Principal: Marie Wright **Student Wellbeing Leader:** Victoria Corbett
Coordinator Pedagogy and Practice: Joshua MacWilliams **Coordinator Behaviour Practitioner:** Dana Lauck

CYBER SAFETY POLICY

Policy Reviewed: Term 3, 2017 (Document Updated: Term 1 2022)

Introduction

Learning is a social activity. ICTs provide children and students with new and engaging ways to learn. ICTs expand social and knowledge networks so that children and students access current information, interact with experts and participate in peer teaching and learning. Using ICTs they can publish their learning, as evidence of achievement or to invite feedback for improvement.

It is important to both protect and teach children, students and adults, while they learn to use ICTs and become responsible digital citizens.

Our Cyber-Safety policy is supported by our Behaviour Management Policy and also complements the teaching and learning topics and resources available in the Keeping Safe: Child Protection Curriculum.

Overview

Port Noarlunga Primary School makes every reasonable effort to achieve a safe, engaging and effective cyber-safe learning environment by:

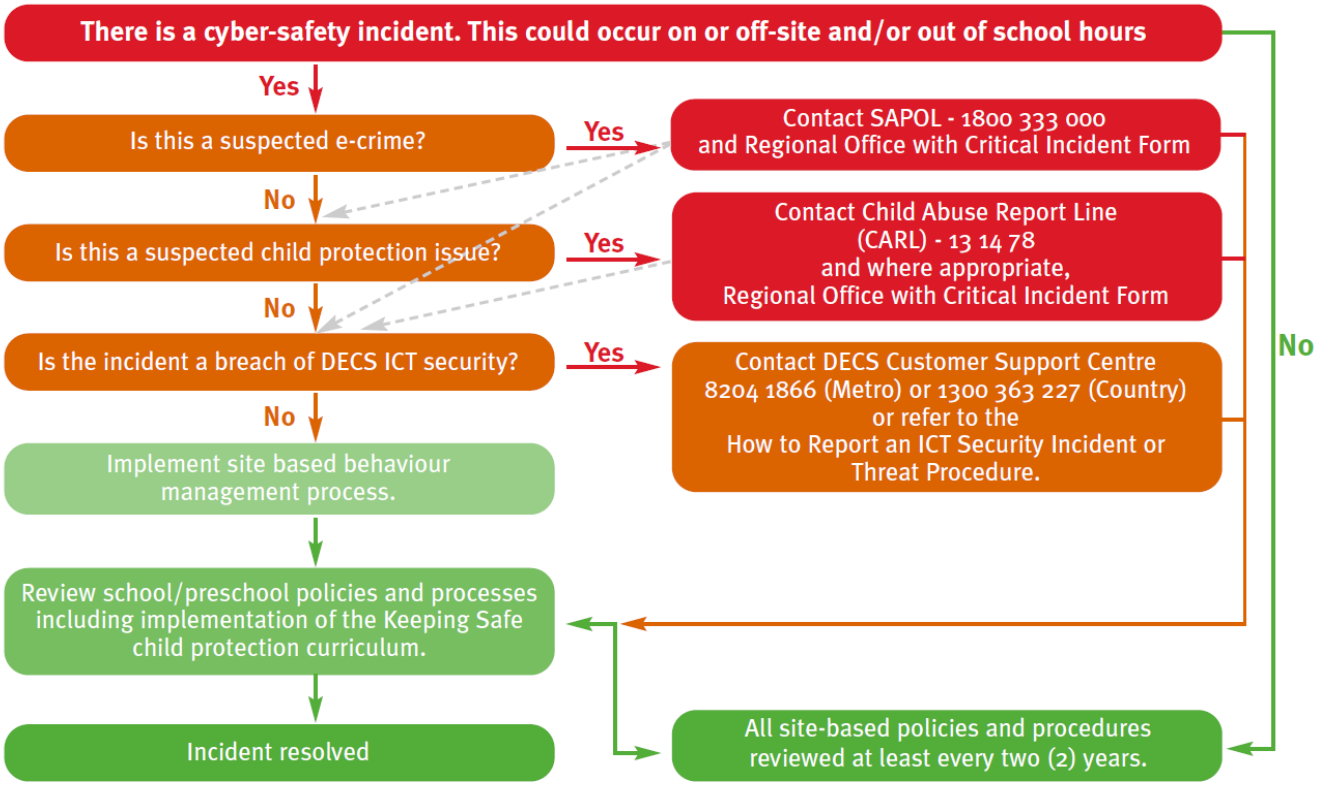
- developing programmes to educate and inform children, students and parents about the opportunities and challenges of ICTs in learning programs
- monitoring and logging e-mail traffic and Internet use, and providing filters to help guard against access to inappropriate materials
- providing direction and advice about ICTs (including the Internet and mobile phones) use and misuse, such as bullying and e-crime
- supporting police officers in undertaking an investigation and the collection of evidence following a principal or director reporting a suspected e-crime.

In matters relating to cyber-safety, PNPS works with, and is advised by:

- the 'Keeping Safe: Child Protection Curriculum'
- the Responding to Abuse and Neglect Training program (previously Mandatory Notification Training)
- the Australian Communications and Media Authority (ACMA), which manages a national cyber-safety education and awareness programme.
- South Australia Police (SAPOL)

Incident Response
The flow chart indicates the procedures followed by the school should a cyber-safety incident occur.

This document has been taken from the DECD 'Cyber-Safety: Keeping Children Safe in a Connected World'. The document is slightly outdated and is currently under review. We will monitor for updated content.



Mobile Phones
Students:

- Mobile phones are brought to school at entirely the owner's risk. The school will not be involved in disputes and/or investigations over damage, loss or theft.
- Phones must be handed to the class teacher during the school day.
- Phones are not to be taken on excursions or camps.
- Students breaching the policy will be subject to the normal student behaviour management consequences. The student will be instructed to pass the phone to the leadership team for the rest of the day
- If procedures continue to not be followed, the phone will be confiscated from the student and the parent will be asked to collect the phone from the leadership team.

Staff:

- Personal mobile phones are brought to school at the owner's risk.
- Personal mobile phones are to be switched to mute or discrete during class teaching and learning periods and during scheduled school meetings.

DECD Policy-Informed Practices

- Cyber-safety Use Agreements are in place for all children and students.
- Students must use the Internet in a safe and considerate manner.
- Students must follow the copyright and licensing laws with respect to software, information and other
- material retrieved from, or published on, the Internet.
- Students and staff are aware of the importance of ICT security and safety, and how to properly react and deal with ICT security incidents and weaknesses.
- Staff members must report to SAPOL if cyber behaviour is suspected to be an e-crime. A critical Incident report must be made.
- Staff members must make a mandatory notification to the Child Abuse Report Line (13 1478) if they suspect child abuse and/or neglect.

Leadership Responsibilities

- 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. The following steps should be followed
  • Ensure the confiscated evidence is placed in a secure location
  • Do not open and view any evidence on an electronic device as this will compromise the evidence
  • Cease any further investigation
  • Complete a Critical Incident Report
  • 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.

Teacher Responsibilities

- observe a duty of care - this means they will take reasonable care to protect students from foreseeable risk of injury when using DECD online services
- provide appropriate supervision for 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 students
- teach 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, 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.
- 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.
- Students will be accountable for any inappropriate actions (e.g. bullying, accessing or sending inappropriate material) undertaken by someone using their personal user-ID.

Appropriate Behaviour and Use

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 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 (e.g. viruses, worms)
- accessing files, information systems, communications, devices or resources without permission
- using for personal financial gain
- using non-approved file sharing technologies
- 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.