Penola High School

JCT & Cyber Safety

User Agreement

Student Name:.................................................................

The measures to ensure appropriate use of ICT equipment/devices and the cyber-safety of Penola High School are based on our vision and motto.

To assist Penola High School to enhance learning through the safe use of information and communication technologies (ICTs), parents / caregivers are asked to read this document and sign the attached User Agreement Form.

It is an expectation that students will make use of the available technologies in line with the school values and behaviour code. This user agreement is to be completed by all students wishing to make use of the Information Technology systems and Internet facilities at Penola High School.

Rigorous cyber-safety practices are in place, which include User Agreements for staff and students, Child protection education and provision of information about remaining safe when using new technologies. The computer network, Internet access facilities, computers and other ICT equipment/devices bring great benefits to the teaching and learning programs at Penola High School, and to the effective operation of the school. The ICT equipment is for educational purposes appropriate to this environment, whether it is owned or leased either partially or wholly by the school, and used on or off the site.

All students will be issued with a User Agreement and once signed consent has been returned to school, students will be able to use the school ICT equipment.

Appropriate Use of Online Services

The Department of Education and Children’s Service’s (DECS) online services such as e-mail, Internet access, instant messaging and learning services are provided to assist students in their education. By using these services students agree to follow the strategies set out in the User Agreement and to abide by DECS policies. Students and their parents/caregivers also give consent to logging, monitoring, auditing and disclosure of students’ use of these services.

Inappropriate use of these services can result in disciplinary action that may include withdrawal of access to services or suspension or exclusion from attendance at school, as per the DECS School Discipline Policy. The Department of Education and Children’s Services, Student Online Policy and other related documents can be viewed at:


Material sent and received using the network may be monitored and filtering and/or monitoring software may be used to restrict access to certain sites and data, including e-mail. Where a student is suspected of an electronic crime, this will be reported to the South Australia Police. Where a personal electronic device such as a mobile phone is used to capture images of a crime, such as an assault, the device will be confiscated and handed to the police.

Inappropriate Use

Inappropriate use includes, but is not limited to:

- Infringing on others intellectual property including copyright and trade mark rights.
- Unauthorised access to private or confidential material.
- Conducting of any business or activity for financial gain.
- The creation, accessing, transmission, retrieval and storage of offensive material.
- Impersonating someone else or unauthorised access to another’s files.
- Soliciting money, services or information by false pretences.
- Generating or passing on chain letters or sending unsolicited mail (junk mail).

The access, transmission, retrieval, storage or display of the following is strictly unacceptable unless forming the part of a legitimate educational inquiry as laid out in writing by a teacher:
- Sexually explicit material.
- Hate speech or offensive material.
- Material regarding illicit drugs or violence.
- Material regarding criminal skills and/or illegal activities.
- Material of a defamatory, discriminatory or harassing nature.

**Appropriate Use of Mobile and Loaned Devices**

Prior to distribution and use of any learning technologies all students and their parents/caregivers are required to sign a *User Agreement*. This 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 learning technologies including applications and files is for the benefit of student learning. The use of allocated and loaned resources is on the understanding that the user will access applications and files in safe and ethical ways. Students and their parents/caregivers must be aware that the school’s *Student Management* process encompasses outside of school hours and off-site use and behaviours.

It is an expectation that students will make use of the available technologies in line with the school values and behaviour code.

Digital devices provided by Penola High School are only available for the use of enrolled students and other authorised persons. They are not to be used for private business or other unauthorised activities. Equipment has been set up to enable the user to have access to the applications that are needed to fulfil course requirements.

The use of allocated and loaned resources is on the understanding that the user will access applications and files in safe and ethical ways. Students and their parents/caregivers must be aware that the school’s *Student Management* process encompasses outside of school hours and off-site use and behaviours.

Use that breeches the User Agreement will result in sanctions in line with the Student Management and DECS Policy. Breeches of an illegal nature will be forwarded to the police.

**Ownership**

All equipment purchased through the DER program is the property of the South Australian Minister for Education.

If a student leaves before completing Year 12, any loan equipment must be returned to the school. As part of the return process, a maintenance check will occur to ensure that the equipment 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.

**Transport, Care and Storage of Learning Technologies**

Staff and students are expected to care for learning technologies and digital devices.

Staff and students have access to digital devices with the knowledge that devices are in good care and working order. At the time of use individuals are required to report operational or damage issues to the Penola High School Computer Systems Manager.

In the case where a loan device has been provided to a student for in school use, it is provided in good care and working order and is confirmed at the time. If at any time there are operational or damage issues, the user will report it to the Penola High School Computer Systems Manager using the appropriate documentation. If the damage is wilful or if the device is lost from an unsecured location, the user or their parents/caregivers may be responsible for the full replacement cost of the device. School policies related to the recovery of debts will apply.
If a loan device is damaged or lost by neglect, abuse or malicious act, the principal will determine whether replacement is appropriate and/or whether or not the individual retains access to another loan laptop for home use. In such cases repair or replacement costs may be passed on to the user or their parent/caregiver for payment. School policies related to the recovery of debts will apply. Students will be provided with a laptop bag in which they will store and transport their devices. Devices available for loan will be loaned along with the bag they are stored in. Devices must be secured in a bag when moving from one learning space to another.

**Personal Mobile Devices**

Mobile devices may only be used to support or enhance learning. Students are expected to demonstrate etiquette in the use of personal mobile and portable devices at school. Any conditions that are requested of the individual to use such equipment must be adhered to in the interest of the security of the network.

Penola High School reserves the right to monitor the content of mobile devices used by students at school. It is a condition of use that any personal storage device, mobile technology or media found in possession of a student will be presented to staff on request for checking if reasonable doubt exists as to the appropriate nature of the contents. Failure to comply with such requests and use that breaches the User Agreement will result in sanctions in line with the Student Management and DECS Policy. Breeches of an illegal nature will be forwarded to the police.

**Guidelines**

Unless their use forms part of a legitimate educational inquiry as laid out in writing by a teacher mobile devices are to be switched off in all buildings and are not to be visible in class. Except for critical calls mobile phones are only to be used out of lesson times and out of the school buildings.

1. **Negotiation** with the Deputy Principal needs to occur if a critical call is expected and in most circumstances these phone calls should be directed through the front office.
2. **Students must complete the ICT & Cyber-safety User Agreement prior to bringing a mobile device to school.**
3. **If students are unwell, arrangements for going home need to be made through the Front Office, not from students’ mobile phones.**
4. **Students must take full responsibility for the security of their mobile devices.** The school takes no responsibility for lost, stolen, or damaged devices.
5. **Mobile devices are not to be used in change rooms, toilets or sleeping areas at school or when involved in school activities (excursions/camps).**
6. **Inappropriate use of mobile devices will be dealt with through the school Student Management Policy.**
7. **In the event that students do not have their devices switched off inside the building or are found using mobile devices for reasons other than as a part of a legitimate learning program during a lesson the following consequences will apply:**
   - **First offence:** The teacher will warn the student and ask them to put the device away.
   - **Second offence:** The teacher will request the device and pass the device and information on to the Deputy Principal / Principal who will record the infringement. The device will be kept for the remainder of the day.
   - **Third offence:** The teacher will request the device and pass the device and information on to the Deputy Principal / Principal who will record the infringement and call home. The phone will be kept for the remainder of the day.
   - **Fourth offence:** The teacher will request the device and pass the device and information on to Deputy Principal / Principal. The device will be kept in the school safe for one week.
   - **Fifth offence:** The Principal / Deputy Principal will speak with the parent / caregiver about the student no longer being able to have the device at school.

Teachers may ask students to leave their mobile devices with the teacher if they need to leave the classroom during class time.
Security

It is an expectation that passwords are changed regularly, and if it is considered likely that the password has been breached, that the password is changed as a matter of expediency and a staff member informed.

A user should not intentionally, or by negligence, divulge to anyone else the password(s) associated with their login or anyone else’s. Nor should they allow others to use their login.

Students should not attempt to interfere with computer equipment in any way, specifically when it may lead to malicious damage of infrastructure or systems.

