



CYBERSAFETY POLICY

BACKGROUND

Waitakere SDA School has a statutory obligation to maintain a safe physical and emotional environment, and to be a good employer.

The Board places 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 cybersafety practices, which are directed and guided by this cybersafety policy.

POLICY

1. Waitakere SDA School will develop and maintain rigorous and effective cybersafety practices which aim to maximise the benefits of the Internet and ICT devices/equipment to student learning and to the effective operation of the school, while minimising and managing any risks.
2. 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 information and communication technologies.
3. To develop a cybersafe 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 Network for Learning (N4L) programme for schools, endorsed by the New Zealand Ministry of Education.
4. 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. 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.
5. Use 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 teachers, trainees, external tutors and providers, contractors, and other special visitors to the school.



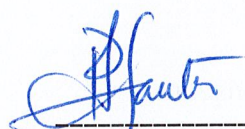
6. Use of the Internet and the ICT devices/equipment by staff, students and other approved users is to be limited to educational, professional development, and personal usage appropriate in the school environment, as defined in individual use agreements.
7. The school has the right to monitor, access and review all use. This includes personal emails sent and received on the school's computer/s and/or network facilities at all times. 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.
8. 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.
9. 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 N4L, the New Zealand School Trustees Association and/or a lawyer with specialist knowledge in this area. If illegal material or activities are suspected, the matter may need to be reported to the relevant law enforcement agency.
10. The school will provide relevant educational material and training on cybersafety to staff, students, and the wider school community.
11. The school will obtain written authorisation to publish the student's personal image or work online.

PROCEDURES

1. The Principal is responsible for the establishment and maintenance of the school's cybersafety programme. This will include the three components of (a) an infrastructure of appropriate policies, procedures and Use Agreements (b) and effective security system and (c) a comprehensive cybersafety education programme for the school community.
2. The Principal will report annually, or as the need arises, to the Board on the implementation of this policy.
3. On enrolment, all students must read, or in the case of some children, be read to, the Cybersafety Use Agreement. Parents will sign this. From Year 4 onwards the Cybersafety Use Agreement is to be re-signed each year by the student and parent. Students who don't sign will not be permitted to access the relevant school technologies; their parents/caregivers will be informed of this situation.
4. All Board/employees must sign the Cybersafety Use Agreement. They will be provided with an individual login username, password, and will be provided with an individual e-mail account. This needs to be kept confidential.
5. Cybersafety rules and information will be made readily accessible to students and displayed in each area/classroom involving cyber use.
6. Cybersafety education will be provided where relevant, through teaching programmes. This will include making decisions about which websites to visit, to limit (or not provide) personal information, and how to make published work 'private' (secure).



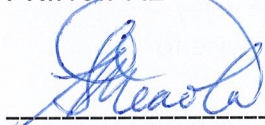
7. Processes for reporting any breaches of cybersafety regulations (by any member of the school community) are covered by the school's policies and procedures on: 'Concerns and Complaints' and 'Protected Disclosures'. Less serious matters (e.g. Unintentional misuse such as pop-up windows and accidentally accessing inappropriate sites) should be documented and reported to the Principal.
8. Original material created by students attracts protection under the Copyright Act 1994.
9. The school will only publish a student's image or work with written authorisation from the student's legal guardians.
10. The school will identify students on any websites only by their first name and year at school.
11. The school will not publish, access or pass on material that may defame anyone, be objectionable from a human rights point of view, be obscene, or infringe the copyright of third parties.
12. Students will be supervised while using the internet.



PRINCIPAL

2/2/2022

DATE



CHAIRPERSON

02/02/2022

DATE

RATIFIED BY BOARD: 02/02/2022

NEXT REVIEW DATE: FEB 2025



STUDENT USE AGREEMENT FORM

As a responsible student using technology, I understand the following is expected of me when using a Chromebook during the school year 2022:

- The use of the Chromebook in our classroom is a privilege. I, _____ agree that I will not take advantage of that privilege.
- I agree to place the Chromebook back in the assigned place each day.
- While using the Chromebook, I agree to not change any settings, that are on the Chromebook or digital device.
- I agree to neatly wrap the cords around the chargers and headphones and place them in the assigned place each day.
- While using the Chromebook, I agree to only use the Chromebook for assignments and schoolwork that my teachers have assigned.
- I will keep my hands on my own device, and not touch other people's devices.
- I will report any damage to the teacher.
- I will not place any decorations on my device.

If I fail to follow the device rules stated above, I can expect any or all the following consequences:

- 1st offense: Verbal warning. Students will be directed to put the device away.
2nd offense: Device will be confiscated, and I will not be able to use a device for the following two days.
3rd offense: Device will be confiscated, and I will not be able to use a device for the following week.
4th or more offense: Device will be confiscated, and I will not be able to use a device for the remainder of the term.

At any point, my parents and whanau may be called to school to discuss the way I have been using a digital device.

By signing below, I understand that using a Chromebook is a privilege and not my right. I will follow the above rules and will suffer any of the above consequences if I choose not to do what is expected of responsible Chromebook users.

Signed: _____

Your name: _____

Date: _____



Waitakere Seventh-day
Adventist School

Educating for Eternity

STAFF/BOT USE AGREEMENT FORM

CYBERSAFETY USE AGREEMENT FOR ALL STAFF AND BOT MEMBERS

This document outlines what Waitakere SDA School is doing to help ensure the cybersafety of the work environment. We are committed to maintaining the highest standards of professional behaviour, and a work environment which is safe.

Waitakere SDA School provides ICT equipment and devices for work related activities only. It is not available for personal use.

Any staff member who allows another person, who does not have a signed use agreement with Waitakere SDA School, to use ICT, is responsible for that use, and may be held responsible for any misuse.

The use of privately owned ICT devices in the workplace or at any work-related activity must be appropriate to the environment.

When using ICT at any time in the workplace you must not initiate access to, save, copy, show or print inappropriate, objectionable and / or illegal material.

ICT must not be used to deliberately facilitate any illegal or inappropriate workplace behaviour. This includes electronic communication that could cause offence to others, harass, or harm them, or put staff at potential risk.

All staff will be provided with a personal user account by Waitakere S D A School which they will use to access ICT resources. It is important that passwords are strong. Passwords must use a combination of upper- and lower-case letters, numbers, and symbols, and be a minimum of 8 characters in length. Passwords must be kept confidential and not shared with anyone else. Users should not allow any other person access to any equipment/device logged in under their own user account, unless as part of authorised work.

Staff must verify the contact details of recipients before sending confidential and/or sensitive information.

All ICT equipment/devices should be cared for in a responsible manner. Any damage, loss or theft of ICT equipment/devices must be reported immediately to your Principal.

The school currently operates a sustainable workplace policy which includes a reference to the use of ICT resources. Staff should familiarise themselves with this policy, to ensure that our sustainability objectives are met.

Copyright laws and licensing agreements must be respected at all times. All material and links published on Waitakere S D A website should be appropriate to the work environment. Published material can be posted only by those given the authority to do so.

No employee may bring the school into disrepute on any website.

I have read and am aware of the obligations and responsibilities outlined in this Waitakere SDA School's Staff/BOT Cybersafety Use Agreement document. I understand them, and I agree to follow them.

I also understand that apparent breaches of this agreement will be investigated and could result in disciplinary action.

Name: _____ Signature: _____ Role: _____ Date: _____