CYBER-SAFETY AT RICHMOND PRIMARY SCHOOL

Dear Parent/Caregiver,

The measures to ensure the cyber-safety of Richmond Primary School are based on our core values. To assist us to enhance learning through the safe use of information and communication technologies (ICTs), we are now asking you to please read this document and sign the attached Use Agreement Form for every child in your family who attends this school.

Rigorous cyber-safety practices are in place, which include Cyber-Safety Use Agreements for staff and students. 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 ICT equipment/devices bring great benefits to the teaching and learning programs at Richmond Primary 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.

The overall goal of Richmond Primary School is to create and maintain a "Cyber-Safety Culture" that is in keeping with our values and with legislative and professional obligations. The 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.

Bullying has taken on a new dimension with the introduction of new forms of electrobnic communication. Cyber bullying can be perpetrated at any time of the day or week. This behaviour can threaten the safety or wellbeing of others.

Under regulations 40 and 41 of the Education Regulations 1997, principals can suspend or exclude a student who acts in a manner that threatens the safety or wellbeing of a student or member of staff, or another person associated with the school. These regulations do not preclude an event that occurs outside of school hours or off site. Principals can therefore use these procedures with a student enrolled at their school if the principal believes, on reasonable grounds, that the student has acted in such a manner, even if this behaviour occurred outside of school hours or off site.

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

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 DECD 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. DECD 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 ICT equipment/devices.

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.

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 and I have signed my Use Agreement Form and the completed form has been returned to school.

2. I will use the computers and other ICT equipment only for my learning.

3. I will go online or use the Internet at school only when a teacher gives permission and an adult is present.

4. If I am unsure whether I am allowed to do something involving ICT, I will ask the teacher first.

5. 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.

6. I will keep my password private.

7. 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.

8. 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.
   - report any attempt to get around, or bypass, security, monitoring and filtering that is in place at our school.

9. 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.

10. Only with written permission from home and the school will I bring any ICT equipment/devices to school. This includes things like mobile phones, iPods, games, cameras, and USB/portable drives. I understand these devices are NOT to be used during school hours and are to be handed into the front office at the beginning of the school day and collected at home time.

11. 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.

12. The school cyber-safety strategies apply to any ICTs brought to school.

13. 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.

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
   - photos of me and/or people close to me.

'Learning & caring for Life'

15. 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.

16. If I do not follow cyber-safety 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.