Computer Use at School and Taken Home

The aim of the Australian Government's Digital Education Revolution (DER) is to ensure all Year 9-12 students have improved access to computers to improve their learning. To this end, Stuart High School, together with the Department of Education and Children's Services (DECS), have embarked on an extensive program to upgrade and increase the number of computers in school. The agreement will remain in force as long as your child is enrolled at this school.

As part of the program, Use Agreements are required to be signed by students and parents/caregivers in relation to the use of the computers at school and if on loan to be taken home. This agreement supersedes all previous signed agreements relating to computer use in schools.

When a computer is taken home it is considered to be on loan from the school to the student for either a short or long term period.

If it becomes necessary to add/amend any information or condition, you will be advised in writing.

Acceptable Use

As is the case with all Information and Communication Technologies (ICTs) in DECS' schools and preschools, policies on the safe and acceptable use of ICT apply to DER computers.

All students and their parents/caregivers are required to sign a Use Agreement which covers the care, use and management of computers in a cyber-safe learning environment. Included in the management are security, email, Internet access and virus protection as well as cyber-safety.

The use of school applications and files is for the benefit of students' learning. As such the use of the allocated computing resource is on the understanding that your child will access applications and files in safe and ethical ways. Your child needs to be aware that the school's wellbeing and behaviour management processes extend outside of school hours or off site.

Stuart High School reserves the right to monitor the content of computers on loan. This may involve the student returning the computer to Stuart High School for a random inspection of the contents.

Cyber-safety

Stuart High School is committed to being a cyber-safe learning environment. Please see the attachment "*Strategies to help keep students Cyber-safe"* for strategies to help us stay safe when using ICT at school and after formal school hours.

It should be noted that if a student who is enrolled in a school behaves online in a manner that threatens the wellbeing of another child, student, parent or member of the school community, even if this occurs off-site and/or out of school hours, the principal has the authority under the Regulation pursuant to the Education Act 1972 to suspend or exclude a student from attendance at school.

If the principal suspects an electronic crime has been committed, this must be reported to the South Australian Police Department (SAPOL). Where there is a further reasonable suspicion that evidence of a crime, such as an assault, is contained on a mobile phone or other electronic device eg computer, the device will be confiscated and handed to the investigating police officer. SAPOL will determine any further action.

2/…

Responsibilities when Computers are used at School and are Taken Home

Care of computers

Students are expected to care for loan computers in relation to carrying, cleaning, storage and security both on and off-site. The virus protection software which is installed must be kept up to date and not tampered with.

Students are expected to bring loan computers fully charged to school each day.

Parents must ensure that students report lost, stolen or damaged computers to the school within 24 hours of the incident occurring. If a computer has been lost or stolen, it must be reported to the police.

In some cases, parents may be responsible for the full replacement cost of the computer, eg if the damage is wilful or if it is lost from an unsecured location.

If a loan computer is damaged or lost by neglect, abuse or malicious act, the principal will determine whether replacement is appropriate and/or whether or not the student retains access to a computer on loan for home use. In such cases repair or replacement costs may be passed on to the parent/caregiver for payment. School policies related to the recovery of debts will apply.

Where a loss or damage occurs that is not covered by parents' car or home contents insurance policies, students will, at the discretion of the principal, receive no more than one replacement computer during the time they are participating in the program. Parents/caregivers may be required to contribute to the cost of the second replacement.

Any replacement computer will usually be the same age and model as the one it replaces and may be pre-used by other students.

Repair and maintenance

The school is responsible for the repair and maintenance of computer computers through regular maintenance or servicing schedules. Students will be notified of such scheduling.

Loan computers
Stuart High School has established a small pool of replacement loan computers for students to use if an on loan computer is unavailable for more than five days because it is being repaired under warranty or after being damaged. Availability of a replacement loan computer is not guaranteed.

Software

A standard suite of programs will be installed by Stuart High School, including a word processing package, spreadsheet, publishing and presentation software. Antivirus, networking and anti-spyware software will also be installed. The software is not to be modified unless as part of the regular update process. No software installed by Stuart High school is to be disabled or removed.

Network setting must not be altered. When installing 3G wireless broadband, such as BigPond, Optus or Internode, the original network settings must not be altered. Technical advice will be available from Stuart High School.

At all times the performance of computers is for the primary purpose of student learning. Some software can slow down the performance of the device or corrupt it so that it is unusable. Approval from the school must be sought before loading non-school software. Some software, even if approved for installation, may not be supported by the school.

The consequence of contravening school policies on the use of non-school applications may be the restoration of the computer to its original specifications, with the consequential loss of all student data. It is the responsibility of the student to ensure files related to their learning are backed-up in an alternative location as good practice. Persistent contravening of the school policy could result in recall of the on-loan device and / or loss of access for home use.

