This document contains three sections.

- Cybersafety initiatives and rules
- Staff requirements regarding student cybersafety
- Cybersafety and technology user agreement for staff and adult volunteers

All school staff and adult volunteers must read this document and sign the agreement at the end.

This document should be read with:

- NAG 5: Cybersafety policy
- ICT user agreement for students

Additional background information on user agreements can be found on the NetSafe website (www.netsafe.org.nz/ua)

Instructions

- Read this entire document carefully.
- If any clarification is required, discuss this with the Principal before you sign the document.
- Detach the cybersafety and technology user section (the last two pages of this document).
- Sign it.
- Return it to the office.
- Retain the rest of this document future reference.

Terms used in this document

For the purposes of this document, the following definitions apply.

ICT	Information and communication technology
Cybersafety	The safe use of the internet and ICT equipment/devices, including mobile phones
School ICT	The school's computer network, internet access facilities, computers, and other school ICT equipment/devices (as outlined below)
ICT equipment/devices	This includes, but is not limited to: ● computers (such as desktops, laptops, PDAs) ● storage devices (such as USB and flash memory devices, CDs, DVDs, iPods, iPads, MP3 players) ● cameras (such as video, digital, webcams) ● all types of mobile phones ● gaming consoles ● video and audio players/receivers (such as portable CD and DVD players) ● any other similar technologies, as they come into use
Objectionable	In this agreement, 'objectionable' means material that deals with matters such as sex, cruelty, or violence in such a manner that it is likely to be injurious to the good of students or incompatible with a school environment. This definition is intended include the definition used in the Films, Videos and Publications Classification Act 1993.

Cybersafety initiatives and rules

The measures in document are designed to ensure the cybersafety of Waituna Creek School, and are based on our core values.

The school's computer network, internet access facilities, computers and other school ICT equipment/devices bring great benefits to our teaching and learning programmes, and help with the effective operation of our school.

We have rigorous cybersafety practices in place. This includes ICT user agreements for all school staff, students and volunteers, whether or not they make use of the school's computer network, internet access facilities, computers or other ICT equipment/devices in the school environment.

The overall goal is to create and maintain a cybersafety culture which is in keeping with the values of our school as well as our legislative and professional obligations.

1. This user agreement includes information about:
    - your obligations
    - your responsibilities
    - possible consequences of cybersafety breaches that undermine the safety of our school environment.
2. All staff and adult volunteers must read these pages carefully and return the signed cybersafety and technology user agreement (at the end of this document) to the school office for filing.
3. The school's computer network, internet access facilities, computers and other school ICT equipment/devices are for educational purposes appropriate to the school environment. Staff may use school ICT for professional development and personal use, as long as it is reasonable and appropriate to the school environment. This applies whether the ICT equipment is owned or leased, either partially or wholly, by the school and whether it is used on or off the school site.
4. Any staff member who has a signed user agreement with the school who allows another person, who does not have a signed user agreement, to use school ICT is responsible for that person's use.
5. The use of any privately owned/leased ICT equipment/devices on the school site, or at any school-related activity, must be appropriate to the school environment. This includes any images or material present or stored on privately owned/leased ICT equipment/devices brought onto the school site or to any school-related activity. This also includes the use of mobile phones.
6. When using school ICT, or privately owned ICT on the school site or at any school-related activity, users must not:
    - initiate access to inappropriate or illegal material
    - save or distribute such material by copying, storing, printing or showing to other people.
7. Users must not use any electronic communication (e.g. email, Facebook, Twitter, Instagram, text) in a way that could:
    - cause offence to others or harass or harm them
    - put anyone at potential risk
    - in any other way be inappropriate to the school environment.
8. Staff are reminded to be aware of their professional and ethical obligations when communicating via ICT with students outside school hours.
9. Users must not attempt to download, install or connect any software or hardware onto school ICT equipment, or utilise such software/hardware, unless authorised by the ICT Manager.

