

Glendowie School

Cybersafety 'Responsible Use'

Agreement for STUDENTS

Revised February 2022



1. Cybersafety 'Responsible Use' Agreement - INTRODUCTION

The school's computer network, internet access facilities, computers and other school IT equipment/devices bring great benefits to the teaching and learning programmes at Glendowie School and to the effective operation of the school. The measures to ensure the cybersafety of Glendowie School outlined in this document are based on our core values;

I Care, Respect, Integrity, Honesty and Responsibility.

Our school has rigorous cybersafety practices in place, which include 'Responsible Use' agreements for all school staff and students. The school monitors traffic and material sent and received, using the school's IT network. The school uses filtering and monitoring software to restrict access to certain sites and data, including email. The school may audit its computer network, internet access facilities, computers and other school IT equipment/devices or commission an independent forensic audit.

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. This document includes information about student obligations, responsibilities, and the nature of possible consequences associated with cybersafety breaches which undermine the safety of the school environment.

The school's computer network, internet access facilities, computers and other school IT equipment/devices are for educational purposes appropriate to the school environment. This applies whether the IT equipment is owned or leased either partially or wholly by the school, and used on or off the school site. This also applies to student owned devices when used on the school site.

All students will be familiar with the Cybersafety 'Responsible Use' Agreement and teachers will revisit this document with their students each year. Year 3 to Year 8 teachers will ensure rules are put in homework books at the beginning of each year.

Terms and definitions used in this document

IT	Sometimes called ICT, both refer to Information and Communication Technologies.
School IT	School IT, refers to the computer network, internet access facilities, computers and other school IT devices.
IT equipment or devices	This includes but not limited to, <ul style="list-style-type: none">• computers (ie desktops, laptops, netbooks, ipads or tablets),• storage devices (ie USB, flash memory devices, CD, DVD, iPads, MP3 players)• cameras (ie video, digital, webcams)• mobile phones, gaming consoles, video and audio players/receivers (ie portable CD & DVD players)• and any other similar technologies that may come into use eg robotics and coding/computational thinking equipment
e-learning	Learning and teaching that is facilitated by, or supported through the appropriate use of IT.
Cybersafety	Refers to the safe use of the internet, IT equipment/devices, including mobile phones.
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 is entered to be inclusive of the definition used in the Films, Videos and Publications classification Act 1993.
Parent	The term parent used throughout this document also refers to legal guardians and caregivers.
BYOD	Bring Your Own Device <i>(please note there is a school procedure for BYOD)</i>

2. Cybersafety 'Responsible Use' Agreement - RULES

As a safe and responsible user of IT, I will help keep myself and other people safe by following these rules:

I will:

- 1) **READ** the school Cybersafety 'Responsible Use' Agreement each year and follow the rules outlined.
- 2) **USE** the devices for school related work.
- 3) **ASK** the teacher first, if I am unsure whether I am allowed to do something involving IT.
- 4) **LOG ON**, only with my username (if I have my own username). I will not allow anyone else to use my username and I will log off correctly when I have finished.
- 5) **NOT TELL** anyone else my password - except my parents and teacher.
- 6) **ONLY** go online or access the internet at school, when a teacher gives permission and an adult is supervising. This includes lunchtimes, before and after school.
- 7) **NOT**, at any time, use the internet, blogs, email, mobile phones or any IT equipment to be mean, rude and offensive, to bully, harass, or in any way harm anyone else within or outside our school, or the school itself, even if it is meant as a 'joke'.
- 8) **NOT** attempt to search for things online I know are not acceptable at our school. This could include anything that is rude or violent or uses unacceptable language such as swearing.
- 9) **NOT** make any attempt to get around, or bypass, security, monitoring and filtering that is in place at our school.
- 10) **FOLLOW THE PROCEDURE BELOW** if I find anything objectionable, mean or rude or things I know are not acceptable at our school on any IT:
 - a) Not show others
 - b) Turn off the monitor
 - c) Get a teacher straight away
- 11) **NOT** download or copy any files such as music, videos, games or programmes without the permission of a teacher. This is to ensure we are following copyright laws.
- 12) **HAVE** permission from home before bringing in any device to school. This includes things like mobile phones, iPods, games, cameras, and USB drives. BYOD document must be signed by myself, parent(s) / caregiver(s) and the teacher before I can bring in the device.
- 13) **NOT** connect any device (such as a USB drive, camera or phone) to school IT or run any software without the teacher's knowledge. I understand that the teacher may or may not allow me to connect the device at his/her discretion. This includes to all wireless technologies.
- 14) **UNDERSTAND** that the school cybersafety rules apply to any personal devices brought to school like a mobile phone or a BYOD.
- 15) **NOT** share personal information, this includes knowing :
 - a) To **ONLY** use the first name for myself and others (no surnames) when publishing work or photos/videos online. To also get permission from any students visible in photos/videos first, incase they wish to say no.
 - b) I must get teacher's permission when emailing others outside the school for my learning. I know that I must always use my school email at school and NOT a personal email.
 - c) I must **NEVER** give out personal information of myself or others. This includes:
 - i) a full name,
 - ii) personal address or personal email address
 - iii) personal phone numbers
 - iv) photos.
- 16) **RESPECT** all school IT and will treat all equipment/devices with care. This includes:
 - a) Not intentionally disrupting the smooth running of any school IT systems
 - b) Not attempting to hack or gain unauthorised access to any system
 - c) Following all school cybersafety rules, not joining in if other students choose to be irresponsible with IT, and reporting irresponsible behaviour.
 - d) Reporting any breakages/damages, viruses or other problems to a staff member.
 - e) Ensuring my behaviour does not cause damage to any device within the school
- 17) **ACCEPT** that if I break these rules, the school may need to inform my parents. In serious cases the school may take disciplinary action against me and my family may be charged for repair costs.

3. Cybersafety 'Responsible Use' Agreement - READ & SIGN

Glendowie responsibilities include:

1. Enhancing learning with digital technologies through the safe use of IT. This includes working to restrict access to inappropriate, illegal or harmful material on the Internet or school IT equipment/devices at school, or at school-related activities.
2. Work progressively with children and their families to encourage and develop an understanding of the importance of cybersafety through education designed to complement and support the use agreement initiative. This includes providing children with strategies to keep themselves safe in Cyberspace.
3. Display these cybersafety rules for students to access.
4. Respond to any breaches in accordance with our Discipline Procedure and review procedures when required.
5. Welcome enquiries from parents or students about cybersafety issues.
6. Knowing the students who do not have permission to publish their images or first name online, and implement procedures to ensure teachers and others are aware of this.

Student responsibilities include:

1. To become familiar with this Cybersafety 'Responsible Use' Agreement and follow the rules.
2. To talk with an adult if they have any questions or concerns about keeping themselves cybersafe.

Parent responsibilities include:

1. To become familiar with this cybersafety document and to discuss the information with their child, explaining why it is important.
2. Supporting the school's cybersafety programme by encouraging their child to follow the cybersafety rules, and to always ask the teacher if their child is unsure about any use of IT.
3. Contacting the Principal, teacher or IT teacher, to discuss any questions or concerns about cybersafety.

I have acknowledged I have read the Cybersafety 'Responsible Use' Agreement and understand the rules.

Student Name:	
Student Signature:	
Room:	

Parent/Caregiver name:	
Signature:	
Date:	

Additional information can be found on the NetSafe website www.netsafe.org.nz