CYBER SAFETY AND DIGITAL DEVICES POLICY

Rationale:

Tea Tree Gully Primary School is committed to providing opportunities to enhance learning through the safe, responsible and ethical use of Information and Communication Technologies (ICTs). It is important to both protect and teach children while they learn to use ICTs and become responsible global citizens.

Important Terms:

'Cyber-safety' refers to the safe use of the Internet and digital devices.

'Cyber bullying' is bullying which uses e-technology as a means of victimising others. It is the use of an internet service or mobile technologies - such as e-mail, chat room discussion groups, instant messaging, webpages, social media or SMS (text messaging) - with the intention of physically or mentally harming another person.

'School and preschool ICT' refers to the school's computer network, internet access facilities, computers, and other digital devices as outlined below.

'Digital devices' some examples include: computers (such as desktops, laptops, iPads, tablets, Chromebooks), storage devices (such as USB and memory devices, CDs, DVDs, iPods), all types of mobile phones, cameras (such as video and digital cameras and webcams), gaming consoles, video and audio players (such as portable CD and DVD players), 'smart' watches and any other similar technologies.

'Inappropriate material' means material that deals with matters such as sex/sexual acts, full and partial nudity, cruelty or violence in a manner that is likely to be injurious to children or incompatible with a school or preschool environment.

'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.

'Digital Citizens' refers to people utilising ICT/digital devices regularly and effectively in order to participate online.

'Digital Citizenship' refers to appropriate, responsible technology use

Department for Education (DfE) 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

Use 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
- Password must not be based on anything somebody else could easily guess or obtain using person-related information
- Students must not disclose their personal passwords to any other person.
- 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:

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, jokes and images
- Bullying, harassing, defaming or giving offence to other people
- Spreading any form of malicious software (e.g. viruses)
- 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

Please note that:

- Child protection education, such as the Keeping Safe child protection curriculum, includes information about remaining safe when using new technologies and is provided to all students
- Material sent and received using the school computer network may be monitored and filtering software may be used to restrict access to certain sites and data, including e-mails. Where a student is suspected of an electronic crime, this will be reported to the South Australian Police. Where a personal electronic device such as a mobile phone is used to capture images of a crime such as an assault, the device will be confiscated and handed to the police
- While every reasonable effort is made by schools and DfE administrators to prevent children's exposure to inappropriate content when using the Department's online services, it is not possible to completely eliminate the risk of such exposure. In particular, DfE cannot filter internet content accessed by your child from home, from other locations away from school or on mobile devices owned by your child. DfE recommends the use of appropriate internet filtering software

Staff responsibilities:

- Observe a duty of care – this means staff 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 mandatory notification to the Child Abuse Report Line if child abuse and/ or neglect is suspected
- Model the responsible and ethical use of ICT in learning and teaching
- All staff are encouraged to be responsible models for students and be conscious of their online presence on social media sites, where settings are set to public

Leadership responsibilities:

- Gain written permission from parents before publishing video and photographs eg. images of their child/ren

- 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

DIGITAL DEVICES:

Parents/Caregivers, Visitors responsibilities:

- All users are to switch their phones to mute or discreet when in public areas, including meetings, interviews and classrooms
- All parents and visitors are requested to take and make phone calls outside teaching and learning areas
- Photographs of students at school, other than your own, are **not** to be used on social media. Parents should ensure that they have parental consent before photographing other people's children.

Student/Caregiver responsibilities:

- Portable digital devices (eg. mobile telephones, tablets, 'smart' watches, laptops) are brought to school entirely at the owner's risk. The school will not be involved in disputes and /or investigations over damage, loss or theft. Any damage or loss must be covered by the owner's family
- Students are not to have mobile phones or portable digital devices in their possession during school hours unless permission is given by the teacher to use the device for specific learning and research purposes. Their phones and devices need to be handed to the class teacher at the beginning of the school day and collected by the students at the end of the day. Devices will be secured in a lockable compartment
- Phones are not to be taken on excursions or camps
- Students breaching the policy will be subject to normal student behaviour management consequences. The student will be instructed to pass the phone to the leadership team for the rest of the day

Staff responsibilities:

- Personal phones or devices are brought to school at the owners' risk
- Personal calls are strongly discouraged during class teaching and learning periods
- All users are to switch their phones to mute or discreet when in public areas, including during meetings and interviews

Wi-Fi:

If using personal digital devices for educational purposes students will access the school Wi-Fi using the accepted school procedures. This enables students to access the internet within the normal school protections, which include a number of sites being blocked by DfE. Staff and students using the Tea Tree Gully Primary School Wi-Fi must sign the school internet user agreement and keep their username and password safe (not sharing it with anyone). Usage is monitored by the school.

Exemptions and Procedures for inappropriate behaviour:

- Exemptions from the expectations of this policy can only be approved by the Principal and then only in exceptional circumstances
- Misuse of mobile phones or other portable digital devices at school will be brought to the attention of school leadership for appropriate review of the student's privilege
- Students will follow these guidelines. Inappropriate use of any ICT's or digital devices will result in the withdrawing of computer privileges and reinstatement will be at the discretion of Leadership