



CYBER BULLYING POLICY

Overview

Measures to ensure the cyber-safety of Melrose Primary School are based on our core values and through our vision being:

Melrose Primary School empowers students to excel in learning and in life. We nurture relationships that challenge and support students to contribute to a more just and compassionate world.

Melrose Primary School is all about our children. We create and uphold a nurturing environment for our children, families, teachers, volunteers, and the wider community. We are a small rural school of educators and learners who strive for excellence in education, and we are innovative and collaborative in our approach. We aim to maintain a sense of belonging for all our children encouraging them to reach their full potential.

To assist us to enhance learning through the safe use of information and communication technologies (ICTs), all parents/caregivers are asked to read and support the following document and have their child/ren sign the Use Agreement Form distributed to all students at the beginning of every school year.

Use Agreement and Practices

Rigorous cyber-safety practices are in place at our school, which include cyber-safety Use Agreements for students. Child protection education, such as the Keeping Safe Child Protection curriculum also includes information about remaining safe when using new technologies and is provided to students.

The computer network, Internet access facilities, computers and other ICT equipment/devices bring great benefits to the teaching and learning programs at Melrose Primary School, and to the effective operation of the school.

Within this area the overall goal of Melrose Primary School is to create and maintain a cyber-safety culture that is in keeping with school values and within legislative and professional obligations. The Use Agreement includes information about individual obligations, responsibilities, and the nature of possible consequences associated with cyber-safety breaches that undermine the safety of the school environment. All students will be issued annually with a Use Agreement and once signed consent has been returned to school, students will be able to use the school ICT equipment.

Monitoring and Filtering

Material sent and received using the school network may be monitored and filtered 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 DfE administrators to prevent exposure of children to inappropriate content when using departmental online services, it is not possible to completely eliminate the risk of such exposure.

In particular, DfE cannot filter Internet content accessed by a child from home, from other locations away from school or on mobile devices owned by a child.

DfE recommends the use of appropriate Internet filtering software on all devices. More information about Internet filtering can be found on the following websites:

Australian Communications and Media Authority <http://www.acma.gov.au>

Net Alert <http://www.netalert.gov.au>

Kids Helpline <http://www.kidshelp.com.au>

Bullying No Way <http://www.bullyingnoway.com.au>

For further information or to discuss any concerns or queries regarding cyber safety or using the Internet and ICT equipment/devices, please contact the Principal.

Strategies to keep Melrose Primary 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 Melrose Primary School invites all parents/caregivers to discuss with their child the following strategies to help stay safe when using ICT at school and after formal school hours.

- Not using school ICT equipment until the Use Agreement Form has been completed and returned to school
- Only using the computers and other ICT equipment for learning
- Only going online or using the Internet at school when a teacher gives permission and an adult is present
- Always asking a teacher first if unsure whether allowed to do something involving ICT
- Only using their own username and not allowing anyone else to use that user name
- Keeping all passwords private
- Only using the Internet, e-mail, mobile phones or any ICT equipment for positive purposes
- Not being mean, rude or offensive, bullying or harassing, or in any way harming anyone else, or the school itself, even if it is meant as a joke
- While at school only attempting to search for things online that are known to be acceptable at school. This excludes anything that is rude or violent or uses unacceptable language such as swearing, and reporting any attempt to get around, or bypass, security, monitoring and filtering that is in place at the school
- Following the three steps below if anything is found that is upsetting, is mean or rude, or that is known to be unacceptable at school:
 - not showing or sharing with others
 - turning off the screen
 - getting a teacher straight away
- Only connecting an ICT device to school ICT technologies, or running software (e.g. USB/portable drive, camera or phone) with permission from the teacher. This includes all wireless/Bluetooth technologies
- Only using charging devices that have been electrically tested and certified by the school
- Complying with the school cyber-safety strategies for any ICTs brought to school
- Only downloading or copying files such as music, videos, games or programs with the permission of a teacher or owner of the original material to ensure compliance with copyright laws

- Always asking a teacher’s permission before putting personal information online, which includes any of the following:
 - full name
 - address
 - e-mail address
 - phone numbers
 - photos
- Respecting and treating all school ICT equipment/devices with care, including:
 - 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 teacher straight away.

Breaches

If a student or students do not follow cyber-safety practices, the school may inform parents/caregivers, and in serious cases, may take disciplinary action against the student(s). Families may also be charged for any damage or repair costs where applicable. 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 personal items securely for potential examination by police. Such actions may occur even if the incident occurs off-site and/or out of school hours.

Responsibilities

Melrose 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. This includes providing children with strategies to keep themselves safe in a connected online world
- respond to any breaches in an appropriate and timely manner
- welcome enquiries at any time from parents/caregivers/legal guardians or children about cyber-safety issues.

Parents/Caregivers are expected to:

- discuss information about cyber-safety with their child and explain why it is important
- support the school’s cyber-safety program by emphasising to their child the need to follow cyber-safety strategies and sign the Cyber Safety Use Agreement
- contact the principal or a teacher to discuss any questions or concerns they may have about cyber-safety and/or the Cyber Safety Use Agreement.

Glossary

Cyber-safety - the safe use of the Internet and ICT equipment/devices, including mobile phones.

Cyber bullying - bullying which uses e-technology as a means of victimising others. It is the use of an Internet service or mobile technology - such as e-mail, chat room discussion groups, instant messaging, webpages or SMS (text messaging) - with the intention of harming another person.

School ICT - the school'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 (e.g. USB and flash memory devices, CDs, DVDs), 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 - 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 environment.

E-crime - when computers or other electronic communication equipment/devices (e.g. Internet, mobile phones) are used to commit an offence, are targeted in an offence, or act as storage devices in an offence.

Tabled 19/3/19

Ratified 19/3/19

To be reviewed March 2021