MORPHETT VALE PRIMARY SCHOOL

Cyber Safety Policy

ACCESS AND SECURITY

At Morphett vale Primary School we have age appropriate Cyber-safety Use Agreements for all children and students. The age-appropriate agreement must be agreed to and signed by the child/student and his/her parents at the beginning of each calendar year and at time of enrolment.

• Children and students must use the Internet in a safe and considerate manner.
• Children and students must follow the copyright and licensing laws with respect to software, information and other material retrieved from or published on the Internet.
• Children, students and staff will be made aware of the importance of ICT security and safety, and how to properly react and deal with ICT security incidents and weaknesses.
• Our school will report to SAPOL any cyber behaviour, suspected to be an e-crime. The principal will also forward a Critical Incident Form to the regional director.
• Educators will make a mandatory notification to the Child Abuse Report Line (13 1478) if they suspect child abuse or neglect.

Principal Responsibility:
To approve the posting of any information to Internet web pages, news groups, web-based forums etc. and ensure it conforms to minimum standards
• ensure that private information is not accessible on any publicly available web page. This includes the requirement that images should never include any names identifying any of the children/students in images
• gain written permission from parents before publishing video, photographs, comments or work samples of their child
• report to SAPOL any incident suspected to be an e-crime and provide to the investigating officer confiscated evidence.
• support staff members in making a mandatory notification if they suspect child abuse and/or neglect
• ensure that a developmentally appropriate child protection curriculum is being made available to every learner every year.

Educator Responsibility:
To observe a duty of care - this means they will take reasonable care to protect children and students from foreseeable risk of injury when using DECS online services
• provide appropriate supervision for children and students so that they comply with the practices designed for their own safety and that of others
• design and implement appropriate programs and procedures to ensure the safety of children and students

• teach children and students about dangerous situations, materials and practices
• fulfil their responsibilities to deliver child protection curriculum within whole of site planning for such delivery
• must make a mandatory notification to the Child Abuse Report Line if child abuse or neglect is suspected.

USER IDENTIFICATION AND PASSWORDS

To log on, children and students must use a unique user identification (user-ID) that is protected by a secure password.
• Passwords must be kept confidential and not displayed or written down in any form.
• Passwords must not be words found in a dictionary, or based on anything somebody else could easily guess or obtain using person-related information.
• Passwords must not be included in log-on scripts or other automated log-on processes.
• Children and students must not disclose their personal passwords to any other person. Where other users are authorised to use group user-IDs, the password must not be disclosed to unauthorised people.
• Children and students will be accountable for any inappropriate actions (eg bullying, accessing or sending inappropriate material) undertaken by someone using their personal user-ID.

APPROPRIATE BEHAVIOUR AND USE

Children and students may use the Internet only for learning related activities that are approved by a teacher. They must not cause interference or disruption to other people or equipment, and children may not access or distribute inappropriate material. This includes:
• distributing spam messages or chain letters
• accessing or distributing malicious, offensive or harassing material, including jokes and images
• bullying, harassing, defaming or giving offence to other people
• spreading any form of malicious software (eg viruses, worms)
• accessing files, information systems, communications, devices or resources without permission
• using for personal financial gain
• using non-approved file sharing technologies (eg Torrent)
• using for non-educational related streaming audio or video
• using for religious or political lobbying
• downloading or sharing non-educational material.

All children and students must have annual access to developmentally appropriate child protection curriculum.

MORPHETT VALE PRIMARY SCHOOL

Cyber Safety Policy

CYBER SAFE USE AGREEMENT

DECS ICT Security policy and the DECS Standard - Acceptable Use Policies for Schools, Preschools and Children's Services Sites contain the following main provisions regarding acceptable use policies and agreements.

• Cyber-safety Use Agreements must be in place for all children and students who use DECS online services.

• Policies must be implemented in the form of written agreements, signed by staff and children/students and/or their parents.

• Agreements may be modified by the school or preschool but they must outline the key terms and conditions of use of DECS online services, online behaviour and access privileges, and the consequences of non-compliance.

• These agreements must be reviewed and updated regularly to ensure their appropriateness and effectiveness.