KEYNETON PRIMARY SCHOOL

CYBER-SAFE POLICY AND GUIDELINES

Policy

In accordance with the DfE ICT Security and Internet Access and Use policies, this policy contains the following main provisions:

Access and Security

- Cyber-safety *Internet and Email User Contract* must be in place for all students.
- Children and students must use the Internet in a safe and considerate manner.
- Children must follow the copyright and licensing laws with respect to software, information and other material retrieved from or published on the Internet.
- The school to ensure that 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.
- Schools must report to SAPOL if cyber behaviour is suspected to be an e-crime. The Principal must also forward a Critical Incident Form.

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 (eg Torrent)
    - using for non-educational related streaming audio or video
    - using for religious or political lobbying
    - downloading or sharing non-educational material
- All students must have annual access to developmentally appropriate child protection curriculum.

User Identification and Passwords

- Students must use a unique user identification (user-ID) that is protected by a secure password to log on.

- 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 student. 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 (eg bullying, accessing or sending inappropriate material).

Principal Requirements:

- Inform parents and staff of the existence of 'Cyber-Safety: Keeping Children Safe in a Connected World - Guidelines for Schools and Preschools'.

- Ensure signed consent is obtained from the parent/guardian before photographs of students are published on the school website. Separate consent forms will be required for other websites and social media eg: activities with Mid Murray Council, Planet Ark Tree Day. To avoid identifying children personally in photographs individual names will not be included unless specific permission is granted.

- Advise parents that, while DfE will make every reasonable effort to provide a safe and secure online learning experience for students when using DfE online services, Internet filtering is not 100 per cent effective and it is not possible to guarantee that students will not be exposed to inappropriate material.

- Inform parents that Internet browsing by their child at home or from other non-DfE sites will not occur via DfE online services and therefore will not be filtered or monitored by DfE.

- After highlighting learning opportunities and risks, gain written permission from parents before modifying Internet access safeguards, such as the Internet filtering, for targeted programs and projects.

- 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 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 and forward a Critical Incident Form.

- 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.

- Consider ways of maintaining confidentiality of child and students' passwords, with additional consideration given to younger children or those with special needs.

- Provide appropriate supervision for students using the Internet at school.

- Create and implement age appropriate *Internet and Email User Contract*s that:
    - Involve young people in the authorising of such an agreement and a commitment to personal and cyber-safe learning environments, for themselves and others regardless of age.

    - Are read, understood and signed by students and/or their parents.

    - Reinforce the fact that the agreement is taken seriously and is part of the partnership between school and home.

    - Clearly describe strategies for personal safety and privacy (eg students do not give out identifying information online, use only their first name, and not share their home address, telephone number or any other personal information).

    - Make clear that students should never respond to message or bulletin board items that are suggestive, obscene, belligerent, threatening or make them feel uncomfortable, and that these messages should be reported to a teacher.

    - Are signed by the parents, who agree to ensure their child is aware of personal safety strategies.

    - Students will take increasing responsibility for their own actions by agreeing to use DfE ICT facilities in a responsible manner, but with parents acknowledging on the agreement the responsibility for their child undertakes.

    - Are linked to the policies, goals and objectives of the school or preschool, particularly in relation to the purposes of providing ICT facilities and services.

    - Include the potential consequences of unacceptable use.

    - Are signed and a copy of the agreement is placed in the student's file for reference.

Educators' Requirements:

- Observe a duty of care – this means they will take reasonable care to protect students from foreseeable risk of injury when using DfE 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.

- 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.

- Encourage students not to use their school email addresses in non-school online communications as this email 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.

- Teach topics and use resources contained in the *Keeping Safe: Child Protection Curriculum*.

- Encourage students to inform a teacher if they come across inappropriate material or anything online that makes them uncomfortable.

- Teach strategies to manage online presence, protect identity through privacy settings, examine 'terms and conditions' associated with user agreements of Internet services and highlight the opportunities to report abuse or offensive online behaviour to the appropriate service provider or authority.

- Teach students (in an age-appropriate way) how to identify and avoid inappropriate materials. These can include:
    - Pornography – both illegal and legal pornography. It is prevalent on the Internet and can be accessed through websites, sent as spam via emails, shared in peer-to-peer networks or sexting through mobile phone messaging.

    - Hate groups – including racial, religious, political, homophobic and other groups that are discriminatory.

    - Violence or illicit drugs – websites containing explicitly violent behaviour (like rape or assault), material regarding illicit drugs or inciting suicide, vigilante or violent groups' websites, and instructional websites (like weapon or bomb making).

    - Illegal activity – content that promotes illegal activity (like copyright infringement on music), security breaches (like hacking) or fraudulent schemes online.

    - Extremist groups and cults – groups online that offer information about their extremist or cult activities, goals and missions; these groups can use the Internet to recruit new members or incite action.

    - Social networking – many social networking sites place students at some risk through exposing their identity, invading privacy and providing opportunities for bullying.

    - Online advertising – some online advertising can be inappropriate for children and students; the Internet is an inexpensive medium for advertisers and is therefore widespread.

    - Online gambling – websites which contain and promote gambling practices.

- Keep up to date about the relative risk and educational benefit of online activity in learning programs.

- Check that any material planned for publication on the Internet or intranet has the approval of the principal, as per the DfE ICT Security policy, and meets copyright and privacy requirements.

- Be aware of the steps to take and advice to give if students notify them of inappropriate or unwelcome activity online by other students or members of the public; such steps may include:
    - Collecting as much information as possible about the Internet, including copies of communications
    - Emphasising to the students that the event is not necessarily their fault
    - Identifying any risky behaviour on the part of the reporting student and counselling them on the need to adopt more protective behaviour
    - If the incident warrants further attention, escalating it to school and/or department authorities as per the DfE policies.

- Be involved in the development, approval and signing of a Cyber-safety Use Agreement which suits local needs and is consistent with the DfE Standard – Acceptable Use Policies for Schools, Preschools and Children's Services Sites and Code of Ethics for the South Australian Public Sector.

- Ensure that their 'digital footprints' from their personal online identities, including social networking sites, are consistent with the role of educators, the Code of Ethics for the South Australian Public Sector and the Teacher Registration Board of South Australia's Code of Ethics for the Teaching Profession in South Australia

The requirements and recommendations stated in this policy have come from the DfE Cyber-Safety: Keeping Children Safe in a Connected World – Guidelines for Schools and Preschools.

Ratified at Governing Council Meeting, Term 2, 2020

_____ _____

Principal Governing Council Chairperson

Term 2, 2020
Review Term 2, 2022