CYBER SAFETY POLICY

PURPOSE: The measures to ensure the cyber-safety of McLaren Vale Primary School students and staff are based on our core values of respect, integrity and success. To assist us to enhance learning through the safe use of digital and communication technologies, we are now asking you to read this document and sign the attached User Agreement Form.

TEACHING ABOUT CYBER SAFETY: Rigorous cyber-safety practices are in place, which include cyber-safety User Agreements for students. The Child Protection Curriculum includes information about remaining safe when using technologies and is provided to all students. Our Year 5 and 6 students participate in a cyber-safety session with the Carly Ryan Foundation learning about the dangers of online platforms and strategies for keeping themselves safe online and reporting problems faced online.

OUR NETWORK: The computer network, Internet access facilities, computers and other equipment and devices bring great benefits to the teaching and learning programs at McLaren Vale Primary School. The digital technology equipment is for educational purposes appropriate to this environment.

The overall goal of McLaren Vale Primary School is to create and maintain a cyber-safe culture that is in keeping with our values and with legislative and professional obligations. The User Agreement includes information about obligations, responsibilities, and the nature of possible consequences associated with cyber-safety breaches that undermine the safety of the school environment.

Material sent and received using the network may be monitored using filtering and/or monitoring software. This may be used to restrict access to certain sites and data, including email. 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.

FILTERING SYSTEMS: 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. Our school uses the SWiFT online filtering and reporting system. This provides the school with detailed reports about content accessed by students and immediate alerts are flagged when something potentially harmful or inappropriate is accessed. The Leadership Team will decide on the next step in following this up and any further consequences.

MORE INFORMATION: Internet filtering information 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.
- The Carly Ryan Foundation https://www.carlyryanfoundation.com/

Please contact the school's leadership team if you have any concerns about your child's safety in using the internet and digital equipment or devices.

Important terms:
'Cyber-safety' refers to the safe use of the Internet and digital equipment or 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 digital equipment or devices as outlined below.
'Digital equipment or 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)

Policy reviewed June 2023