Sandy Creek Primary School

Cyber-safety Policy

Current as of: **February 2018**
To be Reviewed: **February 2021**

(This policy is based on DECD policies and guidelines and also Sheidow Park Primary School's Policy)

Core Beliefs	'It is important to both protect and teach children, students and adults, while they learn to use ICTs and become responsible digital citizens. This includes adults thinking ahead of new risks and children and students learn how to avoid exposure to inappropriate material or activities, and protecting themselves when they are online. They need to learn how to use ICTs, including mobile technologies and social networking sites, in responsible and ethical ways. In addition, they need to feel confident about alerting the adults in their lives when they are feeling unsafe, threatened, bullied or exposed to inappropriate events. In response, these adults need to take appropriate actions to protect the child or young person.' (DECD Cyber-Safety Guidelines) Bullying is when someone, or a group of people, upset or create a risk to another person's health and safety – either psychologically or physically – or their property, reputation or social acceptance on more than one occasion. People who bully deliberately set out to intimidate, exclude, threaten and/or hurt others repeatedly. Bullying is a clear form of harassment. People who use the internet, email, intranets, social media, phones or similar technologies to bully others are cyber bullying.
Access and Security	• Computer and Internet Use Agreements are in place for all students. The agreements are signed by the student and his/her parents. • All staff and students at Sandy Creek Primary School will abide by the Sandy Creek ICT Policy. • Students must use the Internet in a safe and considerate manner. • Staff and students must follow the copyright and licensing laws with respect to software, information and other material retrieved from or published on the Internet. • Cyber bullying which affects students, staff or volunteers within the school will be responded to by the school.
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 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 ○ using for non-educational related streaming audio or video ○ using for religious or political lobbying ○ downloading or sharing non-educational material. • All students will have annual access to developmentally appropriate child protection curriculum.
Responsibilities	The Principal will: • approve the posting of information to Internet web pages, news groups, web-

of the Principal	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 will be followed
	  o Ensure the confiscated evidence is placed in a secure location
	  o Do not open and view any evidence on an electronic device as this will compromise the evidence
	  o Cease any further investigation
	  o Complete and forward a Critical Incident online
	• 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.

Responsibilities of Educators	Educators will: • 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 • make a mandatory notification to the Child Abuse Report Line (131478) if child abuse or neglect is suspected. • teach strategies for personal safety and advise students that they should not reveal personal or identifying information including names, addresses, financial details (eg credit card), telephone numbers or images (video or photographic) of themselves or others • Teach all students how to respond in the event of cyber bullying or accidental access to inappropriate content or graphics in the school environment as part of an anti-bullying program delivered in all classes. • Reassure students that any reported cyber bullying will be followed up with action or reporting and that the cyber bullying will stop, making every effort to prevent retaliation from the perpetrator. • raise student awareness about courteous and appropriate use of ICT for personal and public communication • encourage students not to use their school e-mail address in non-school online communications as this e-mail address contains their personal name and school details • teach responsibilities associated to intellectual property and copyright law and ethics, including acknowledging the author or source of information that is used
Responsibilities of Students	Students will: • read, sign and follow the student Computer and Internet Use agreement • comply with the school ICT policy and this Cyber-safety policy • follow staff instructions at all times • inform staff of any inappropriate sites accessed or seen by minimising the screen and allowing the staff member to check the site and web address • use all ICT equipment with care and immediately inform a staff member of any issues with ICT use or equipment • If they are being cyber bullied, report it to a trusted adult who can take action to make it stop. • If cyber bullying occurs using email, texting, social media posts, etc. be sure to print or save any evidence.

	• Don't retaliate or respond to the cyber bullying. • Turn the screen off, but leave the computer/device on so that you can show it to an adult. • Keep telling trusted adults if the cyber bullying does not stop after you have reported it.
Responsibilities of Parents	Parents play a crucial role in the prevention of Cyber bullying because they have the capacity to monitor and educate students in the use of digital technologies. Parents also fund the use of digital technologies for students outside school hours and as such have a responsibility to monitor how these resources are being used, just as schools have the same responsibility for the use of school resources. This means limiting student access to age defined social media applications and websites used by their own children. Parents will: • Supervise the use of social media and internet websites directly (history checks, language filters, family filters, child passwords known), and indirectly (supervision, discussion, use in a public area of the house). • Restrict access to social media and internet sites to age appropriate sites. • Teach your child what to do in the event of cyber bullying or accidental access to inappropriate content or graphics. • Reassure your child that any reported cyber bullying will be followed up with action or reporting and that the cyber bullying will stop. • Record as many details as possible. *(Eg, what time, date, website, app, username, person details).* • If cyber bullying occurs using email, texting, social media posts, etc. be sure to print or save any evidence. • Consider carefully whether a generic response is warranted, such as; **'This message is from a trusted adult of the recipient. Your messages are considered offensive or inappropriate and will be forwarded to the relevant authorities for follow up'.** • Don't respond with any content that could be considered offensive or threatening. • Cyber bullying and sharing of inappropriate content is an e-crime. It is best managed by an authority that has authority to take action against the perpetrator. Such authorities include : S.A. Police, Managers of the social media app or website. • Where the cyber bullying impacts on the relationship or well-being of the child at school, the school should be notified. • The school has a mandated responsibility to report any legal concerns (S.A. Police matters, Child Protection matters) and causation factors (eg, age access to social media, adult involvement), to the relevant authorities (S.A. police, Child Abuse Report Line). • Keep the child informed about the action being taken on their behalf to prevent the cyber bullying from recurring. • Do not discuss, or encourage discussion about the matter publicly or with people not involved in the reporting process.