
# Whakatane High School

## Cybersafety Use Agreement for students and parents/caregivers

*Challenging Students to Achieve – Kia Whakatane Au I Ahau!*

# Cybersafety Use Agreement for students and parents/caregivers

Please make sure you read and understand the information contained in this booklet before you sign the Student Cybersafety Use Agreement. If you are not sure of what you are reading, ask your parents/caregivers or your teacher.

Cybersafety in the School Environment

- Important Whakatane High School Cybersafety and Digital Citizenship Initiatives
- Cybersafety Rules
- Additional information
- Student Cybersafety Use Agreement Form (to complete and return)

**Instructions for students**

You and your parent/caregiver are asked to read this booklet carefully.

1. If help is needed to understand 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.
2. You and your parent/caregiver should then sign the *Student Cybersafety Use Agreement Form* attached to this booklet and return that page to the school.
3. It is important to keep this booklet at home 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, Social Media Networking, 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.*

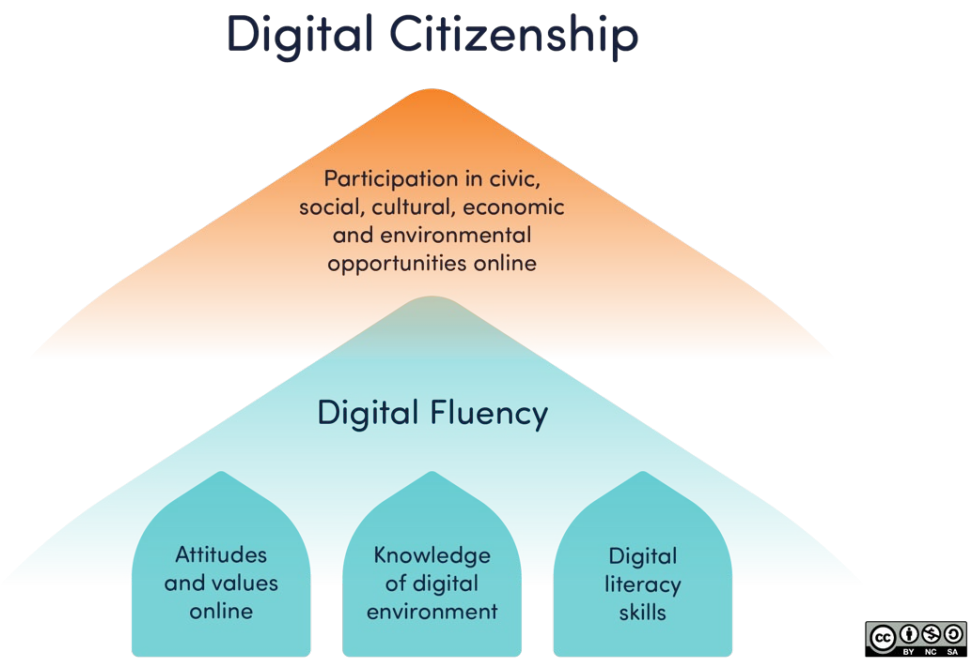
*(d) The term 'ICT equipment/devices' used in this document, includes but is not limited to, computers (such as desktops, Chromebooks, laptops, tablets,), storage devices (such as USB and flash memory devices, external storage devices, CDs, DVDs, iPods, MP3 players), cameras (such as video, digital,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

**Challenging Students to Achieve – Kia Whakatane Au I Ahau!**

# Cybersafety and Digital Citizenship in the School Environment

**Important Whakatane High School Cybersafety and Digital Citizenship Initiatives**
The values promoted by Whakatane High School include **respect** for yourself and all others in our school community, and commitment to *challenge students to achieve* their personal best in a school which is physically and emotionally safe. The measures to ensure cybersafety and digital citizenship within the school environment are based on these core values.

**Digital Citizenship Definition (source: Netsafe)**
Someone who engages with, and participates in, online opportunities safely, respectfully and meaningfully.




