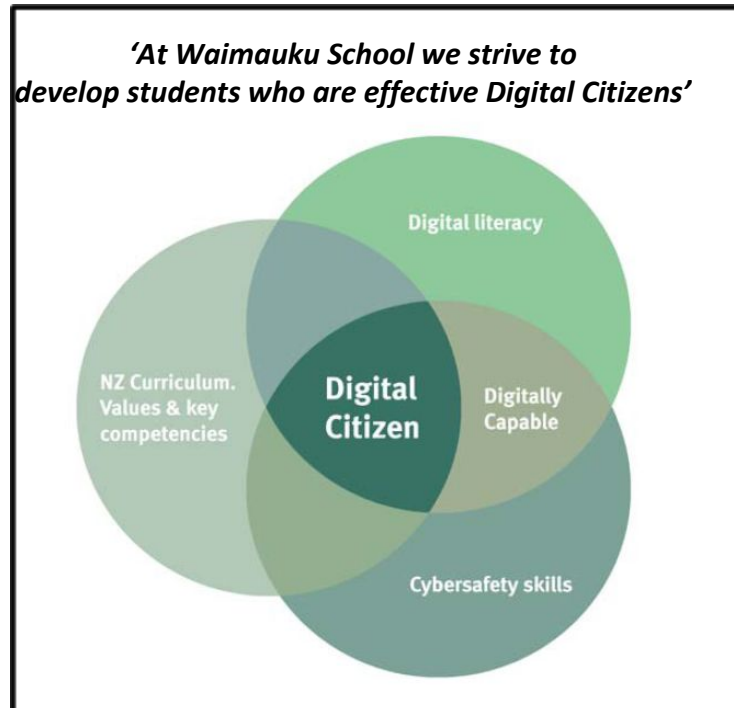# THE DIGITAL CITIZEN POLICY

BACKGROUND

The concept of creating a cyber-safe environment has moved from protecting people to giving people the skills, knowledge and confidence to maximise the opportunities the effective use of technology can bring.

A DIGITAL CITIZEN:

• is a confident and capable user of Information and Communication Technologies (ICT)

• uses technologies to participate in educational, cultural, and economic activities

• uses and develops critical thinking skills in cyberspace

• is literate in the language, symbols, and texts of digital technologies

• is aware of ICT challenges and can manage them effectively

• uses ICT to relate to others in positive, meaningful ways

• demonstrates honesty and integrity and ethical behaviour in their use of ICT

• respects the concepts of privacy and freedom of speech in a digital world

• contributes and actively promotes the values of digital citizenship

Digital literacy or the ability to understand and fully participate in the digital world is fundamental to digital citizenship. It is the combination of technical and social skills that enable a person to be successful and safe in the information age. Like literacy and numeracy initiatives which provide people with the skills to participate in the workforce, digital literacy has become an essential skill to be a confident, connected, and actively involved lifelong learner.

RATIONALE

Providing the framework for safe access to the communication technologies, such as the Internet, computers and mobile devices for all users, both staff and children is fundamental to our school.

PURPOSE

1. To provide Internet access, so all staff and students can become effective digital citizens.
2. To understand that the use of the Internet facilities at this school is strictly for educational purposes. This includes personal use and use for professional development of staff.

GUIDELINES

A   STUDENT USE OF THE INTERNET:

1   All students must sign the Student Cybersafety and Internet Use Agreement **AND** have the signed permission of a parent/caregiver before using the Internet at school. This document will be signed at time of enrolment and entered onto the school's database and originals are filed and kept in the office with enrolment records.

2   Classroom teachers unsure if a 'Cybersafety and Internet Use Agreement' has been signed are responsible for checking with the office staff to see if one has. If not, then these students are not permitted to use the Internet until an agreement is in place.

3   The Internet Safety Guidelines will be displayed near all computers that children have access to. They are as follows:
      Never give out your surname, address, phone numbers or passwords to anyone.
      Search using suitable and sensible keywords
      Turn off the screen and tell a teacher if a 'NO'* picture or website appears.
      Check with a teacher before downloading anything.
      If in doubt ask a teacher.

4   There will be restrictions on when students are able to use the Internet for learning (an automatic timer will disable students wireless Internet outside school hours).

5   Consequences for failure to follow these rules will result in disciplinary action, which can lead to the removal of Internet and computer privileges for up to 10 weeks. Serious breaches or continual failure to follow guidelines may result in serious disciplinary action.

      * A 'NO' picture or website is one that includes content that makes a child feel uncomfortable. These may include material of a pornographic nature or explicit violence etc.

