CYBERSAFETY AT WAIROA COLLEGE

CYBERSAFETY USE AGREEMENT

FOR ALL STUDENTS

<u>This document is comprised of a cover page and two sections:</u>

Section A – Cybersafety In The School Environment
- Important school cybersafety initiatives
- General cybersafety rules

Section B – Information Specifically For Students
- Additional information
- Additional rules / responsibilities
- Cybersafety Use Agreement Form

Instruction for secondary students:
1. You and your parent/legal guardian/caregiver are asked to read Section A 'Cybersafety In The School Environment' and Section B 'Information Specifically For Secondary Students' carefully.
2. If help is needed to understand all the language, or there are any points your family would like to discuss with the school, let the school office know as soon as possible.
3. You <u>and</u> your parent/legal guardian/caregiver should then sign the Student Use Agreement Form at the back of Section B before you return that page to the school.
4. It is important to keep Section A and Section B for you and your family to read again in the future.

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 mobil 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 player), cameras (such as video, digital webcams), all types of mobile phones, video and audio player/receivers (such as portable CD and DVD players), and any other, similar, technologies as they come into use.

IMPORTANT WAIROA COLLEGE CYBERSAFETY INITIATIVES

The values promoted by Wairoa College include respect for self and all others in the school community, and commitment to enabling everyone to achieve their personal best in an environment which is physically and emotionally safe. The measures to ensure the cybersafety of the school environment which are outlined in this document are based on these core 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 Wairoa College, and to the effective operation of the school. (Examples of what is meant by 'ICT equipment/devices' can be found on page one.) However, it is essential that the school endeavours to ensure the safe use of ICT within the school community.

Thus Wairoa College has rigorous cybersafety practices in place, which include cybersafety use agreements for all school staff and students.

Cybersafety use agreement documents include information about obligations, responsibilities, and the nature of possible consequences associated with breaches of the use agreement which undermine the safety of the school environment. The cybersafey education supplied by the school to its learning community is designed to complement and support the use agreement initiative. The overall goal of the school in this matter is to create and maintain a cybersafety culture which is in keeping with the values of the school, and legislative and professional obligations. All members of the school community benefit from being party to the use agreement initiative and other aspects of the school cybersafety programme.

1. **Cybersafety use agreements**

    1.1   All staff and students, whether or not they make use of the school's computer network, Internet access facilities, computers and other ICT equipment/devices in the school environment, will be issued with a use agreement. They are required to read these pages carefully, and return the signed use agreement form in Section B to the school office for filing. A copy of this signed form will be provided to the user.

    1.2   Staff and students are asked to keep the other pages of the agreement for later reference. (if necessary, a replacement copy will be supplied by the school's Cybersafety Manager.)

    1.3   Wairoa College encourages anyone with a query about the agreement to contact the Cybersafety Manager or the Principal as soon as possible.

2. **Requirement regarding appropriate use of ICT in the school learning environment**

    The use of the school's legislative obligation to maintain a safe physical and emotional learning environment, and be consistent with the values of the school:

    2.1   The use of **the school's** computer network, Internet access facilities, computers and other School ICT equipment/devices, on or off the school site, is limited to educational purposes appropriate to the school environment. This applies whether or not the ICT equipment is owned/leased either partially or wholly by the school. If any other use is permitted, the user(s) will be informed by the school.

    2.2   Wairoa College has the right to monitor, access, and review all the use detailed in 2.1. This includes Personal emails sent and received on the school's computers and/or network facilities, either during or outside school hours.

    2.3   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/stored on privately-owned/leased ICT equipment/devices brought onto the school site, or to any school-related activity.

    Such equipment/devices could include a laptop, desktop, PDA, mobile phone, camera, recording device, or portable storage (like a USB or flash memory device). Anyone unsure about whether or not it is appropriate to have a particular device at school or at a school-related activity, or unsure about whether the planned use of a particular device is appropriate, should check with the ICT Manager, or with the Cybersafety Manager.

