

CYBER-SAFETY AT NORWOOD PRIMARY SCHOOL – Reception to Year 2

The measures to ensure the cyber-safety of Norwood Primary School are based on our core values. Rigorous cyber-safety practices are in place, which include cyber-safety Use Agreements for staff and learners, who have been involved in the development of the agreement. 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 and other digital technology equipment/devices bring great benefits to the teaching and learning programs at Norwood Primary School, and to the effective operation of the school. The digital technology 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 Norwood 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.

All learners will be issued with a Use Agreement and once signed consent has been returned to school, learners will be able to use the school digital technology 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.

While every reasonable effort is made by schools, preschools 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.

More information about Internet filtering can be found on the websites of the Australian Communications and Media Authority at <http://www.acma.gov.au>, the Kids Helpline at <http://www.kidshelp.com.au> and Bullying No Way at <http://www.bullyingnoway.gov.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.

'Digital Technology 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 digital technologies at school and after formal school hours.

1. Students will use school digital technology equipment only when parents/caregivers have signed their child's Use Agreement form and the completed form has been returned to school.
2. Students will use the computers and other digital technology equipment only for learning and only with teacher's permission.
3. Students will go online or use the internet at school only when a teacher gives permission and an adult is present.
4. If there is something a student is not sure about, they will ask their teacher.
5. Students will use the internet, e-mail, mobile phones and any other digital technology equipment only for positive purposes. Students will not be mean, rude or unkind to or about other people.
6. Students will keep their password private.
7. If students find anything that upsets them, is mean or rude, or that they know is not acceptable at our school, they will:
 - not show others
 - turn off the screen
 - get a teacher straight away.
8. Students will ask their teacher's permission before they put any personal information online. Personal identifying information includes any of the following:
 - full name
 - address
 - e-mail address
 - phone numbers
 - photos of them and/or people close to them.
9. Students will be careful and will look after all our school digital technology equipment by:
 - not being silly and playing around with it
 - following our school cyber-safety strategies
 - telling a teacher about anything wrong or damaged.
10. If students are not cyber-safe, the school may need to inform parents/caregivers and there may be consequences associated with their behaviour.

Norwood Primary School will:

- do its best to enhance learning through the safe use of digital technologies. This includes working to restrict access to inappropriate, illegal or harmful material on the Internet or on digital technology 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.

Parent 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.

Cyber Safety Curriculum taught as part of the Australian Curriculum:

R-2	3-5	6-9
Online safety	3.1 Media classifications 3.2 Video media and computer games 3.3 Television programs 3.4 Internet 3.5 Photographs and digital images 3.6 Magazines	3.1 Being aware on the internet 3.2 Online abuse 3.3 Abuse using mobile phones 3.4 Sexting 3.5 Developing a cyber safety fact sheet 3.6 Cyber safety and the law