

CYBERSAFETY AT Taradale Intermediate School

CYBERSAFETY USE AGREEMENT YEAR 7- 8 STUDENTS TIS



The document is comprised of this cover page and two sections:

Section A

- The Role of Use Agreements in the Taradale Intermediate School Cybersafety Programme
- Cybersafety Rules for Year 7 - 8 Students, including explanatory notes for Parents*/Legal Guardians/Caregivers

Section B

- Cybersafety Use Agreement Form is in the STUDENT DIARY – “Licence to use the Internet”
-

Instructions for Parents*/Legal Guardians/Caregivers

1. Read Sections A and B carefully. If help is needed to understand all the language, or there are any points you would like to discuss with the school, let the school office know as soon as possible.
2. Discuss the Cybersafety Rules for Year 7 - 8 Students with your child.
3. **Both you and your child should sign the Use Agreement in the STUDENT DIARY and this will be checked by your child’s teacher. No access to ICT devices will be permitted until this agreement is signed.**
4. Please keep this Booklet for future reference.

* The term ‘Parent’ used throughout this document also refers to legal guardians and caregivers.

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, video and audio players/receivers (such as portable CD and DVD players), and any other, similar, technologies as they come into use.
 - (e) A Staff ICT Management Team (including the principal) will take responsibility for ICT development across the school. Technical issues will be managed by the ICT Manager (technician) with support from the Management Team.
-

SECTION A – CYBERSAFETY AND THE SCHOOL COMMUNITY

- THE ROLE OF USE AGREEMENTS IN THE TARADALE INTERMEDIATE SCHOOL CYBERSAFETY PROGRAMME -

The values promoted by Taradale Intermediate School include Caring, Sharing and Daring through 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 Taradale Intermediate School, 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 Taradale Intermediate 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 school environment. 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 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 Principal.)
- 1.3. The school encourages anyone with a query about the agreement to contact the Principal 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, 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 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 principal.

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. Taradale Intermediate School has an electronic access monitoring system which has the capability to record Internet use, including the user details and sites visited.
- 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 cybersafe 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

- 4.1. The school 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. The school 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. 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 keep children, young people and adults cybersafe in all areas of their lives. If more information is required the Principal can be contacted.

- CYBERSAFETY RULES FOR YEAR 7 - 8 STUDENTS -

Note for Parents/Legal Guardians/Caregivers:

The sections marked **i** are designed to provide a guide to the rules covered by this use agreement, and to help you discuss the rules with your child.

Teachers will also go over this section with students.

The meaning of 'ICT' or 'ICT equipment/devices' can be found on page one.

- 1. I must have a use agreement signed by me and by my parent or caregiver before I am allowed to use the school ICT equipment.**

i All students, regardless of age or ability, must have a use agreement signed by their parent. Year 7 - 8 Students sign their use agreements along with their parents. Use agreements are becoming accepted as an essential part of cybersafety policy and programmes for schools and other organisations, including businesses.

- 2. I can use the school computers and other school ICT only for school work.**

i This helps to ensure the equipment is available when students need to use it for their learning. It will also help to reduce the likelihood of any inappropriate activities taking place which put at risk the safety of the learning environment.

- 3. If I am unsure whether I am allowed to do something involving ICT, I will ask the teacher first.**

i This helps children and young people to take responsibility for their own actions, and seek advice when they are unsure of what to do. It provides an opportunity for the teacher and student to work through an issue and so avoid the student making an unwise decision which could possibly lead to serious consequences. Young children need ongoing advice and guidance to help them become safe and responsible users of ICT.

- 4. I will follow the cybersafety rules, and will not join in if others are being irresponsible.**

i Unfortunately, along with many benefits, technology has also provided new ways to carry out anti-social activities. Bullying and harassment by text message, for example, is becoming a major problem in New Zealand and in many other countries. Often children become involved in these acts through peer pressure, without thinking of the consequences.

- 5. If I accidentally come across mean, or rude, or dangerous material I will tell the teacher straight away, without showing any other students.**

i Because anyone at all can publish material on the Internet, it does contain material which is inappropriate, and in some cases illegal. The school has taken a number of steps to prevent this material from being accessed. However, there always remains the possibility that a student may inadvertently stumble across something inappropriate. Encouraging students to tell a teacher immediately if they find something which they suspect may be inappropriate, encourages critical thinking and helps children to take responsibility for their actions and keep themselves, and others, safe. This way, they contribute to the cybersafety of the school community.

