TOKOMARU SCHOOL

POLICY 5.3

CYBER SAFETY POLICY

Important terms used in this document:

*(a) The abbreviation **'ICT'** in this document refers to the term 'Information and Communication Technologies.*

*(b) **'Cyber safety'** refers to the safe and responsible use of the Internet and ICT equipment/devices, including mobile phones*

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

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

Rationale

Tokomaru School has a statutory obligation to maintain a safe physical and emotional environment, and a responsibility to consult with the community. In addition Tokomaru School Board of Trustees has a responsibility to be a good employer.

These three responsibilities are increasingly being linked to the use of the Internet and Information Communication Technologies (ICT), and a number of related cyber safety issues. The Internet and ICT devices/equipment bring great benefits to the teaching and learning programmes, and to the effective operation of the school, as well as skills required for the future.

The Board of Tokomaru School places a high priority on providing the school with Internet facilities and ICT devices / equipment which will benefit student learning outcomes, and the effective operation of the school.

However, the Board 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.

The Board thus acknowledges the need to have in place rigorous and effective school cyber safety practices, which are directed and guided by this cyber safety policy.

Policy Guidelines

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

To develop a cyber safe school environment, the board 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 latest version of the NetSafe® programme for schools, endorsed by the New Zealand Ministry of Education. *The NetSafe® Kit for Schools,* including its templates for policies and use agreements, will play a central role in this process.

A process for reporting back to the board by the principal will be agreed upon and established. Frequency and content of reporting will be included.
In recognition of its guardianship and governance role in the cyber safety of the school, the Board is also covered by 5.3.2b BOT ICT User Agreement (in regard to the of ICT devices / equipment for BOT business). This will cover all use of school-owned/leased and privately owned/leased ICT devices/equipment containing school data/information on or off the school site.

Guidelines for Tokomaru School Cyber Safety Practices

1. The school's cyber safety practices are to be based on information contained in the latest version of the *NetSafe® Kit for Schools*, which is endorsed by the New Zealand Ministry of Education as best practice for New Zealand schools.

2. No individual may use the school Internet facilities and school-owned/leased ICT devices/equipment in any circumstances unless the appropriate use agreement has been signed and returned to the school (except for Board of Trustees members, or guests to the school as mentioned in #3 below). Use agreements also apply to the use of privately-owned/leased ICT 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. Board of Trustee members and registered guests needing to use the Tokomaru School wifi network, will be given access via a Guest Wireless with a specific password (set by the school). Board members using the Guest Network for regular meetings need to sign and return 5.3.2b BOT ICT User Agreement, but guests being hosted by the school for a one-off event, do not.

4. A BYOD Agreement must be signed in order for students to bring and use their own devices at school.

5. User agreements for students are to be signed on enrolment.

6. Tokomaru School User Agreements will cover all board employees, all students (including adult and community), and any other individuals authorised to make use of the school Internet facilities and ICT devices/equipment, such as teacher trainees, external tutors and providers, contractors, and other special visitors to the school (whether an ICT User Agreement has been signed or not).

7. The use agreements are also an educative tool and should be used as a resource for the professional development of staff.

8. Use of the Internet and the ICT devices/equipment by staff, students and other approved users at Tokomaru School is to be limited to educational, professional development, and personal usage appropriate in the school environment, as defined in individual use agreements.

9. 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 ICT devices/equipment.

10. 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.

11. 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 ICT devices/equipment used on the school site or at any school related activity.

12. 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 2020.

13. The safety of children is of paramount concern. Any apparent breach of cyber safety will be taken seriously. The response to individual incidents will follow the procedures developed as part of the school's cyber safety practices. In serious incidents, advice will be sought from an appropriate source, such NetSafe, the New Zealand School Trustees Association 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.

14. These guidelines also all apply to any student who receives assistive technology.

Supporting Documents:	
Procedures:	**Supporting Documents:**
5.3.1 Cybersafety Policy - Student Procedure	5.3.1a Student ICT User Agreement 5.3.3 BYOD Guidelines for Usage
5.3.2 Cybersafety Policy – Staff Procedure	5.3.2a Staff ICT User Agreement 5.3.2b BOT ICT User Agreement 5.3.3 BYOD Guidelines for Usage 5.3.6 ICT User Breach Form

REVIEWED: **May 2023**
APPROVED: **June 2023**
NEXT REVIEW DATE: **May 2026**

APPROVED BY _____ **DATE** 20/6/2023
Presiding Member, BOT