10. All material submitted for publication on the school website or intranet sites should be appropriate to the school environment. Such material can be posted only by those given the authority to do so by senior management.

11. Any photographs of students or examples of their work that are published online must meet the school's guidelines for publishing student information. This includes checking that parents have given consent for their child's image or work to be published, and obtaining the child's permission to use their work. Also refer to:
    - NAG 5: Health and safety procedures - publishing student information
    - The Ministry of Education's guidelines on privacy, safety and copyright associated with student material: www.tki.org.nz/r/governance/ curriculum/copyguide_e.php

12. All school ICT equipment/devices should be cared for in a responsible manner. Any damage, loss or theft must be reported immediately to the ICT Manager.

13. All users are expected to practise sensible use to limit wastage of computer resources and bandwidth. This includes avoiding unnecessary printing, internet access, uploads or downloads.

14. The users of school ICT equipment and devices must comply with the Copyright Act 1994 and any licensing agreements relating to original work. Users who infringe copyright may be personally liable under the provisions of the Copyright Act 1994.

15. Passwords must be strong, kept confidential and not shared with anyone else.

16. Users should not allow any other person access to any equipment/device logged in under their own user account, except with special permission from senior management.

17. The principles of confidentiality and privacy extend to accessing, inadvertently viewing or disclosing any information about staff, students or their families, which is stored on the school network or any ICT device.

18. Any electronic data or files created or modified on behalf of Waituna Creek School on any ICT, regardless of who owns the ICT, are the property of Waituna Creek School.

Dealing with incidents

19. Any incidents that involve unintentional or deliberate access of inappropriate material by staff or students must be recorded in handwriting in the cybersafety incident book with the date, time and other relevant details.

20. In the event of access of such material, users should:
    - not show others
    - close or minimise the window; **and**
    - report the incident to the Principal as soon as practicable.

21. If an incident involves inappropriate material or activities of a serious nature, or is suspected of being illegal, the incident must be reported to the Principal **immediately**.

Monitoring by the school

22. The school may monitor traffic and material sent and received using the school's ICT infrastructure.

23. The school reserves the right to use filtering and/or monitoring software where appropriate to restrict access to certain sites and data, including email. Users must not attempt to circumvent filtering or monitoring.

Breaches of the agreement

24. A breach of the user agreement may constitute a breach of discipline and may result in a finding of serious misconduct.

25. A serious breach of discipline would include involvement with objectionable material, antisocial activities such as harassment, or misuse of the school ICT in a manner that could be harmful to the safety of the school or call into question the user's suitability to be in a school environment.

26. If there is a suspected breach of the user agreement involving privately owned ICT on the school site or at a school-related activity, the matter may be investigated by the school. The school may request permission to audit the equipment/device(s) as part of its investigation into the alleged incident.

27. Involvement with material that is deemed 'objectionable' under the Films, Videos and Publications Classification Act 1993 is serious. In addition to any enquiry the school may undertake, the incident may be referred to an another agency to investigate offences under the Act. The agency may be notified at the commencement, during or after the school's investigation.

28. The school reserves the right to conduct an internal audit of its computer network, internet access facilities, computers and other school ICT equipment/devices, or commission an independent audit. If deemed necessary, this audit will include any stored content, and all aspects of its use, including email.

29. An audit may include any laptops provided by or subsidised by/through the school, or provided/subsidised by the Ministry of Education.

30. Conducting an audit does **not** give any representative of Waituna Creek School the right to enter the home of school personnel, nor the right to seize or search any ICT equipment/devices belonging to that person, except to the extent permitted by law.

Queries or concerns

31. Staff should take any queries or concerns regarding technical matters to the Principal.

32. Queries or concerns regarding cybersafety issues should be taken to the Principal.

33. In the event of a serious incident occurring while the Principal is not available, another member of senior management should be informed immediately.

Staff requirements regarding student cybersafety

All staff have the professional responsibility to ensure the safety and wellbeing of children using the school's computer network, internet access facilities, computers and other school ICT equipment/devices on the school site or at any school-related activity.

