Hallett Cove South Primary School Cyber Safety Policy

Introduction

To create and maintain a cyber-safety culture that is in keeping with school values and with legislative and professional obligations. This policy is part of several inter related policies for the safety and wellbeing of students, parents, volunteers, visitors and any other members of our school community. This policy should be read in conjunction with the following:

- Behaviour Code of Conduct
- Bullying and Harassment Policy
- BYOD Policy
- ICT User Agreement
- Student Code of Conduct

At Hallett Cove South Primary School we believe:

- All people in our community have the right, to teach and learn in a supportive, caring and safe environment, without fear of being bullied.
- Every individual in school has a duty to report an incident of bullying whether it happens to themselves or to another person.
- Staff, as educators, has the responsibility to provide teaching and learning environments that enable students to develop the skills and attitudes that support self-management and positive behavioural choices.
- School is a place for students to further develop and practise their interaction and social skills in a safe and monitored environment.

Cyber Bullying

Cyber Bullying is a deliberate act towards an individual or group intended to cause harm with the intention to seriously embarrass, harass, threaten or humiliate. Cyber Bullying is a risk to people's health, safety and psychological wellbeing. Avenues for Cyber Bullying are: Internet service, email, chat room, discussion group, Facebook, instant messaging, mobile phone applications and technologies.
HCSPS does not tolerate any form of bullying and consequences exist for persons who choose to bully others.

Procedures in place

- Students are taught how to use technologies safely and know about the risks and consequences of misusing them.
- Students know what to do if they or someone they know are being cyber bullied
- Students, staff and parents/caregivers and legal guardians must read and sign our ICT user agreement
- Students and staff access websites, programs, training and guest speakers related to cyber safety
- Monitoring and filtering of the school network through the Department for Education-Technology & Knowledge Management Services
- The school will report to SAPOL if cyber behaviour is suspected to be an E-Crime

Responsibilities / Strategies

Parents/caregivers legal guardians and teachers all play a critical role in developing knowledge, understanding and ethics around student safety and the safe use of technology. It is recognised that students have access to ICT equipment out of school hours; incorrect use of personal equipment still has the potential to affect the wellbeing of other people and school. Any activity involving ICT use outside of school hours that affects in-school operation will be deemed to fall under the school's ICT agreement of use.
We invite all parents/caregivers and legal guardians to discuss with their child/children the following strategies to help them stay safe when using ICT both at home and at school.

- School ICT equipment may not be used until the ICT User Agreement Form has been completed and returned to school.
- Ask a teacher/adult if unsure whether to use ICT in a particular manor.
- Only logging in using the appropriate username given and not allowing anyone else to use that user name.
- All passwords must be kept private and not disclosed to other parties.
- Use of the Internet, e-mail, mobile phones or any ICT equipment for positive purposes only.
- Appropriate mannerism must be upheld while representing HCSPS. Conduct not allowed: being mean, rude or offensive, bullying, harassment, cause harm to anyone in any way, shape or form, even if it is meant as a joke.
- Always checking with an adult before entering personal details online, including but not limited to any of the following: name, address, e-mail address, phone numbers, photos, bank details and any other identifying information.

To support a positive and safe environment Hallett Cove South PS staff will:

- Enhance learning through the safe use of ICT, including working to restrict access to inappropriate, illegal or harmful material on the Internet or on ICT equipment/devices at school or school related activities.
- Promote responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of cyber-safety policy in both administration and curriculum, including secure school network design and use
- Safe and secure broadband including the effective management of content filtering.
- Respond to any breaches in an appropriate manner.
- Notify parents/caregivers and legal guardians if ICT equipment or services are used in any way that is found to be inappropriate or detrimental to persons or the physical environment.

Students will:

- Follow the ICT user agreement by using the internet and ICT in a safe and considerate manner.
- Only access the internet for learning purposes whilst at school.
- Only use social media websites that your parents have given approval for, and for which you meet the required age of use.
- Follow the copyright and licensing laws with respect to software, information and any other materials retrieved from or published on the internet.
- Only search for things online that are known to be acceptable, this excludes anything that is rude, violent or uses unacceptable language whilst at school
- Report any attempt to get around or bypass security, monitoring or filtering that is in place in the school.

Follow these steps if anything is found that is upsetting, mean or rude or that is known to be unacceptable at school.
- Not showing or sharing with others
- Turning off the screen and getting a teacher/adult straight away
- If you are being cyber bullied – report it to a trusted adult straight away, record details, screen shot it or save the evidence.
- Don't respond or retaliate to cyber bullying – inform an adult.
- Keep telling trusted adults if the cyber bullying continues after you have reported it.

Families/Caregivers Legal Guardians will:

- Be aware of the school ICT use agreement and other relevant policies
- Be supportive and encourage children to maintain the school values and the ICT user agreement
- Supervise the use of social media and internet websites directly (history checks, filters, passwords) and indirectly (supervision, discussion, use in public areas of home)
- Restrict access to social media and internet sites to age appropriate sites. Providing access to sites above the age of the child may constitute a breach of duty of care.
- 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.
- Record as many details as possible if cyber bullying occurs with screen shots, print outs, etc.
- Contact the school principal or teacher if they have any questions or concerns about cyber safety or cyber bullying.

Breaches:

If 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). This may result in restricted access to ICT or students being banned for a period of time.

If illegal materials or activities are involved or an e-crime is suspected, it may be necessary for the school to inform the police. The police can confiscate and search mobile devices.

Glossary of Terms:

BYOD - Bring Your Own Device Policy

Cyber Bullying - Bullying through information and communication technologies e.g. online chat, social media and social networking

Cyber Safety – Educating the safe use of the Internet and ICT equipment.

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.

HCSPS – Hallett Cove South Primary School

ICT – Information Communication Technology

ICT equipment / devices - includes computers such as desktops, laptops, chrome books and storage devices - USB's, portable hard drives, iPads and iPods. It also includes cameras – video and digital, webcams, all types of mobile phones, gaming consoles, TV, DVD and any other similar device

Inappropriate Material- is any content not related to learning or provided by the teacher. Examples of this include but are not limited to sex, cruelty, discrimination or violence in such a manner that it is likely to be injurious to the good of students or incompatible with a school or preschool environment.

School ICT - refers to the school's computer network, Internet access facilities, computers and other ICT equipment / devices as outlined below.

Review Date:
-