COMPTON PRIMARY SCHOOL

Government of South Australia
Department for Education and Child Development

Cyber-Safety Policy and User Agreement

Cyber Safety encompasses technology such as the Internet and electronic communication devices including mobile phones, iPads, laptops, iPhones and other wireless technology. It is important to both protect and teach children while they learn to use ICTs and become responsible digital citizens. This includes adults thinking ahead of new risks and children learning how to avoid exposure to inappropriate material or activities, and protecting themselves online. Children need to learn how to use ICTs, including mobile technologies and social networking sites, in responsible and ethical ways. In addition, they need to feel confident about alerting the adults in their lives when they are feeling unsafe, threatened, bullied or exposed to inappropriate events.

It is a Department for Education requirement that schools have in place a Cyber-Safety User Agreement in the form of a written agreement, signed by parents and students (or for younger students, parents only). Therefore, to assist us to enhance learning through the safe use of information and communication technologies (ICTs), we are now asking you to read this document and sign the attached User Agreement Form.

The computer network, Internet access facilities, computers, iPads and other ICT equipment/devices bring great benefits to the teaching and learning programs at Compton Primary School, and to the effective operation of the school. The overall goal of our school is to create and maintain a cyber-safety culture that is in keeping with our values and with legislative and professional obligations.

Steps we take at school to promote cyber-safety.

- Teach strategies for personal safety and advise students that they should not reveal personal or identifying information (e.g. passwords, names, images, telephone numbers)
- Teach topics and use resources contained in the Keeping Safe: Child Protection Curriculum.
- Encourage students to inform the teacher if they come across inappropriate material or anything online that makes them feel uncomfortable.
- Use of a filtered service when accessing the internet. All access is through the Department of Education service which is designed to filter out inappropriate material. Also, 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.

While every reasonable effort is made by schools, preschools and Department of Education 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, DECD cannot filter Internet content accessed by your child from home, from other locations away from school or on mobile devices owned by your child. The Department of Education recommends the use of appropriate Internet filtering software.

Cyber bullying

Cyber bullying is repeated harassment through the use of communication technology and can occur in many forms. Some common examples include:

- Text messages that are threatening or cause discomfort.
- Picture/video/audio clips sent to make the victim feel embarrassed or threatened.
- Phone calls that are abusive or using someone else's phone to harass others.
- Email/chat room/social network sites that are used to cause discomfort, embarrassment or harm.

Handling of cyber-safety complaints.

- Prompt action will be taken if a complaint is made, including establishing the facts of the situation.
- Appropriate sanctions will align with the school's behaviour policy, and in more serious situations, the police will be contacted.

CANBERRA CAMP (Yr 6/7 students)

Mobile phones and iPad are allowed to be brought on camp but **must** have internet access disabled for the entire duration of the trip. Content on these devices needs to be screened by parents and students prior to camp so that any inappropriate material is removed (eg: song lyrics, images, movie content). During camp, if a device is discovered to have inappropriate material or internet access, then it will be confiscated and parents notified. If you seek any further clarification about this matter please speak to your child's class teacher or principal.

Important terms:

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

'Cyber bullying' is repeated harassment 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.

'ICT equipment/devices' includes computers (such as desktops, laptops, iPads), 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 or preschool environment.

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

Cyber-safety User Agreement

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. The User 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.

For students:

1. I will use the computers and other ICT equipment only for my learning and only with my teacher's permission.
2. I will go online or use the Internet at school only when a teacher gives permission and if there is something I'm not sure about, I will ask my teacher.
3. I will use the Internet, e-mail, and any other ICT equipment only for positive purposes. Therefore, I will not be mean, rude or unkind to or about other people. I will comply with copyright laws and only download material with permission of my teacher.
4. I will keep my password private.
5. 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
    - get a teacher straight away.
6. Mobile phones and other ICT devices are not to be brought to school unless the Mobile Phone and ICT Agreement Policies have been read, discussed and signed and there is a suitable reason as to why the equipment need to be at school. This includes things like mobile phones, iPods, iPads, games, cameras, and USB/portable drives.
7. I will be careful and will look after all our school ICT equipment by:
    - not disrupting existing school ICT systems.
    - following our school cyber-safety strategies.
    - telling a teacher about anything wrong or damaged.
    - 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 photos of me and/or people close to me.
8. If I'm not cyber-safe, the school will inform my parents/caregivers and there may be consequences associated with my behaviour. In serious cases, the school may take disciplinary action against me. If illegal activities are involved or e-crime is suspected, it will be necessary for the school to inform the police and hold personal items for potential police examination.

For Parents:

Please read this page carefully to check that you understand your responsibilities under this agreement.
I understand that Compton Primary 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 ICT 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 Use Agreement initiative. 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 this Use Agreement.

COMPTON PRIMARY SCHOOL - CYBER-SAFETY USER AGREEMENT

We have read and understood this Cyber-Safety User Agreement and I am aware of the school's initiatives to maintain a cyber-safe learning environment.

Student to write or sign name here: _____

Name of parent/caregiver: _____

Signature of parent/caregiver: _____ 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.