    > Note that examples of a **'school-related activity'** include, but are not limited to, a field trip, camp, sporting or cultural event, wherever its location.

2.4 **When using a global information system** such as the Internet, it may not always be possible for the school to filter or screen all material. This may include material which **is inappropriate** in the school environment (such as 'legal' pornography), **dangerous** (such as sites for the sale of weapons), or **illegal** (which could include material defined in the Films, Videos and Publications Classification Act 1993, such as child pornography; or involvement with any fraudulent activity).

However, the expectation is that each individual will make responsible use of such systems.

3. **Monitoring by the school**

   3.1 Wairoa College has an electronic access monitoring system which has the capability to record Internet Use, including the user details, time, date, sites visited, length of time viewed, and from which computer or device.

   3.2 Wairoa College monitors traffic and material sent and received using the school's ICT infrastructures. From time to time this may be examined and analysed to help maintain a cybersafe school environment.

   3.3 Wairoa College will deploy filtering and/or monitoring software where appropriate to restrict access to Certain sites and data, including email.

   However, as noted in 2.4, the expectation is that each individual will be responsible in their use of ICT.

4. **Audits**

   4.1 Wairoa College will from time to time conduct an internal audit of its computer network, Internet access facilities, computers and other school ICT equipment/devices, or may commission an independent audit. If deemed necessary, auditing of the school computer system will include any stored content, and all aspects of its use, including email. An audit may also include any laptops provided or subsidised by/through the school or subsidised by a school-related source such as the Ministry of Education.

5. **Breaches of the use agreement**

   5.1 Breaches of the use agreement can undermine the values of the school and the safety of the learning Environment, especially when ICT is used to facilitate misconduct.

   5.2 Such a breach which is deemed harmful to the safety of the school (for example, involvement with Inappropriate material, or anti-social activities like harassment), may constitute a significant breach of discipline and possibly result in serious consequences. Wairoa College will respond to any breach of the use agreement in an appropriate manner, taking into account all relevant factors, including contractual and statutory obligations.

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

   5.4 Involvement with **material** which is deemed 'age-restricted', or 'objectionable' (illegal), under the Films, Videos and Publications Classification Act 1993, is a very serious matter, as is involvement in an **activity** which might constitute criminal misconduct, such as harassment. In such situations, it may be necessary to involve law enforcement in addition to any disciplinary response made by the school as a result of its investigation.

6. **Other aspects of the school's cybersafety programme**

   6.1 The use agreements operate in conjuction with other cybersafey initiatives, such as cybersafety Education supplied to the school community. This education plays a significant role in the school's overall cybersafey programme, and also helps keep children, young people and adult's cybersafe in all areas of their lives. If more information is required, the Cybersafey Manager, or the Principal, can be contacted.

GENERAL CYBERSAFETY RULES

These general rules have been developed to support the important school cybersafety initiatives outlined in Section A: Important Wairoa College Cybersafety Initiatives.

1. Staff and students are required to sign use agreements with the school

   1.1   Please sign the last page of this use agreement and the enrolment form.
   NB You should keep the entire document to refer to later, including this signed form.

2. Use of any ICT must be appropriate to the school environment

   2.1   **For education purposes only.** The school's computer network, intertnet access facilities, computers and other school ICT equipment/devices can be used only for educational purposes appropriate to the school environment. This rule applies to use on or off the school site. If any other use is permitted, Wairoa College will inform the user/s concerned.

   2.2   **Permitting someone else to use school ICT.** Any staff member or student who has a signed use Agreement with Wairoa College and allows another person **who does not have a signed use agreement as per point 1** (above) to use the school ICT, is responsible for that use.

   2.3   **Privately-owned ICT.** Us of 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/stored on privately-owned/leased ICT equipment/devices brought onto the school site or to any school-related activity. It also includes the use of mobile phones. Any queries should be discussed with the Cybersafety Manager, or with the Principal.