Netsafe asserts that digital citizenship combines the *confident, fluent use and combination* of three key elements:

- **Skills and strategies** to access technology to communicate, connect, collaborate and create;
- **Attitudes, underpinned by values** that support personal integrity and positive connection with others;
- **Understanding and knowledge of the digital environments and contexts** in which they are working, and how they integrate on/offline spaces;

and then *critically:*

- The ability to **draw on this competency of 'digital fluency'** to participate in life-enhancing opportunities (social, economic, cultural, civil) and achieve their goals in ways that make an important difference.

The school's computer network, social networking sites, website, video conferencing, messaging, applications, internet access facilities, Chromebooks, computers, G Suite For Education platform, and other school ICT equipment (devices), provide relevant 21st Century learning at Whakatane High School, and contribute 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 and positive digital citizenship in general.

Therefore Whakatane High School 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 the school's learning community. The cybersafety 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's cybersafety programme.

**1. Cybersafety Use Agreement**

1.1. All staff and students, whether or not they make use of the school's: computer network, social networking sites, website, video conferencing, messaging, applications, internet access facilities, Chromebooks, computers and other ICT equipment/devices in the school environment, will be issued with a use agreement. They are required to read the agreement carefully, and return the signed Cybersafety Use Agreement form to the school office for filing. 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 office.)

1.2 The school encourages anyone with questions about the agreement to contact a teacher or the Deputy Principal Of Pastoral Care, Carole Hughes, as soon as possible.

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

In order to meet 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, social networking sites, website, video conferencing, messaging, applications, Chromebooks, 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 The school has the right to monitor, access, and review all the use detailed in 2.1. This includes emails, public posts to social networking sites, messaging, video conferencing and other applications using the school's computers, Chromebooks or other school ICT equipment/devices, or cellular devices and/or network facilities, during school hours and after hours if the student uses their school sign in.

2.3 The use of any privately-owned/leased ICT equipment/devices at school, or at any school-related activity must be appropriate to the school environment. This includes any images, videos, social networking sites, websites, applications, 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 computer, Chromebook, tablet, mobile phone, camera, recording device, drone, or portable storage (like a USB or flash memory device), or alternate 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 a teacher or the Deputy Principal Of Pastoral Care, Carole Hughes.

*Note:*
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 Whakatane High School uses an internet management and network security system which has the capability to record Internet use, including: user details, time, date, sites visited, length of time viewed, and the computer or device MAC address.

3.2 The school 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 cyber safe school environment.

3.3 The school 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**

The school will from time to time conduct an internal audit of its computer network, internet access facilities, computers, Chromebooks, social networking posts, website, applications, and other school ICT equipment/devices, or may commission an independent audit. If deemed necessary, auditing of the school network will include any stored content, and all aspects of its use, including email. An audit may also include any laptops, Chromebooks, or other devices 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 bullying), may constitute a significant breach of discipline and possibly result in serious consequences. The school will respond to any breach of the use agreement in an appropriate manner and in accordance with the school's pastoral care policies, taking into account all relevant factors, including contractual and statutory obligations.

5.3 If there is a suspected breach of the use 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 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 conjunction with other cybersafety initiatives, such as cybersafety education supplied to the school community. This education plays a significant role in the school's overall cybersafety programme, and also helps children, young people and adults to become positive digital citizens in all areas of their lives. If more information is required, a teacher, or the Deputy Principal Of Pastoral Care, Carole Hughes, can be contacted.

# Cybersafety Rules

These general rules have been developed to support the school's cybersafety initiatives outlined above.

**1. Students are required to sign Cybersafety Use Agreements with the school**

1.1 Please sign the Student Cybersafety Use Agreement and return at the time of enrolment. This booklet should be kept to refer to in the future.

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

2.1 For educational purposes only

The school's computer network, internet access facilities, computers, Chromebooks, social networking sites, website, applications and other school ICT equipment/devices can be used only for educational purposes appropriate to the school environment. This rule applies to ICT use onsite or at school-related activities. If any other use is permitted, the school will inform the user/s concerned.

2.2 Permitting someone else to use school ICT

Students are not permitted to allow another person to use their personal school sign in to access the school's network or wifi, or for any other purpose. Students are responsible for keeping their sign in private and confidential. Any issues around digital privacy or security are to be raised immediately with a teacher. Abuse of this system is monitored via the school network, internet management system, and student sign ins.