B   STAFF USE OF THE INTERNET:

1   Training for staff who wish to use these facilities is available through the ICT Coordinators and/or the Principal and is **essential** for the safety and protection of staff, students, and equipment.

2   All staff members must sign a copy of this School Cybersafety and Internet Use Agreement before using the Internet themselves, indicating they are aware of the details of this Policy. This documentation will be kept on file by the school.

3   Staff will have individual Internet E-mail accounts.

4   In consultation with the ICT Coordinators and/or the Principal, staff can request websites to be 'unblocked' for educational purposes.

5   Standards of Conduct – the Internet should only be used as part of the normal execution of teacher's responsibilities and should be used in a manner that is consistent with the employer's standards of conduct.

6   Protocols – information communicated via the Internet should be subject to the same protocols and publication standards as traditional means of communication.

7   Monitoring Rights – the management of the school reserves the right to monitor the volume and cost of network traffic generated by each person at all times, and the right to monitor, access, retrieve and read all communications.

8   Appropriate Activities – staff using the Internet must ensure that the use they make is "appropriate". Examples of appropriate use include:
        a.   Conducting research and/or investigation.
        b.   Communication and information exchange with Government agencies and other organizations as required by teachers work.
        c.   Retrieving news stories or other information of interest to the school
        d.   Professional development activity.

9   Prohibited Activities – staff must not use the Internet for inappropriate purpose. Inappropriate use includes but is not limited to:
        a.   Visiting sites or voluntarily receiving communications that contain material that is obscene, objectionable, or likely to be offensive.
        b.   Gambling
        c.   Soliciting for personal gain or profit
        d.   Making or posting indecent remarks and proposals
        e.   Uploading or downloading commercial software in violation of its copyright.

10   Passing off personal views as representing those of the school.

11   Any activity that violates New Zealand laws and/or the public service code of conduct.

12   Extensive private usage – extensive when it either interferes with the teacher's role or generates unacceptable costs to the school.

STAFF ARE RESPONSIBLE FOR:

1.   Immediately informing the ICT Coordinators and/or the Principal if a virus is detected on any computer.

2.   Adhering to the Cybersafety and related BOYD policy and guidelines, and immediately reporting to the Resource Manager and/or ICT Coordinator, any perceived weaknesses or breaches of this policy as soon as they become aware of them.

3.   Making a reasonable attempt at validating and authenticating information retrieved from the Internet before it is used for educational purposes especially it is of a sensitive nature.

4.   Ensuring all information posted to or communicated via the Internet is accurate and has an appropriate level of authorization.

5.   Not sharing their password, user identification or other secure information.

6.   Not using unauthorized codes or passwords to gain access to other's files.
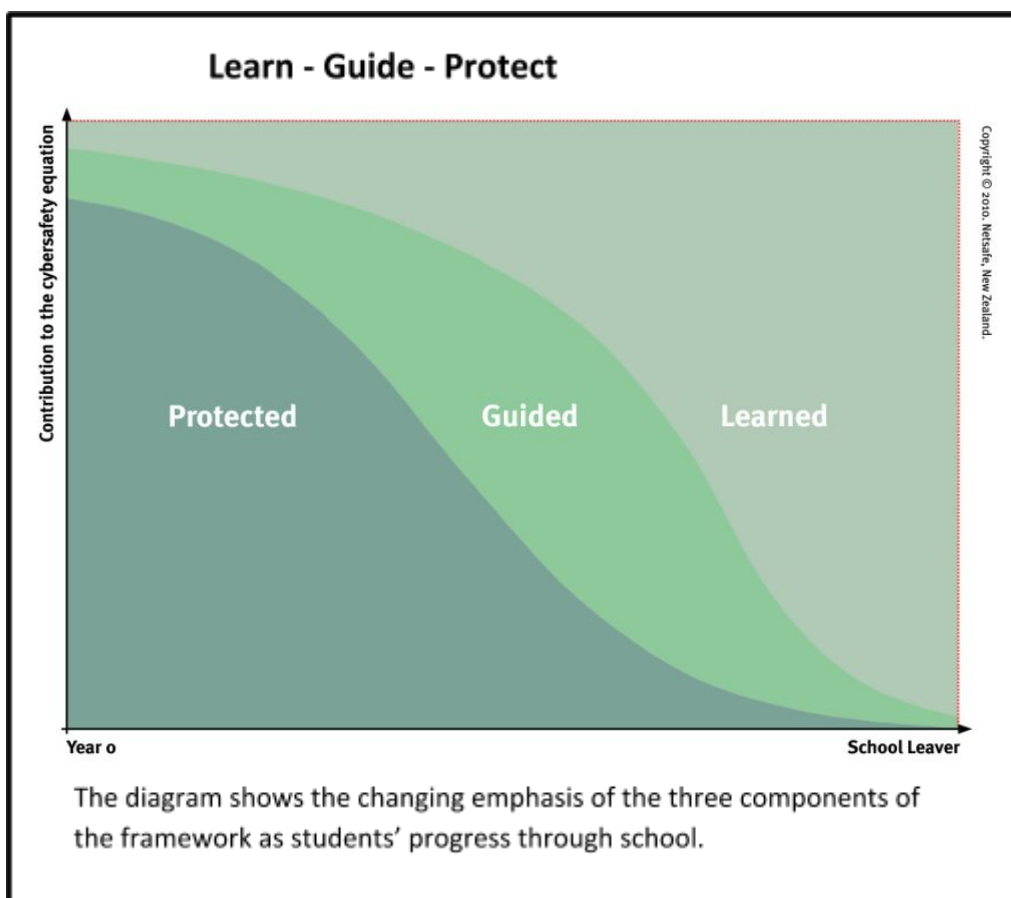
C   GENERAL
1   Any use of the Internet other than that specified here e.g. by custodial staff, staff or student's family, or use after hours, must be with the agreement of the ICT Coordinator and/or Principal and under supervision approved by that teacher.
2   The above 'Internet Safety Guidelines' will be clearly displayed on the wall of the computer room, and beside classroom computers.
3   All classroom computers will be monitored by IT service providers NRC, along with the Principal, ICT Coordinator and Technical Support. Internet Filtering will be provided by Internet Service Provider 'Watchdog'.
4   The school will continue to refine methods of improving safety on the Internet.