   2.4   **Responsibilities regarding access of inappropriate or illegal material.**
   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 or printing.

In the event of accidental access of such material, users should:
1. Not show others
2. Close or minimise the window
3. Report the incident
• Students should report to a teacher immediately
• Staff should report such access as soon as practicable to the ICT Manager, or to the senior manager designated as the school Cybersafety Manager.

   2.5   **Misuse of ICT.** Under no circumstances should ICT be used to facilitate behaviour which is either inappropriate in the school environment or illegal.

3. Individual password logons (user accounts)

   3.1   **Individual user name and password.** If access is required to the school computer network, computers and internet access using school facilities, it is necessary to obtain a personal user account from the school.

   3.2   **Confidentiality of passwords.** It is important to keep passwords confidential and not shared with anyone else.

   3.3   **Access by another person.** Users should not allow another person access to any equipment/device logged in under their own user account, unless with special permission from senior management. (Any inappropriate or illegal use of the Wairoa College computer facilities and other school ICT equipment/devices may be traced by means of this login information.)

   3.4   **Appropriate use of email.** Those provided with individual, class or group email accounts are expected to use them in a responsible manner and in accordance with this use agreement. This includes ensuring that no electronic communication could cause offence to others or harass or harm them, put he owner of the user account at potential risk, or in any other way be inappropriate in the school environment.

4.   Disclosure of personal details

4.1   For personal safety, users should be very careful about revealing personal information about them-selves, such as home or email addresses, or any phone numbers including mobile numbers. Nor should such information be passed on about others.

5.   Care of ICT equipment/devices

5.1   All school ICT equipment/devices shoul be cared for in a responsible manner.

5.2   Any damage, loss or therft must be reported immediately to the ICT Manager.

6.   Wastage

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

7.   Connecting software/hardware

7.1   Users must not attempt to download, install or connect any unauthorised software or hardware onto school ICT equipment, or utilise such software/hardware. This includes use of such technologies as Bluetooth, infrared, and wireless, and any other similar technologies which may be developed. Any user with a query or a concern about this issue should speak with the ICT Manager.

7.2   In a special case where permission has been given by the ICT Manager to connect or install privately-Owned equipment/devices or software, it is with the understanding that the school may scan this equipment/device/software at any time thereafter as part of a regular or targeted security check, such as for viruses.

8.   Copyright and licensing

8.1   Copyright laws and licensing agreements must be respected. This means no involvement in activities such as illegally copying material in any format, copying software, downloading copyrighted video or Audio file, using material accessed on the Internet in order to plagiarise, or illegally using unlicensed products.

9.   Posting material

9.1   all material submitted for publication on the school Internet/Intranet should be appropriate to the school environment.

9.2   Such material can be posted only by those given the authority to do so by senior management.

9.3   The ICT Manager, or the Cybersafety Manager, should be consulted regarding links to appropriate websites being placed on the school Internet/Intranet (or browser homepages) to provide quick access to particular sites.

9.4   There is only one official website relating to the school with which there should be involvement unless approval has been given by senior management.

10. Queries or concerns

10.1 Staff and students should take any queries or concerns regarding technical matters to the ICT Manager.

10.2 Queries or concerns regarding other Cybersafety issues should be taken to the senior manager with the role of School Cybersafety Manager, or to the Principal.

10.3 In the event of a serious incident which occurs when the Cybersafety Manager and the Principal are not available, another member of senior management should be notified immediately.

SECTION B – INFORMATION SPECIFICALLY FOR SECONDARY STUDENTS

ADDITIONAL INFORMATION

1. **The student Cybersafety Use Agreement**

   1.1 A teacher will go over this use agreement with you and answer any questions. If you have any more questions later, you should ask staff, including the senior manager who has been designated the School's Cybersafety Manager. If you parent/legal guardian/caregiver would like to discuss any school cybersafety issue, the Principal or Cybersafety Manager will be happy to discuss this with them.

