



SCHOOL NETWORK, INTERNET and CYBER SAFETY USE POLICY

To enhance learning through the safe use of information and communication technologies (ICT), please read this with your child to understand their responsibilities under this agreement and sign the permission slip that is included in the new student enrolment pack.

Our computer systems bring great benefits to the teaching and learning programs at PASS and to the effective operation of the school. Our ICT equipment is provided for educational purposes, appropriate to this environment.

This policy includes information about your child's obligations, responsibilities, and the nature of possible consequences associated with cyber-safety breaches that undermine the safety of the school environment.

Where a student is suspected of an electronic crime, this will be reported to the South Australian 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.

While every reasonable effort is made by PASS and DfE 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, DfE cannot filter Internet content accessed by your child from home, from other locations away from school or on mobile devices owned by your child.

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 encourage you to discuss this issue with your child and view the following websites to stay safe when using ICT at school and after formal school hours.

① <https://esafety.gov.au/youngandesafe>

① <https://www.kidshelpline.com.au>

① <https://www.esafety.gov.au/education-resources/parent>

① <http://www.bullyingnoway.com.au>

① <https://www.education.sa.gov.au/parenting-and-child-care/parenting/parenting-sa>

Below are the PASS expectations

1. I will log on only with my own user name. I will not allow anyone else to use my account.
2. I will keep my password private.
3. 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).
4. I will use the computer systems 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.
5. I will use my mobile phone/s only at the times agreed to by the school during the school day.
6. I will go online or use the Internet at school only when a teacher gives direction.
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
 - report any inappropriate material that is accessed to a teacher immediately.
8. To ensure copyright laws are abided by, 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.
9. My privately owned ICT equipment/devices I bring to school or a school related activity, are also covered by this policy. Any images or material on such equipment/devices must be appropriate to the school environment. I understand that if I am required to connect my equipment/device to a power source, that it must be electrically tested by the Resource Technology Centre before it is used on site.
10. I understand that the school does not provide insurance for accidental loss or damage to student owned devices. Claims may only be met under the department's public liability insurance where the loss or damage is attributable to a negligent act or omission on the part of the school.

11. I will follow all cyber-safety practices before I put any personal information online.
12. I will respect and treat all ICT equipment/devices with care and not cause any damage to equipment. This includes:
 - reporting any breakages/damage to a staff member
 - following all school cyber-safety strategies, and not joining in if other students choose to be irresponsible with ICT systems and networks
 - not attempting to hack or gain unauthorised access to any system
13. 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.
14. The school may monitor and audit its computer systems and network, 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.
15. If I do not follow this use agreement, 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 securely hold personal items for potential examination by police. Such actions may occur even if the incident occurs off-site and/or out of school hours.
16. **Signing the permissions slip acknowledges that you are aware and will abide by the following:**
 - follow the cyber-safety strategies and instructions whenever I use the school's ICT systems and networks
 - follow 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
 - avoid 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
 - take proper care of school ICT systems and networks. I know that if there is evidence that I have caused damage, loss or theft of ICT equipment/devices, I and/or my family may have responsibility for the cost of repairs or replacement

LearnLink Office 365 is a customised package of Microsoft Office Word, Excel, Publisher, Powerpoint, Onedrive and Sharepoint available for students. This is offered at no additional charge to parents\guardians whilst their child remains at PASS.

To access further information on what Office 365 has to offer and the risks involved see the following link

<http://pass.sa.edu.au/docs/office-365.pdf>

What if I do not want my child(ren) to use the LearnLink Office 365 Services?

PASS requires written notification if you do not consent to your child(ren) using the additional LearnLink Office 365 Services. Please visit or email PASS on the following email address to advise. dl.0790.ictadmin@schools.sa.edu.au

Important terms:

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

'**Cyber bullying**' is bullying which 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 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, 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 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.