CONCLUSION

As a state school we strive to educate students to develop positive, ethical behaviours in cyberspace. We guide professional learning resources and lesson activities to teach digital citizenry and to create a positive school culture for digital citizenship. And we protect through technology, infrastructure and school policies that support the establishment of a safe and secure technology environment.

"Be the change that you wish to see in the world."
Mahatma Gandhi

The diagram shows the changing emphasis of the three components of the framework as students' progress through school.

STUDENT CYBERSAFETY AND INTERNET USE AGREEMENT

I understand that:

- The only purpose for school computers, mobile devices and other Information Technology resources is to support teaching and classroom learning.
- The school will do its best to keep me safe while using global information systems such as the computer and the Internet.
- I know that I am not permitted to access material through the Internet which is offensive (e.g. pornographic), dangerous, inappropriate at school, or illegal*
- I am forbidden to pass on such material by copying, storing or printing it.
- If my teacher requires me to use e-mail / messaging at school, I am not permitted to send any messages which are offensive, dangerous, inappropriate at school, or illegal*

* Students please ask your teacher if you need any of these terms explained to you.

I understand how important it is to:

1   Take care of Information Technology resources, such as computers, iPads, iPods and the Internet.
- Be careful with equipment and furniture
- Respect the copyrights on software that prohibit copying.
- Use only school software on school computers.

2   Be considerate of other users.
- Share available equipment
- Be careful not to waste computer resources e.g. paper.
- Avoid disruption of the running of any computer or network by adapting settings.
- Take care not to scan or display graphics, record or play sounds, or type messages which could cause offence to others or the people I am recording.
- Remove immediately from the screen any material that would not be allowed at the school which I accidentally come across, and tell the teacher right away.

3   Be responsible for privacy and security.
- I will not give anyone on the Internet information about myself or anyone else – this includes address, phone number, photographs or credit card information.
- I will use portable data storage only to backup and deliver work.
- I will tell the teacher immediately if I come across a virus or security problem.

4   Apps or other such programmes are not to be downloaded at school.

5   No mobile phones are to be brought to school.

STUDENT CYBERSAFETY AND INTERNET USE AGREEMENT

STUDENT

I have read this Agreement and know the importance of the school rules for the use of computers and the Internet.

I know that if I break these rules I will lose the right to use a school computer and the school may take other disciplinary action against me, which could include my removal from any course that involves computer use.

NAME   (please print clearly)   ROOM

SIGNATURE   DATE

PARENTS/CAREGIVERS

I have read this Agreement and understand that my child is responsible for using school equipment and the Internet as outlined here.

I have gone through the Agreement with my child and explained its importance and that there may be consequences for breaking the Agreement

I understand while the school will do its best to restrict student access to offensive, dangerous, inappropriate at school, or illegal material on the Internet or through e-mail, it is the responsibility of my child to have no involvement in such material.

I give my permission for _____ to be given access at school to global information systems such as the Internet or e-mail.

NAME   (please print clearly)

SIGNATURE   DATE

*   If you would like to discuss this document or need help with translation, please contact the school office.