TECOMA PRIMARY SCHOOL

CYBERSAFETY POLICY

Important terms used in this document:

*(a) **'Cybersafety'** refers to the safe and responsible use of the Internet and Digital Technology equipment/devices, including mobile phones*

*(b) **'School Digital Technologies'** refers to the school's computer network, Internet access facilities, computers, and other school DT equipment/devices as outlined in (c) below*

*(c) The term **'Digital equipment/devices'** used in this document, includes but is not limited to, computers (such as desktops, laptops, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, smart watches, video and audio players/receivers (such as portable CD and DVD players),Gaming Consoles, and any other, similar, technologies as they come into use.*

PURPOSE

Tecoma Primary School has a statutory obligation to maintain a safe physical and emotional environment, and a responsibility to consult with the community. In addition Tecoma Primary School Council has a responsibility to be a good employer.

These three responsibilities are increasingly being linked to the use of the Internet and Digital Technologies and a number of related cybersafety issues. The Internet and Digital devices/equipment bring great benefits to the teaching and learning programmes, and to the effective operation of the school.

Tecoma Primary School places a high priority on providing the school with Internet facilities and digital devices/equipment which will benefit student learning outcomes, and the effective operation of the school.

However, School Council recognises that the presence in the learning environment of these technologies (some provided partly or wholly by the school and some privately owned by staff, students and other members of the school community), can also facilitate anti-social, inappropriate, and even illegal, material and activities. The school has the dual responsibility to maximise the benefits of these technologies, while at the same time to minimise and manage the risks.

Council thus acknowledges the need to have in place rigorous and effective school cybersafety practices which are directed and guided by this cybersafety policy.

SCOPE

This policy applies to all student, staff and members of the school community.

POLICY

Tecoma Primary School will develop and maintain rigorous and effective cybersafety practices which aim to maximise the benefits of the Internet and digital devices/equipment to student learning and to the effective operation of the school, while minimising and managing any risks.

These cybersafety practices will aim to not only maintain a cybersafe school environment, but also aim to address the need of students and other members of the school community to receive education about the safe and responsible use of present and developing digital technologies.

Guidelines

Associated issues the school will address include:

- the need for on-going funding for cybersafety practices through inclusion in the annual budget,
- the review of the school's annual and strategic plan,
- the deployment of staff,
- professional development and training,
- implications for the design and delivery of the curriculum,
- the need for relevant education about cybersafety for the school community,
- disciplinary responses appropriate to breaches of cybersafety,
- the availability of appropriate pastoral support, and potential employment issues.

To develop a cybersafe school environment, School Council will delegate to the principal the responsibility to achieve this goal by developing and implementing the appropriate management procedures, practices, electronic systems, and educational programmes. These will be based on the eSmart programme for schools, of which Tecoma PS is a member. *eSmart* resources will play a central role in this process.

A process for reporting back to Council by the principal will be agreed upon and established. Frequency and content of reporting will be included. The School council will invite the eSmart coordinator to present at a school Council meeting annually.

Guidelines for Tecoma Primary School cybersafety practices

1. The school's cybersafety practices are to be based on information contained in the latest version of eSmart*.*
2. No individual may use the school Internet facilities and school-owned/leased digital devices/equipment in any circumstances unless the appropriate use agreement (Appendix A) has been signed and returned to the school. Use agreements also apply to the use of privately-owned/leased digital devices/equipment on the school site, or at/for any school-related activity, regardless of its location. This includes off-site access to the school network from school or privately-owned/leased equipment.
3. Tecoma Primary School use agreements will cover all DET employees, all students (including adult and community), and any other individuals authorised to make use of the school Internet facilities and digital devices/equipment, such as teacher trainees, external tutors and providers, contractors, and other special visitors to the school. Refer to the Internet and Email Policy.
4. The use agreements are also an educative tool and should be used as a resource for the professional development of staff.
5. Use of the Internet and the digital devices/equipment by staff, students and other approved users at Tecoma Primary School is to be limited to educational, professional development, and personal usage appropriate in the school environment, as defined in individual use agreements.
6. Signed use agreements will be filed in a secure place, and an appropriate system devised which facilitates confirmation that particular individuals are authorised to make use of the Internet and digital devices/equipment.
7. The school has the right to monitor, access and review all use. This includes personal emails sent and received on the schools computer/s and/or network facilities at all times.
8. The school has the right to audit at any time any material on equipment that is owned or leased by the school. The school may also request permission to audit privately owned digital devices/equipment used on the school site or at any school related activity.
9. Issues relating to confidentiality, such as sighting student or staff information, reasons for collecting data and the secure storage of personal details and information (including images) will be subject to the provisions of the Privacy Act 1993.
10. The safety of children is of paramount concern. Any apparent breach of cybersafety will be taken seriously. The response to individual incidents will follow the procedures developed as part of the school's cybersafety practices. In serious incidents, advice will be sought from an appropriate source, such as eSmart, DET and/or a lawyer with specialist knowledge in this area. There will be special attention paid to the need for specific procedures regarding the

gathering of evidence in potentially serious cases. If illegal material or activities are suspected, the matter may need to be reported to the relevant law enforcement agency.

POLICY REVIEW AND APPROVAL

This policy has a review cycle of 3-4 year	This policy was approved by school council on **18th May, 2021** and is scheduled for review in **May, 2024**. **Reviewed by:**
Reviewed by	*Rohan Thompson, Di Double, Chelsey Robins, Stuart McLean, Matt Ford, Bec Hale, Lisa Hoskins-Faul*
Approved by	***Principal** – Rohan Thompson* ***School Council President** – Lisa Dell*

APPENDIX A (FROM THE INTERNET AND EMAIL ACCESS POLICY)

INTERNET / EMAIL CODE OF PRACTICE

Student Agreement

I agree to use the internet, emails and class blogs at our school in a responsible manner for purposes stated by my teacher.

If I find myself in unsuitable locations I will immediately turn off the screen and inform my teacher.

When working on the internet I will:

- Only work on the web for purposes specified by my teacher.
- Not give out information such as my surname, address, telephone number, or parents' work address/telephone number.
- Never send a person my picture without first checking with my teacher.
- Always have my teacher's permission before sending email.
- Compose email messages using only language I understand is acceptable in my school.
- Not download any programs onto school computers.
- Not intentionally waste limited resources, including time.
- Not respond to any messages that are unpleasant or that make me feel uncomfortable in any way. It is not my fault if I get a message like that.
- I will not use material from other web sites unless I have permission from the person who created the material. If I am unsure I will check with my teacher.
- Follow school guidelines and procedures when preparing materials for publication on the web.
- Not damage computers by spreading viruses or changing system configurations.

I understand that breaches of the rules will see me lose my internet/email access rights for a period of time determined by my teacher and the ICT committee.

Student Name ______________________________

Student Signature ______________________________

Date ______________________________

Parent/Guardian:

I have discussed this agreement with my child and will support the school's internet/email Code of Practice.

Parent/Guardian Signature ______________________________

Parent/Guardian Name ______________________________

Date ______________________________