Dear Parent/Caregiver,

The measures to ensure the cyber-safety of Coromandel Valley 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 read this document and discuss with your child/ren.

Rigorous cybersafety practices are in place, which include cybersafety user agreements for staff and learners. 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 learners.

The computer network, Internet access facilities, computers mobile devices and other ICT equipment bring great benefits to the teaching and learning programs at CVPS, 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 Coromandel Valley 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 user agreement includes information about user obligations, responsibilities, and the nature of possible consequences associated with cyber-safety breaches that undermine the safety of the school environment.

All students are required to accept the terms of the user agreement each time they use a computer or device. 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 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 and cybersafety can be found on the following websites:

- Officer of the Children’s e-Safety Commissioner https://www.esafety.gov.au
- Bullying No Way http://www.bullyingnoway.com.au
- Information about Internet security can be found at NetAlert http://www.netalert.net.au/
Social Media

Social media refers to a range of online services and tools used for publishing, sharing and promoting interaction and dialogues. Many services and sites such as Snapchat, Facebook and Instagram require a person to over a certain age before they can be used. For example, Snapchat age is 13. It is the school's aim to maintain a safe learning environment. Students therefore, may not use any school or BYOD electronic equipment to subscribe to or access any social media site within school hours and while on the school site, unless it is a part of the teacher’s learning program and prior permission has been given by the teacher.

Social media is a useful learning tool. For example, iTunes U, Weebly, Edmodo and SeeSaw all have interactive capabilities through blogs. These can be locked down from public access with password protection and managed as age appropriate. The school is currently developing a social media policy using DECD social media guidelines. The parent ICT committee will be involved in this development.

Other 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.

Please contact the principal, if you have any concerns about your child's safety in using the Internet and ICT equipment/device.
Strategies to help keep Coromandel Valley Primary School Students Cyber-safe
Middle and Upper Years 3-7

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 unless I agree during the computer login process that I will abide by the user agreement.
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. I will follow the school's electronic device policy. This includes things like mobile phones, iPods, games, cameras, and USB/portable drives.
11. 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.
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.
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 a 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.
To the parent/ caregiver/ legal guardian -
Please read this page carefully to check that you understand your responsibilities under this agreement. Return the signed user agreement to the school.

I understand that Coromandel Valley Primary School will...
- do its best to enhance the 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 user 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 any enquiries at any time from parents/ caregivers/ legal guardians or children about cyber-safety issues.

For the student – my responsibilities include...
- reading this cyber-safety agreement carefully
- following the cyber-safety strategies whenever I use privately – owned ICT devices on the school site or at any school related activity, regardless of it’s location
- asking the teacher if I am not sure about anything to do with this agreement

For the parent/ carer/ legal guardian – my responsibilities include...
- discussing the information about cybersafety 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 to discuss any questions I may have about cyber-safety and/or this user agreement.

Coromandel Valley Primary School Cyber-safety User Agreement

I have read and understood this cyber-safety user agreement and am aware of the school’s initiatives to maintain a cybersafe learning environment.

Name of child……………………………………………………………………………… Class………………

Signature of student……………………………………………………………………… Date………………..

Name of parent/caregiver/legal guardian…………………………………………………………

Signature of parent/caregiver/legal guardian………………………………………… Date………………..

Please note – this agreement will remain 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.