**3. Privately-owned ICT**

Use of privately-owned/leased ICT equipment/devices at school, or at any school-related activity must be appropriate to the school environment. This includes any images, video, social networking sites, website, applications, 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 a teacher, or with the Deputy Principal Of Pastoral Care, Carole Hughes.

3.1 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 posting, copying, storing, printing or by any other means

In the event of accidental access of such material, users should

- Not show others
- Close or minimise the window
- Report the incident - students should report to a teacher immediately

Staff should report such access as soon as practicable to the Deputy Principal of Pastoral Care, Carole Hughes.

3.2 Misuse of ICT

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

**4. Individual password sign ins (user accounts)**

4.1 Individual username and password

If access is required to the school network, computers, Chromebooks and internet using school facilities, it is necessary to obtain a user account from the school.

4.2 Confidentiality of passwords

It is important to keep passwords confidential and not shared with anyone else.

4.3 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 or harm to others, or put the owner of the user account at potential risk, or in any other way be inappropriate.

It is important for students to be aware of the Harmful Digital Communications Act, 2015 which includes NOT:

1. sending or publishing threatening or offensive material
2. spreading damaging rumours
3. sending or publishing sensitive personal information such as embarrassing photos and videos
4. Digital communication is defined widely in the Act to include any form of electronic message such as texts, photos, pictures, recordings etc.

The test for determining what is a harmful digital communication is whether the communication was designed to cause serious emotional distress.

**5. Disclosure of personal details**

5.1 For personal safety, users are advised not to reveal personal information about themselves, such as home or email addresses, or any phone numbers including mobile numbers. Nor should such information be passed on about others.

**6. Care of ICT equipment/devices**

6.1 All school ICT equipment/devices should be cared for in a responsible manner.

6.2 Any damage, loss or theft must be reported immediately to a teacher.

**7. Connecting software/hardware**

7.1 Users must not attempt to download, install or connect to any unauthorised software or hardware using school ICT equipment, or utilise such software/hardware. This includes use of such technologies as Bluetooth, Virtual Private Networks (VPNs), 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 a teacher.

7.2 In a special case where permission has been given by the eHub team 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 files, using material accessed on the Internet in order to plagiarise, or illegally using unlicensed products.

**9. Posting material to Social Networking Sites**

9.1 All material submitted for publication on the school's social networking sites, website, or app should be appropriate to the school environment and should not cause harm.

9.2 Such material can be posted only by those given the authority to do so by senior leadership (Deputy Principals or Principal).

9.3 The eHub team, or the Principal, should be consulted regarding adding links to, or from, appropriate websites and/or social networking sites. Adding applications to the school network must have the prior approval of the eHub team or senior leadership.

9.4 Whakatane High School has one official website, one application and the following social networking accounts: Twitter, Facebook and Instagram. Involvement with these accounts is not permitted without prior approval from the Deputy Principals or the Principal.

9.5 Permission to photograph, video, audio record, and post images of staff and students must be obtained prior to taking the image, audio recording or video, and prior to posting.

**10. Queries or concerns**

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

10.2 Queries or concerns regarding other cybersafety issues should be taken to the Deputy Principal of Pastoral Care, Carole Hughes, or to the Principal.

10.3 In the event of a serious incident which occurs when Ms Hughes and/or the Principal are not available, another member of senior leadership should be notified immediately (Assistant Principals or Deputy Principal), or the eHub team.

**11. Accessing the Internet at school on school ICT**

11.1 The only time you can access the internet at school on a school Chromebook, or 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 Chromebook, laptop, mobile phone or any other ICT device, it must be in accordance with the cybersafety rules in this agreement.

**12. Borrowing school ICT**

12.1 If 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.

**13. Mobile phones**

13.1 Cybersafety rules also apply to mobile phones. You are not permitted to have a phone on in class time unless this is approved by the teacher. Mobile phones must not be used for involvement with inappropriate material or activities, such as:

- Upsetting or bullying students, staff and other members of the school community even as a 'joke'
- Inappropriately using text, 'pxt', email, photographs, video, messaging, web browsing, images, audio recording or any other functions
- Having a mobile phone in your possession, or near you, during any assessment unless with prior approval

**14. Care of the computers and other school ICT equipment/devices, and their appropriate use**

- 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

**15. 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). Students are encouraged to use Google Drive storage, provided for free, with their student account.
- 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, school website, school app, and social networking sites. As well, there should be no student involvement in any unofficial school Internet site which purports to be representative of the school, or of official school opinion**

**16. 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 Chromebook, computer or the school network
- Avoiding involvement in any incident in which ICT is used to send or display messages, images, video or communications which might cause offence or harm 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.

**17. Respect for privacy, safety and security when using the internet and ICT includes**

You must have no involvement in any activity which could put at risk the security of the school network or environment, e.g. no involvement with viruses or with any form of electronic vandalism or theft. This includes `hacking' and any other unauthorised access.

# Additional Information

**1. The Student CyberSafety Use Agreement**

1.1 Students will be taken through this use agreement and answer any questions. If you have any more questions later, you should ask the eHub team, or the Principal. If your parent/legal guardian/caregiver would like to discuss any school cybersafety issue, the eHub team or the Principal will be happy to discuss this with them.

1.2 You cannot use the school's computer network, internet access facilities, computers and other Whakatane High School 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 or others at risk. As well, you must not at any time use ICT to upset, bully, or harm anyone else in the school community, or the school itself, even if it is meant as a 'joke'.

2.2 Unacceptable use could include, but is not limited to, 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 may also include the use of websites, applications, social networking sites, or the like, to facilitate misconduct which puts at risk the safety of the school community. Harmful Digital Communications Act 2015: http://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html

2.3 If any privately-owned ICT equipment/device, such as a Chromebook, laptop, desktop, 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 The school reserves the right at any time to check work or data on the school's: network, internet access facilities, Chromebooks, computers, social networking sites, website, applications and other school ICT equipment/devices. For example, in order to help make sure that the school remains cyber safe, 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. The school 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 the school to inform the police. Harmful Digital Communications Act 2015: http://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html

On the following page is a copy of the Student Cybersafety Use Agreement Form for your reference. Parents, caregivers and students are asked to sign the copy of this form (which is included in the enrolment pack) and return it to the school. This signed agreement is kept on the student's file and entitles them to use ICT equipment at Whakatane High School.

NetSafe are a source of useful information for staying safe online.

To the student and the primary caregiver:

1. Please read this agreement carefully, to check that you understand your responsibilities
2. Sign the appropriate section on this form and return it with your enrolment documents
3. Keep the blue booklet for future reference

We understand that Whakatane High School will:

- Keep the school cyber safe, 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 the use agreement
- Keep a copy of this signed use agreement form on file
- Respond appropriately to any breaches of the use agreement
- 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 responsibilities include:

- **I will read** this Student Cyber Safety Use Agreement document carefully
- **I will follow** the cyber safety rules and instructions whenever I use the school's computer network, internet access facilities, computers and other school ICT equipment/devices
- **I agree not to** use VPNs (Virtual Private Networks) or any other means of circumventing the school's internet management and network safety protocols.
- **I will adhere** to the age limit rules and appropriate behaviour and integrity expectations on all sites**.**
- **I will also follow** the cyber safety rules whenever I am involved with BYOD, BYOC and 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 ask permission from students, staff and anyone on the school grounds before taking, using or posting, recordings, images or videos. I will comply with the school's cyber safety rules relating to the use of recordings, images and videos at all times.
- **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 ask** the relevant staff member if I am not sure about anything to do with this agreement

## Primary Caregiver's responsibilities include:

- **I will read** this Student Cyber Safety Use Agreement document carefully and discuss it with my son/daughter so we both have a clear understanding of my son's/daughter's role in the school's work to maintain a cyber safe environment
- **I will ensure** this use agreement is understood and signed by my son/daughter and by me, and returned to the school
- **I will contact** the school if there is any aspect of this use agreement I would like to discuss
- **I will endeavour** to attend Cyber Safety and Digital Citizenship informational events provided by the school.