. Bringing a laptop to school each day is a condition of participation in the Academic Achievers and Music Excellence Programs, and these students are not eligible for the BYOx Equity Program. Year 12 students may choose to participate in the optional Purchase Your Own Device (PYOD) program. Information about these programs can be found on the college website

https://kelvingrovesc.eq.edu.au/Facilities/Computersandtechnology/Pages/Computersandtechnology.aspx.

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

Use of college network through college approved ICTs (including BYOx & PYOD)

Students may use ICTs for educational purposes, and to complete class and assessment tasks set by teachers, including:

- creating text, artwork, audio and visual material
- conducting research
- accessing online reference material such as dictionaries, encyclopedias, etc.
- communicating or collaborating with other students, teachers, parents or experts through DETE's email (http://owa.eq.edu.au/) and eLearning environments i.e. The Learning Place (http://education.qld.gov.au/learningplace/) and eLearn (http://elearn.eq.edu.au)
- developing literacy, communication and information skills

Senior School Students Only: Use of Mobile Devices during Teacher Directed Learning

On the occasion that a student can't access their BYOx or PYOD device, students may use personal mobile devices* with teacher permission. The college takes no responsibility for security, loss or damage to the mobile device, or associated costs of mobile device data.

It is acceptable for students during teacher directed learning to use personal mobile devices for

- assigned class learning and assessment tasks set by teachers
- developing appropriate literacy, communication and information skills
- authoring text, artwork, audio and visual material for publication on the authorised eLearning spaces for internet for educational purposes as supervised and approved by the college
- conducting general research for school activities and projects
- communicating or collaborating with other students, teachers, or experts in relation to school work
- accessing online references such as dictionaries, encyclopaedias, etc.
- researching and learning through the department's eLearning environment

It is expected that students will:

- be courteous, considerate and respectful of others when using a mobile device
- observe KGSC mobile use policy, and 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

*Mobile devices include but are not limited to laptops, tablet devices, voice recording devices (whether or not integrated with a mobile phone, MP3 player or other device), games devices, USBs, DVDs, CDs and smart phones.

What is unacceptable and inappropriate use or behaviour by a student?

Unacceptable use of college network and approved ICTs (including BYOx and PYOD) includes, but is not limited to:

- using in an unlawful manner

- using in a way not explicitly directed to do so by the teacher
- giving usernames and passwords to any other individual
- logging in or using another user's network account to access the network, files, email or internet
- using for non-educational purposes
- connecting private BYOx and PYOD laptops into college power
- storing inappropriate or offensive material on BYOx and PYOD laptops
- downloading, distributing or publishing offensive messages or pictures
- using obscene or abusive language, especially to harass, insult or attack others
- wasting printing, internet and other resources, including using these for non-educational purposes
- damaging ICTs eg computers, printers or network equipment
- violating copyright laws including plagiarism
- using unsupervised internet chat
- using online e-mail services (e.g. Hotmail)
- sending chain letters or spam e-mail (junk mail).
- creating, downloading, using or circulating anything that attempts to bypass, hack into or disable departmental and college security systems including virus protection, internet filtering
- entering a computer room or using ICTs without a staff member's permission and presence

Unacceptable use of mobile devices during teacher directed learning includes, but is not limited to:

- using the mobile device in an unlawful manner
- using the mobile device in a way not explicitly directed to do so by the teacher
- download, distribute or publish offensive messages or pictures
- storing inappropriate or offensive material on mobile devices used at school
- use of 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
- insult, harass or attack others or use obscene or abusive language
- 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-device 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 device (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 college staff.
- connecting private mobile devices into college power, workstations or other equipment for charging purposes. These devices must not be charged while at school for workplace health and safety reasons, and due to electricity costs.
- deliberately waste printing and internet resources

Personal safety:

To ensure personal safety, students should not give personal information (e.g. name, parent's name, address), via the internet or e-mail to unknown people or organisations, or for reasons other than to fulfil the educational program requirements of the college.

Parents\caregivers should be aware that mobile devices enable access to networks and internet services which may not be secure or include filtering. The college takes no responsibility for security issues or content accessed by students using non college network or internet services, including on mobile devices, at any time.

Device and data security:

Private devices including for storage (e.g. USBs or external hard drives) should be regularly scanned using security software to ensure that they do not contain viruses, malware etc. Please note that personal files may be deleted by the DET security systems. Private devices should be backed up regularly; failure to do so is not grounds for extensions for assessment tasks. Illegal software and non-educational programs should not be installed on private devices used at school.

What awareness is expected of students and their parents\carers?

Students and their parents\carers should:

- understand the responsibility and behaviour requirements that come with accessing the DET and college ICT infrastructure and services
- ensure they have the skills to report and discontinue access to harmful information on the internet or via e-mail
- be aware that:
  - access to ICTs provides valuable learning experiences for students and supports the college's teaching and learning programs
  - ICT infrastructure and services should be used appropriately as stipulated under the department's **Code of School Behaviour;**
  - students who use ICTs in a manner which is not appropriate and breaks departmental and college rules will be subject to disciplinary action by the college. This may include
    - detentions
    - restricted network, internet and\or email access for a period of time as deemed appropriate
    - removal from subjects that require the use of ICTs
    - notification to School Based Police Officer
    - suspension from school for a period of time as deemed appropriate
    - exclusion from school
  - despite departmental and college systems to manage all access to information on the Internet, illegal, dangerous or offensive information may be accessed or accidently displayed
  - teachers will always exercise their duty of care, but avoiding or reducing access to harmful information also requires responsible use by the student

Website Risk Assessment Register

The use of web based educational resources has risen steadily over the last decade and are increasingly being used by teachers to improve student learning outcomes.
Our school and teachers make decisions about the best technology to meet the needs of our students. Sometimes it is beneficial for students to utilise services provided by third party web based providers.

The third party web based services generally require students to be registered as a user. This process may require student personal information to be used (eg. name, email address) in the registration process, which can be stored in or outside of Australia (i.e. on servers not based in Australia that are therefore not bound by Queensland's privacy laws).

Parents\carers should understand what information is collected, how it is used, who accesses it and where the data is stored and consider the implications of use for each third party web based service used by their students.

Refer to the College Website Risk Review Register for information about third party web based services used in the College.
https://kelvingrovesc.eq.edu.au/Facilities/Computersandtechnology/Pages/Website-Risk-Review-Register.aspx

If you do not wish to provide consent for your student\s for a particular third party web based service, please email info@kelvingrovesc.eq.edu.au .

Please include the following details:

- "Attention HOD eLearning" in the subject heading
- your student's name and year level
- the name of the third party web based service
- the web address of the third party web based service

ICT Network Access and Usage Agreement:

This agreement (see separate page) must be signed by the student and by his/her parent or guardian on enrolment and a current version signed at the beginning of each school year in the Student Diary.

Need further assistance?

If you have any concerns re student access to and use of ICT facilities and services provided by KGSC, or use of private mobile devices, please contact the Head of Department, Teaching and eLearning on 07 3552 7333 or email info@kelvingrovesc.eq.edu.au

MIDDLE SENIOR SCHOOLS STUDENT ICT NETWORK ACCESS AND USAGE AGREEMENT

Student Agreement:

- I have read and understood the Kelvin Grove State College Student ICT Network Access and Usage Policy on the college website (Support and Resources tab, Forms and Documents, Policy documents)
- I agree to access and use the ICT facilities and services provided by Kelvin Grove State College and personal devices (including mobile devices for Senior School students) in accordance with this policy
- I agree to accept the consequences for my actions if I choose to breach the policy and this agreement

Student Name: (Print)									
Year Level:		**Username (if known):**							
Signature:									
Date:									

Parent/Guardian Agreement:

- I have read and understood the Kelvin Grove State College ICT Network Access and Usage Guidelines on the college website (Support and Resources tab, Forms and Documents, Policy documents)
- I give consent for my student to access and use the ICT facilities and services provided by the Department and Education and Training and Kelvin Grove State College, and personal devices in accordance with the college's Student ICT Network Access and Usage Policy (**See note below)*
- I agree to accept the consequences of these actions for my student if he/she chooses to breach the policy and this agreement

Parent/Guardian Name: (Print)	
Signature:	
Date:	

If you have any concerns re student access to and use of ICT facilities and services provided by KGSC, or use of private devices, please contact the Head of Department, Teaching and eLearning on 07 3552 7333 or email info@kelvingrovesc.eq.edu.au

Further information about the Computers and Technology at Kelvin Grove State College can be found on the college website at https://kelvingrovesc.eq.edu.au/Facilities/Computersandtechnology/Pages/Computersandtechnology.aspx