Students who have not not signed a user agreement will not be permitted to use school ICT equipment., unless there are special circumstances approved by the Principal. If your are aware of any student who has not signed a user agreement, you should advise the Principal.

Staff should guide students in effective strategies for searching and using the internet.

While students are accessing the internet in a classroom situation, the supervising staff member should be an active presence.The cybersafety manager will advise about cybersafety protocols regarding internet access by students in other situations.

Staff should support students to follow the student user agreement. This includes:

- endeavouring to check that all students understand the requirements of the student agreement
- regularly reminding students of the contents of the user agreement they have signed
- encouraging students to make positive use of ICT.

Staff are expected to follow the instructions of the cybersafety manager regarding their role in maintaining cybersafety where students are permitted to have email accounts. Student email accounts may involve remote access, or access to private non-school email from within the school or on the school network.

Cybersafety and technology user agreement for staff and adult volunteers

All ICT equipment owned by Waituna Creek School will be treated with the utmost care and respect.

Cellphones

- Cellphones are to be put on silent when in the classroom. Occasionally there is a personal need to keep your cellphone sound turned on. This is at the Principal's discretion.
- We discourage communication with parents via text.

Apps on cellphones

At times, apps from personal smartphones may be used if they are directly related to teaching and learning. The Principal needs to be notified if this is the case.

Computers/iPads

Computers/iPads are only to be used for tasks directly related to school work.

Personal emails

Personal email accounts are to be accessed during staff break times on personal equipment only.

Internet use

- The internet is only to be used to access information that is directly related to programmes and for accessing information to increase children's knowledge. History must not be deleted.
- If inappropriate material is accidentally accessed, you must immediately record it in the incident log book in the Principal's office, and notify the Principal.
- All computers used by children must have the highest protection systems in place.
- If children are accessing the internet, they must be supervised at all times. Any sites used for research must be checked by a staff member before sharing with children.

YouTube

Staff must check YouTube clips to ensure they are appropriate before sharing with children and/or other teachers.

Facebook

- The Principal is the only person who may upload to the Waituna Creek School Facebook account. owned by the school.
- Photos of children (and adults) can be put on our school Facebook page if the parent has given permission on a signed parent consent form.
- Children's names must not be used with the photos.
- All photos must:
    - be respectful
    - show children appropriately clothed (tops and pants/shorts or skirts)
    - have professional comments
    - reflect our school philosophy.
- The Principal must be notified immediately if you see any negative feedback on Facebook.
- Staff should not enter into discussions on Facebook.
- We discourage any facebook friend requests from parents, as this can compromise your professional relationships and your teacher's Code of Professional Responsibility

https://educationcouncil.org.nz/sites/default/files/Our%20Code%20Our%20Standards%20web%20booklet%20FINAL.pdf

Email

School-related or child-specific emails can only be sent from school emails and only if consent has been given by the child's parents on the parent consent form.

Printers/photocopier

- School printers are only to be used for work that is directly related to the school.
- If you want to print for community-based programmes, please discuss this with the Principal.
- If personal copying is more than 10 copies at a time please pay 10 cents per copy to the school.
- Teachers will respect the cost of printing and only use where necessary.
- Printing history must not be deleted.
- Any resources created using Waituna Creek equipment and in Waituna Creek School time are owned by the school.

School Gmail account

- Any documents made under your school Gmail account are the property of Waituna Creek School
- Google docs should only be shared within our @waitunacreek.school.nz network. If you want to share outside this group, please discuss this with Principal.
- If your contract is terminated, your gmail account will be deleted within 4 weeks.

Agreement

I agree to follow the agreement set out above. I understand that not meeting this agreement may be treated as misconduct.

I have read Waituna Creek School's cybersafety policy. I understand the contents and agree to ensure that the policy and this agreement are met at all times.

Name:	Signed:	Date: