# KERIKERI HIGH SCHOOL

## *CYBERSAFETY ACCEPTABLE USE POLICY FOR STUDENTS*

**This document is comprised of this cover page and three sections:**

**Section A: Introduction**

**Section B: Cybersafety Acceptable Use Policy for Students**

**Section C: Policy Acceptance Procedures.**

***Important terms used in this document:***

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

(b) ***'Cybersafety'** refers to the safe 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, 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, gaming consoles, video and audio players/receivers (such as portable CD and DVD players), and any other, similar, technologies as they come into use*

(e) *'**Objectionable**' in this agreement 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 is intended to be inclusive of the definition used in the Films, Videos and Publications Classification Act 1993.*

(f) *'**Parent**" in this document refers to a student's legal guardians and caregivers as well as natural parents.*

***Copies of the current version of this document are available at Kerikeri High School's Reception or on the school's website at http://www.kerikerihigh.ac.nz***

***Additional information on cybersafety can be found on NetSafe's website at http://www.netsafe.org.nz***

# SECTION A
# *INTRODUCTION*

The measures to ensure the cybersafety of Kerikeri High School students outlined in this document are based on Kerikeri High School's values.

The school's computer network, Internet access facilities, computers and other school ICT equipment/devices bring great benefits to the teaching and learning programmes at Kerikeri High School and to the effective operation of the school.

Our school has rigorous cybersafety practices in place, which include cybersafety acceptable use policies for all school staff and students.

The overall goal of this policy is to create and maintain a cybersafety culture which is in keeping with the values of the school, and legislative and professional obligations. This policy includes information about students' obligations, responsibilities, and the nature of possible consequences associated with cybersafety breaches which undermine the safety of the school environment.

All new students are issued with the current Cybersafety Acceptable Use Policy for Students and once signed consent has been given to the school, students are be able to use the school's ICT equipment/devices.

The school's computer network, Internet access facilities, computers and other school ICT equipment/devices are only for educational purposes appropriate to the school environment. This applies whether the ICT equipment is owned or leased either partially or wholly by the school, and used on or off the school campus.

# SECTION B
# *CYBERSAFETY ACCEPTABLE USE POLICY FOR STUDENTS*

## As responsible users of ICT, students are expected to keep themselves and others cybersafe as follows:

### Do Schoolwork Only

Students can only use the school's ICT equipment for schoolwork and must not:

- Access, or attempt to access, inappropriate, age restricted, or objectionable material
- Download, save or distribute such material by copying, storing, printing or showing it to other people
- Make any attempt to get around or bypass security, monitoring and filtering that is in place at school.

If students accidentally access inappropriate material, they should:

- Not show others,
- Immediately turn off the screen or close the window and
- Report the incident to a Teacher straight away.

The school monitors traffic and material sent, received or stored using the school's computer network. The school uses filtering systems to restrict access to Internet content and services.

The school audits its computer network, Internet access facilities, computers and other school ICT equipment/devices and may commission an independent forensic audit if required. Auditing of the above items may include any stored content, and all aspects of their use, including email.

## Keep Your Username and Password to Yourself

Students will be issued with a unique network username and given the opportunity to set their own password.

Students must only log on to the network with their own username and password and must log off when finished.

Students must not share their password with anyone and must not let anyone else use a computer that they have logged on to. Students will be held responsible for anything done using their username and password.

## Private Equipment Is Included

These policies also apply to any privately owned ICT equipment or devices such as mobile phones, USB flash drives, digital cameras or personal music players that students bring to school or to a school-related activity. Any images or material on such equipment or devices must be appropriate to the school environment.

Students are not allowed to bring privately owned computers to school unless written permission has been given by the ICT Manager or Cybersafety Manager.

## No Bullying, Harassment or Breaches of Privacy

Students will avoid any involvement with any material or activities that could put at risk the safety, security or privacy of any member of the school community. This applies both at school and off campus.

Students must not at any time use ICT to upset, offend, harass, threaten or in any way harm anyone connected to the school or the school itself.

Students must not give out any personal information about any other person without that person's permission. Personal information includes names, addresses, email addresses, phone numbers, and photos.

## Take Care of the School's Equipment

Students must treat all ICT equipment and devices with care and respect. This includes:

- Not intentionally disrupting the smooth running of any of the school's ICT systems
- Not attempting to hack or gain unauthorised access to any system
- Following the school's cybersafety policies and procedures, and not joining in if other students choose to be irresponsible with ICT
- Reporting any breakages or damage to a staff member immediately.

## Consequences for Breaches

Breaches of the cybersafety policies and procedures, will result in disciplinary action which may include informing parents. Students' families may be charged for physical or electronic damage, loss or theft.

When downloading files such as music and video clips, students must comply with the Copyright Act 1994. Anyone who infringes copyright may be personally liable under this law.

If illegal material or activities are involved in breaches of the cybersafety policies and procedures, it may be necessary for the school to inform the Police.

# SECTION C
# *POLICY ACCEPTANCE PROCEDURES*

## Students, parents, legal guardians and caregivers:

1. **Please read this document carefully** to check that you understand your responsibilities.
2. **Please sign** the appropriate section relating to this document in the student's **Enrolment Form.** The student and one parent must sign.
3. **Please keep this document** for future reference.

## Kerikeri High School will:

- Keep the student's signed Enrolment Form on file.
- Continue to do its best to keep the school cybersafe, by maintaining an effective cybersafety programme. This includes working to restrict access to inappropriate, harmful or illegal material on the Internet or school ICT equipment/devices at school or at school-related activities, and enforcing the requirements detailed in the staff and student cybersafety acceptable use policies.
- Respond immediately and appropriately to any breaches of the cybersafety acceptable use policies.
- Provide members of the school community with cybersafety education designed to complement and support the cybersafety acceptable use policies.
- Take all enquiries from students or parents about cybersafety issues and respond as fully and accurately as possible. Such enquiries should be directed to the school's Cybersafety Manager.

---

**This agreement for will remain in force as long as the student is enrolled at Kerikeri High School. If it becomes necessary to add to or amend the policy, parents will be advised.**

**The latest version of the policy can always be found on the school's website at http://www.kerikerihigh.ac.nz**