Digital Technology / Cyber Safety Guidelines
GLEN OSMOND PRIMARY SCHOOL

Dear Parent/Caregiver,

The measures to ensure the cyber-safety of Glen Osmond Primary School (GOPS) are based on our core values. To assist us to enhance learning through the safe use of Digital Technologies we are now asking you to read this document and discuss it with your child.

Rigorous cyber-safety practices are in place, which include Digital Technology User Agreements for staff and students, who have been involved in the development of the agreement. Child protection education, such as the Keeping Safe child protection curriculum, includes information about remaining safe when using new technologies and is provided to all students.

The computer network, Internet access facilities, computers and other Digital Technology equipment/devices bring great benefits to the teaching and learning programs at GOPS and to the effective operation of the school. Digital Technology 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.

The overall goal of GOPS is to create and maintain a cyber-safety culture that is in keeping with our values and with legislative and professional obligations. The Digital Technology /Cyber Safety Guidelines include information about your obligations, responsibilities, and the nature of possible consequences associated with cyber-safety breaches that undermine the safety of the school environment.

All students will be made aware of the expectations of the Digital Technology / Cyber Safety Guidelines through discussion with their teacher.

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.

While every reasonable effort is made by schools and DfE administrators to prevent children'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. DfE recommends the use of appropriate Internet filtering software.

More information about Internet filtering can be found on the websites of the Australian Communications and Media Authority at http://www.acma.gov.au , NetAlert at http://www.netalert.gov.au , the Kids Helpline at http://www.kidshelp.com.au and Bullying No Way at http://www.bullyingnoway.com.au

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

Important terms:

'Cyber-safety' refers to the safe use of the Internet and Digital Technology 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 and preschool Digital Technology' refers to the schools or preschool's computer network, Internet access facilities, computers, and other Digital Technology equipment/devices as outlined below.

'Digital Technology equipment/devices' includes computers (such as desktops and laptops), storage devices (such as USB), DVDs, iPads/iPods, MP3 players), cameras (such as video and digital cameras), 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.

Digital Technology/ Cyber Safety Guidelines

STUDENTS - CAREFULLY READ THESE POINTS WITH YOUR PARENTS / CAREGIVERS

Keep this page for reference and future discussion

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

1. I will not use school Digital Technology equipment until my parents/caregivers and I have read and agreed to the Digital Technology / Cyber Safety Guidelines.

2. I will use the computers, iPads, USB, Digital Camera and other Digital Technology equipment only for learning purposes and I will not change and alter any settings on any Digital Technology device, without permission from a teacher.

3. I will go online or use the Internet at school only when a teacher gives permission and an adult is present on any Digital Technology device. If I am unsure whether I am allowed to do something involving Digital Technologies, I will ask the teacher first.

4. 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 and I will keep my password private.

5. I will use the Internet, e-mail, mobile phones or any Digital Technology 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. Misuse will be brought to the attention of the Principal for review of student's privileges. If the Mobile Phone is found in a student's possession during lesson time, the students will immediately lodge the phone at the Front Office and parents will be contacted. The student will be able to collect the phone at the end of the school day.

6. While at school, I will:

- attempt to search for things online that I know are acceptable at our school. This would exclude anything that is rude or violent or uses unacceptable language such as swearing
- and will report any attempt to get around, or bypass, security, monitoring and filtering that is in place at our school.

7. If I find anything that upsets me, is mean or rude, or that I know is not acceptable at our school, I will:

- **NOT** show others, turn off the screen and get a teacher straight away.

8. Any personal Digital Technology device I bring to school will be at my own risk, the school will take no liability for lost, stolen or damaged digital devices. It should not be used unless consent is given by the teacher. It should remain switched-off and in my school bag at all times. Use of these Digital Technologies is under the guidance of teachers at all times.

9. I will clearly label my school USB (8GB or less), it will only contain school files, no game software or more than 2 music files for school learning purposes.

10. The school cyber-safety strategies apply to any Digital Technology brought to school, and to ensure my compliance with copyright laws, I will download or copy any files such as music, videos, games or programs only with the permission of a teacher or the owner of the original material.

11. 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, address, e-mail address, phone numbers and photos of me and/or people close to me.

12. I will use LearnLink Office 365, tailored for the South Australian public education system, appropriately as directed by the school. LearnLink Office 365 provides students with an email and collaboration platform to create and/or upload/share content. This may include websites, presentations, written, audio, images and video material as part of their educational program. All data and information within LearnLink Office 365 is stored within an Australian based 'cloud'.

13. I will respect all school Digital Technology and will treat all Digital Technology equipment/devices with care. This includes:

- not intentionally disrupting the smooth running of any school Digital Technology 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 Digital Technologies.
- reporting any breakages/damage to a staff member.

14. If I do not follow expectations of digital technology use and cyber-safety practices, the school will inform my parents/caregivers, which may result in loss of use for a period of time. 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, the school will 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.

Digital Technology / Cyber Safety Guidelines

To the parents/caregivers

Please read this page carefully to check that you understand your responsibilities under these guidelines.

I understand that GOPS will:

- do its best to enhance learning through the safe use of Digital Technologies. This includes working to restrict access to inappropriate, illegal or harmful material on the Internet or on digital technology equipment/devices at school or at school-related activities
- work with children and their families to encourage and develop an understanding of the importance of cyber-safety through education designed to complement and support the Digital Technology / Cyber Safety Guidelines. This includes providing children with strategies to keep themselves safe in a connected online world
- respond to any breaches in an appropriate manner
- welcome enquiries at any time from parents/caregivers/legal guardians or children about cyber-safety issues.

My responsibilities include:

- discussing the information about cyber-safety with my child and explaining why it is important
- supporting the school's cyber-safety program by emphasising to my child the need to follow the cyber-safety strategies
- contacting the principal or nominee to discuss any questions I may have about cyber-safety and/or the Digital Technology / Cyber Safety Guidelines

---