Transfer of Ownership

If your child leaves before completing Year 10, any loan computer must be returned to the school. As part of the return process, a maintenance check will occur to ensure that the computer is in good order. Any repair or replacement costs may be passed on to the parent/caregiver for payment. School policies related to the recovery of debts will apply.

If your child leaves at the end of Year 10, ownership of a three year old computer with the originally supplied base operating system may be transferred from the Minister of Education to her/him.

Such a transfer requires a formal transaction and payment of $1 (GST Inc)[1]. Specific details about disposal will be communicated to you closer to the time.

Strategies to help keep students Cyber-safe

Parents/caregivers play a critical role in developing knowledge, understanding and ethics around their child's safety and safe practices for themselves and the people around them regardless of the time of day. Being cyber-safe is no exception, and we invite you to discuss with your child the following strategies to help us stay safe when using ICT at school and after formal school hours.

1. I will not use school ICT equipment until my parents/caregivers and I have signed my *Computer Use Agreement Form* and the completed form has been returned to school.

2. If I have my own user name, I will log on only with that user name. I will not allow anyone else to use my name.

3. I will keep my password private.

4. While at school or a school related activity, I will inform the teacher of any involvement with any ICT material or activity that might put me or anyone else at risk (eg bullying or harassing).

5. I will use the Internet, e-mail, mobile phones or any ICT equipment only for positive purposes, not to be mean, rude or offensive, or to bully, harass, or in any way harm anyone else, or the school itself, even if it is meant as a joke.

6. I will go online or use the Internet at school only when a teacher gives permission and an adult is present.

7. While at school, I will:
   - access, attempt to access, download, save and distribute only age appropriate and relevant material
   - report any attempt to get around or bypass security, monitoring and filtering that is in place at school.

8. If I accidentally access inappropriate material, I will:
   - not show others
   - turn off the screen or minimise the window
   - report the incident to a teacher immediately.

4/…

9. To ensure my compliance with copyright laws, I will download or copy files such as music, videos, games or programs only with the permission of a teacher or the owner of the original material. If I infringe the Copyright Act 1968, I may be personally liable under this law. This includes downloading such files as music, videos, games and programs.

10. My privately owned ICT equipment/devices, such as a computer, mobile phone, USB/portable drive I bring to school or a school related activity, is also covered by the Use Agreement. Any images or material on such equipment/devices must be appropriate to the school environment.

11. Only with written permission from the teacher will I connect any ICT device to school ICT, or run any software (eg a USB/portable drive, camera or phone). This includes all wireless/Bluetooth technologies.

12. I will ask my teacher's permission before I put any personal information online. Personal identifying information includes any of the following:
    - my full name
    - my address
    - my e-mail address
    - my phone numbers
    - photos of me and/or people close to me.

13. I will respect all school ICTs and will treat all ICT equipment/devices with care. This includes:
    - not intentionally disrupting the smooth running of any school ICT systems
    - not attempting to hack or gain unauthorised access to any system
    - following all school cyber-safety strategies, and not joining in if other students choose to be irresponsible with ICTs
    - reporting any breakages/damage to a staff member.

14. The school may monitor traffic and material sent and received using the school's ICT network. The school may use filtering and/or monitoring software to restrict access to certain sites and data, including e-mail.

15. The school may monitor and audit its computer network, Internet access facilities, computers and other school ICT equipment/devices or commission an independent forensic audit. Auditing of the above items may include any stored content, and all aspects of their use, including e-mail.

16. If I do not follow cyber-safe practices, the school may inform my parents/caregivers. In serious cases, the school may take disciplinary action against me. My family may be charged for repair costs. If illegal material or activities are involved or e-crime is suspected, it may be necessary for the school to inform the police and hold securely personal items for potential examination by police. Such actions may occur even if the incident occurs off-site and/or out of school hours.

5/…

Important terms:

'Cyber-safety' refers to the safe use of the Internet and ICT equipment/devices, including mobile phones.

'Cyber bullying' is bullying that uses e-technology as a means of victimising others. It is the use of an Internet service or mobile technologies - such as e-mail, chat room discussion groups, instant messaging, webpages or SMS (text messaging) - with the intention of harming another person.

'School and preschool ICT' refers to the school's or preschool's computer network, Internet access facilities, computers, and other ICT equipment/devices as outlined below.

'ICT equipment/devices' includes computers (such as desktops, computers, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video and digital cameras and webcams), all types of mobile phones, gaming consoles, video and audio players/receivers (such as portable CD and DVD players), and any other, similar, technologies.

'Inappropriate material' means material that deals with matters such as sex, cruelty or violence in a manner that is likely to be injurious to children or incompatible with a school or preschool environment.

'E-crime' occurs when computers or other electronic communication equipment/devices (eg Internet, mobile phones) are used to commit an offence, are targeted in an offence, or act as storage devices in an offence.

'Computer' includes either a desktop, laptop, notebook, netbook or tablet device.