   1.2 You cannot use the school's computer network, Internet access facilities, computers and other Wairoa College ICT equipment/devices until this Student Use Agreement has been signed by a parent/ Legal guardian/caregiver and signed by you, and the agreement has been returned to the school.

2. **Use of ICT**

   2.1 While at school or a school-related activity, you must not have involvement with any material or activity Which might put yourself at risk. As well, you must not at any time use ICT to upset, harass, or harm anyone else in the school community, or the school itself, even if it is meant as a 'joke'.

   > Unacceptable use could include acts of a malicious or nuisance nature, invasion of privacy, harassment, bullying, hacking, altering the settings on any ICT device or equipment without authorisation, plagiarism, gaming, impersonation/identity theft, spoofing, gambling, fraud, copyright infringement, or cheating in an examination. Behaviour the school may need to respond to also includes the use of websites to facilitate misconduct which puts at risk the safety of the school environment.

   2.2 If any privately-owned ICT equipment/device, such as a laptop, desktop, PDA, mobile phone, camera, Or recording device, portable storage (like a USB or flash memory device), is brought to school or a School-related activity, the school cybersafety rules apply to that device. **If you are not sure whether it is appropriate to have a particular device at school or at a school – related activity, you are expected to check with the relevant teacher before bringing it.**

3. **Monitoring**

   3.1 Wairoa College reserves the right at any time to check work or data on the school's computer network, Internet access facilities, computers and other school ICT equipment/devices. For example, in order to help make sure that the school stays cybersafe, teachers may at any time check student email or work.

   3.2 If there is a suspected breach of use agreement involving privately-owned ICT, the matter may be Investigated by the school. Wairoa College may ask to check or audit that ICT equipment/device as part of its investigation into the alleged incident.

4. **Consequences**

   4.1 Depending on the seriousness of a particular breach of the use agreement, an appropriate response will Be made by the school. Possible responses could include one or more of the following: a discussion with the student, informing parents/legal guardian/caregiver, loss of student access to school ICT, taking disciplinary action. If illegal material or activities are involved, it may be necessary for Wairoa College to inform the police.

ADDITIONAL CYBERSAFETY RULES FOR STUDENTS

1. **Accessing the Internet at school on school ICT.** The only time you can access the Internet at school on a school computer of any kind is when a teacher gives permission and there is staff supervision. If other Internet access on the school site or at a school-related activity is permitted, for example, via a privately-owned laptop, mobile phone or any other ICT device, it must be in accordance with the cybersafety rules in this agreement.

2. **Borrowing school ICT.** If a you have permission to use school ICT equipment at home or anywhere else away from school, it must not be given to anyone else to use unless at the direction of a staff member. The school ICT is to be used only for the purpose it was lent, and you should explain this to your family or whoever else you are with. If a problem occurs, you must report it to the relevant teacher straight away.

3. **Mobile phones.** Cybersafety rules also apply to mobile phones. You are not permitted to have a phone on in class time unless this is approved by a staff member. Mobile phones must not be used for involvement with inappropriate material or activities, such as:
    *   Upsetting or harassing students, staff and other members of the school community even as a 'joke.
    *   Inappropriately us in text, 'pxt', email, photographs or film, phone messages, web browsing, images or any other functions.
    *   Having a mobile phone in your possession, or near you, during any assessment.

4. **Care of the computers and other school ICT equipment/devices, and their appropriate use includes:**
    *   You must not damage or steal any equipment, or try to damage the ICT network. If the damage is deliberate, it will be necessary for the school to inform your parent/legal guardian/caregiver. Your family may have responsibility for the cost of repairs or replacement.

5. **Students need permission from staff to:**
    *   Use storage devices to back-up work or to take work home/back to school. (It is likely the school will need to check any storage device for such things as viruses.)
    *   Print material when in the classroom situation. Any material printed out of class must be appropriate in the school environment.
    *   Contribute material to the school Internet/Intranet site. As well, there should be not student involvement in any unofficial school Internet/Intranet site which purports to be representative of the school or of official school opinion.

6. **Students must be considerate of other users, This includes:**
    *   Sharing with other users and not monopolising equipment.
    *   Avoiding deliberate wastage of ICT – related resources including bandwidth, through actions such as unnecessary printing, and unnecessary Internet access, uploads or downloads.
    *   No intentional disruption of the smooth running of any computer or the school network.
    *   Avoiding involvement in any incident in which ICT is used to send or display messages/communications which might cause offence to others. Examples include text messaging, email messages, or creating, displaying or sending inappropriate graphics, and recording or playing inappropriate audio or video files.
    *   Obtaining permission from any individual before photographing, videoing or recording them.

7. **Respect for privacy, safety and security when using the Internet and ICT includes:**
    *   if you accidentally access inappropriate, dangerous or illegal material you should:
        1. not show others
        2. close or minimise the window
        3. report the incident to a teacher immediately.
    *   You should use data storage devices such as disks, only in accordance with school regulations. This includes portable devices such as USB and flash memory devices.
    *   You must have no involvement in any activity which could put at risk the security of the Wairoa College computer network or environment. For example, no involvement with malware such as viruses or involvement with any form of electronic vandalism or theft. This includes 'hacking' and any other unauthorized access.

WAIROA COLLEGE CYBERSAFETY USE AGREEMENT FORM FOR SECONDARY STUDENTS

To the student, and the parent/legal guardian/caregiver
1. Please read this page carefully, to check you understand your responsibilities under this agreement
2. Sign the appropriate section on this form and also the enrolment form.
3. Keep the document for future reference, as well as the copy of this signed page which the school will provide

We understand that Wairoa College will:
- 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 cybersafety regulations and responsibilities detailed in use agreements
- Keep a copy of this signed use agreement form on file
- Respond appropriately to any breaches of the use agreements
- Provide members of the school community with cybersafety education designed to complement and support the use agreement initiative
- Welcome enquiries from students or parents about cybersafety issues.

STUDENT'S SECTION

My responsibilities include:
- **I will read** this Secondary Student Cybersafety Use Agreement document carefully
- **I will follow** the cybersafety rules and instructions whenever I use the school's computer network, Internet access facilities, computers and other school ICT equipment/devices
- **I will also follow** the cybersafety rules whenever I am involved with privately-owned ICT devices/equipment on the school site or at any school-related activity, regardless of its location
- **I will avoid** any involvement with material or activities which could put at risk my own safety, or the privacy, safety or security of the school or other members of the school community
- **I will take proper care** of computers and other school ICT equipment/devices. I know that if I have been involved in the damage, loss or theft of ICT equipment/devices, my family may have responsibility for the cost of repairs or replacement
- **I will keep** this document somewhere safe so I can refer to it in the future
- **I will ask** the relevant staff member if I am not sure about anything to do with this agreement.

I have read and understand my responsibilities and agree to abide by this Cybersafety Use Agreement. I know that if I breach this use agreement there may be serious consequences.

Name of student: ……………………………………………….

Student signature: ………………………………………………. **Date:** ………………………….

SECTION FOR PARENT/LEGAL GUARDIAN/CAREGIVER

My responsibilities include:
- **I will read** this Secondary Student Cybersafety Use Agreement document carefully and discuss it with my son/daughter so we both have a clear understanding of my child's role in the school's work to maintain a cybersafe environment
- **I will ensure** this use agreement is signed by my child and by me, and returned to the school
- **I will encourage** my son/daughter to follow the cybersafety rules and instructions
- **I will contact** the school if there is any aspect of this use agreement I would like to discuss.

I have read this Cybersafety Use Agreement document and am aware of the school's initiatives to maintain a cybersafe learning environment, including the responsibilities involved.

Parent/Legal Guardian/Caregiver (Please circle which term is applicable.)

Name of Parent: ……………………………………………….

Parent signature: ………………………………………………. **Date:** ………………………….