



Oakbank Area School

154 Onkaparinga Valley Road
OAKBANK SA 5243

Phone: (08) 8398 7200 Facsimile: (08) 8388 4718 Email: dl.0762.info@schools.sa.edu.au
Website: www.oakbankas.sa.edu.au Facebook: <http://www.facebook.com/oakbankas>

Cybersafety / ICT Policy & Agreement

The overall goal of Oakbank Area School is to create and maintain a cyber-safety culture that is in keeping with our values and with legislative and professional obligations. The Cybersafety / ICT Use Agreement includes information about your obligations, responsibilities, and the nature of possible consequences associated with cyber-safety breaches that undermine the safety of the school environment.

Oakbank Area School places a high priority on providing its school community with internet facilities, ICT devices and equipment which will benefit student learning outcomes and the effective operation of the school.

All students and their parents/caregivers are required to sign the attached Cyber-safety/ 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 resources is on the understanding that your child will access applications and files in a safe and ethical way. Your child also needs to be aware that the school's wellbeing and behaviour management processes also extend to outside of school hours or off-site.

If a student who is enrolled at Oakbank Area School behaves online in a manner that threatens the wellbeing of another child, student, staff member, 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 Regulations pursuant to the Education Act 1972, to suspend or exclude the 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 or evidence of a crime, such as an assault, that 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 required.

Material sent and received using the Oakbank Area School network may be monitored and filtering and/or monitoring software may be used to restrict access to certain sites and data, including e-mail.

While every reasonable effort is made by schools, preschools and Department for Education (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 preschool], or on mobile devices owned by your child. DfE recommends the use of appropriate Internet filtering software.

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 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, 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.



Strategies to help keep Oakbank Area School Cyber-safe

Parents/caregivers play a critical role in developing knowledge, understanding and ethics around their child's safety and safe practices 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, I have signed my Cyber-safety/ ICT 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 and will not share my password with any other student.
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 computer, mobile phone or electronic device 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.
9. Whilst at school I will report any attempt by another student to get around or bypass security, monitoring and filtering that is in place at school.
10. If I accidentally access inappropriate material, I will not show others; I will turn off the screen or minimise the window and then report the incident to a teacher immediately.
11. 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.
12. 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 Cyber-safety/ ICT Use Agreement. Any images or material on such equipment/devices must be appropriate to the school environment.
13. Only with 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.
14. 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 and/or photos of me and/or people close to me.
15. I will use my Learnlink school email (or other email services accessed via the school network) for education purposes only, under teacher or ICT coordinator guidance.
16. I will treat all email as written notes. If I receive an email that makes me angry, upset or uncomfortable, I will immediately forward the email to my teacher and the ICT Coordinator. I must NOT DELETE IT, unless directed by the teacher or ICT Coordinator.
17. If I have access to Learnlink Office 365 services via my school email, including Office 365 Pro Plus (Word, Excel, Powerpoint, OneDrive etc.), I will only use them for education purposes only, and will not store sensitive or personal information.
18. I must leave a copy of all my present computer related school work in my home-drive at school.
19. I will not commit plagiarism (copy other people's work and then claim it as my own).
20. I will not commit piracy (using school equipment to illegally copy files and/or software including, but not limited to, music, video and/or pictures).
21. I acknowledge that I cannot use a consequence or breach of the rules as an excuse for not completing my school work.
22. I will only print educational related and/or school work related material.

J:\Common\Policies and Procedures\2019 Amended Policies\OAS Cybersafety ICT Policy Agreement 2018.doc



- 23.** I agree to pay for any printer usage above what I have initially been granted by the school.
- 24.** 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
 - not attempting to introduce files onto the network that are of a non-educational related matter.
 - 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
 - seeking help to fix a computer which is not working, BEFORE attempting to fix the problem myself.
 - Not vandalising or removing any ICT related equipment.
- 25.** 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.
- 26.** 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.
- 27.** 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.
- 28.** I acknowledge that the consequences for failing to follow the above rules may include but not be limited to:
- Internet lockout – (lockout is access removed from the user)
 - Email lockout.
 - Printer lockout.
 - Network (computer) lockout.
 - Completion of work without the assistance of the computer.
 - Student and/or parents being invoiced for repairs to equipment or resources used.
 - Suspension from ICT activities.
 - Suspension from school.
 - Failure to agree to the above rules will result in no access to any ICT related equipment in the school.

Lockout times can vary from, but not be limited to, 5 minutes to the remainder of the school year.

Oakbank Area School Cyber-Safety/ ICT Use Agreement Form

Parent/Caregiver/Legal Guardian:

Please read this page carefully to check that you understand your responsibilities under this agreement and return the signed Cyber-safety/ ICT Use Agreement to the Front Office.

I understand that Oakbank Area 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 Use 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 Cyber-safety/ ICT Use Agreement initiative.
- welcome enquiries at any time from parents/caregivers/legal guardians or students about cyber-safety issues.

For the Student: My responsibilities include...

- reading this Cyber-safety/ ICT Use Agreement carefully.
- following the cyber-safety strategies and instructions whenever I use the school's ICT equipment.
- 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 and others' ICT equipment. 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 relevant staff member if I am not sure about anything to do with this agreement.

We have read and understood this Cyber-safety/ICT Use Agreement and we are aware of the school's initiatives to maintain a cyber-safe learning environment.

Name of student: _____ Group/Class: _____

Signature of student: _____ Date: _____

For the Parent/Caregiver/Legal Guardian: My responsibilities include:

- reading this Cyber-safety/ICT Use Agreement carefully and discussing it with my child so we both have a clear understanding of the schools initiatives in maintaining the care, use and management of ICT equipment in a cyber-safe learning environment.
- Understanding that failure of my child to comply with this agreement may result in behaviour management processes being invoked.
- Understanding that any costs associated with repairs or replacement of ICT equipment while in the care and custody of my child may be borne by me the parent/caregiver.
- ensuring this Use 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.

Name of parent/caregiver/legal guardian: _____

Signature of parent/caregiver/legal guardian: _____

Date: _____

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.

PLEASE RETURN THIS SECTION TO SCHOOL AND KEEP A COPY FOR YOUR OWN REFERENCE.

Authorised by: School Council, Principal
Date of Review: January 2018

Review due: January 2020