Cyber-safety

Penola High School is committed to being a cyber-safe learning environment. Students will undertake Cyber-safety seminars as a part of their induction into Year 8.

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 laptop, the device will be confiscated and handed to the investigating police officer. SAPOL will determine any further action.

While every reasonable effort is made by schools and DECS administrators to prevent student’s exposure to inappropriate content when using the department’s online services, it is not possible to completely eliminate the risk of such exposure. In particular, DECS cannot filter Internet content accessed by your child from home, from other locations away from school or on mobile devices owned by your child. DECS recommends the use of appropriate Internet filtering software.


Please contact the principal, if you have any concerns about your child’s safety in using the Internet and ICT equipment/devices.

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 User 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 use my mobile phone/s only at the times agreed to by the school during the school day.
7. I will go online or use the Internet at school only when a teacher gives permission and an adult is present.
8. 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.
9. 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.
10. 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.
11. My privately owned ICT equipment/devices, such as a laptop, mobile phone, USB/portable drive I bring to school or a school related activity, also is covered by the Use Agreement. Any images or material on such equipment/devices must be appropriate to the school environment.
12. 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.
13. 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.
14. 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.
15. 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.
16. 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.
17. 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.
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 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, laptops, 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.
ICT & CYBER-SAFETY USER AGREEMENT

To the parent/caregiver/legal guardian:
Please read this page carefully to check that you understand your responsibilities under this agreement. Please return the entire signed User Agreement to the school and keep a copy for your reference.

I understand that Penola High School will:
• do its best to enhance learning through the safe use of ICTs. This includes working to restrict access to inappropriate, illegal or harmful material on the Internet or on school ICT equipment/devices at school, or at school related activities; and enforcing the cyber-safety requirements detailed in User Agreements
• respond to any breaches in an appropriate manner
• provide members of the school community with cyber-safety education designed to complement and support the User Agreement initiative
• welcome enquiries at any time from parents/caregivers/legal guardians or students about cyber-safety issues.

For the Parent/Caregiver/Legal Guardian: My responsibilities include:
• reading this ICT & Cyber-safety User Agreement carefully and discussing it with my child so we both have a clear understanding of our roles in the school's work to maintain a cyber-safe environment
• ensuring this User Agreement is signed by my child and by me and returned to the school
• encouraging my child to follow the cyber-safe strategies and instructions
• contacting the school if there is any aspect of this Use Agreement I would like to discuss.

We have read and understood this ICT & Cyber-safety User Agreement and we are aware of the school's initiatives to maintain a positive learning environment.

Name of parent/caregiver/legal guardian.......................................................... .......................................................... .......................................................... ..........................................................
Signature of parent/caregiver/legal guardian .................................................. Date..............2013
.................................................................................. Date..............2014
.................................................................................. Date..............2015
.................................................................................. Date..............2016
.................................................................................. Date....... ......2017

For the Student: My responsibilities include:
• reading this ICT & Cyber-safety User Agreement carefully
• following the cyber-safety strategies and instructions whenever I use the school's ICTs
• following the cyber-safety strategies whenever I use privately-owned ICT devices on the school site or at any school related activity, regardless of its location
• avoiding any involvement with material or activities that could put at risk my own safety, or the privacy, safety or security of the school or other members of the school community
• taking proper care of school ICTs. I know that if I have been involved in the damage, loss or theft of ICT equipment/devices, I and/or my family may have responsibility for the cost of repairs or replacement
• keeping this document somewhere safe so I can refer to it in the future
• asking the Year Level Manager if I am not sure about anything to do with this agreement.

Name of student.......................................................................................... ..........................................................
Signature of student .................................................................................. Date...............2012
.................................................................................. Date..................2013
.................................................................................. Date..................2014
.................................................................................. Date..................2015
.................................................................................. Date..................2016

Phone type and model: .......................................................... Mobile phone number: ..........................................................

Please note: This agreement will remain in force as long as your child is enrolled at this school.
If it becomes necessary to add/amend any information or rule, you will be advised in writing.