- 6. If I am not feeling safe at any time while using the ICT equipment, I will tell the teacher straight away.**

i Taradale Intermediate School strives to create a safe and secure learning environment for all members of the school community. Examples of situations involving the use of ICT which might cause a child to feel unsafe could include: contact being made by a stranger through email or text message, the presence of 'scary' images on a computer screen, and/or misconduct by other students. Staff need to be made aware of such situations as soon as they occur to ensure the school can respond immediately.

- 7. If I have my own password, I will log on only with that password.**

- 8. I will not share my password with any other person.**

i Passwords perform two main functions. Firstly, they help to ensure only approved persons can access the school ICT facilities. Secondly, they are used to track how those facilities are used. Knowing how the equipment is being used and by whom, helps the school to maintain a cybersafe environment for all users, and teaches the child the importance of personal security.

- 9. I will log off or shut down the computer when I have finished using it.**

- 10. I will log off before letting someone else use the computer.**

i Logging off or shutting down, stops others from using a computer under your child's username. When the computer is started up again, the next user has to enter their own details to log on.

- 11. If I am sharing a computer which is logged on under my name, I am responsible for how it is used. If there is a problem, I will tell the teacher immediately.**

i Students often work together at a single computer. Any misuse of the computer can be traced back to whoever was logged on at the time. It is important that your child takes responsibility for sensible use of the computer at all times, and tells the teacher if there is any concern.

- 12. I will check with the teacher before giving anyone information about myself or others when using the Internet or a mobile phone – this includes home and email addresses, and phone numbers.**

i This reduces the risk of your child, or other children, being contacted by someone who wishes to upset or harm them, or use their identity for purposes which might compromise the child's privacy or security online.

- 13. I will not be careless, try to damage, or steal any school ICT equipment. (If this happens, the school will need to inform my family about what has happened. My family may have responsibility for the cost of repairs or replacement.)**

- 14. I will not try to stop the network or any other equipment from working properly.**

15. If I accidentally break something, or I find it broken when I start to use it, I will tell a teacher straight away.

16. I will ask the teacher before changing screensavers, desktop backgrounds, themes or hardware settings.

17. I will have no involvement with making or sending viruses (such as worms) on purpose.

18. I will not print anything without the permission of the teacher.

i Rules 12-18 are designed to help protect the investment the school has made in expensive ICT technologies. Also, certain settings may have been applied to maximise the safety of the students and the equipment (such as antivirus settings or restrictions on Internet access).

19. I will not download any files such as music, videos, or programmes without the permission of the teacher, even if they are for school work. If I am unsure, I will ask the teacher first.

i Many files available on the Internet are covered by copyright, and although they can be easily downloaded, it may be illegal to do so. Sometimes even innocent-looking files may contain malicious content such as viruses, or spyware (software that searches for personal information from your computer and transmits it to others over the Internet). As well, some files may contain inappropriate or illegal material.

20. I must have a letter from home, and permission from school, before bringing any disk or other ICT device from home, unless it is part of my normal school equipment. If I am given permission, then I must use that ICT sensibly.

i The devices referred to in this rule include those specified on page one of this document; for example flash memory devices, iPods, MP3 players or mobile phones. Any students bringing such devices from home are asked to use them sensibly. This applies to the school site, and any school-related activity.

NB Parents should be mindful of the school's specific policy regarding students and mobile phones.

You might like to take this opportunity to have a discussion with your child about their general use of ICT whether in or out of school. It helps keep children cybersafe if they understand that many of these rules should be followed regardless of whose ICT equipment they are using, where they are (for example at home, at school, or at a friend's house), or who they are with.

21. I will ask the teacher to check any disk or ICT device (including all disks, memory storage devices, media players, cameras and mobile phones) I bring from home, before I use it with school equipment.

i This rule is designed to protect the school's online security and equipment from viruses which can easily be transferred using disks or other storage devices such as pen drives or memory cards. If your child is using a disk or other device to transfer work between home and school, it should be freshly formatted, or 'blank', before use. This may also stop any of your own personal material from finding its way onto the school's equipment. Even though every effort is made to keep school equipment virus-free, you should scan your child's disk or device for viruses before they use it again with your home computer.

22. I will not bring software or games from outside school to use on school equipment.

i Installing software from home may cause conflicts with the software installed by the school. Taradale Intermediate School must also abide by any licensing requirements included within the software. This means that unless the school has purchased a copy, it will not usually be legally entitled to install the software. And as mentioned in point 19, inappropriate or illegal content may be involved.

23. I will acknowledge where work has come from if I have copied it from somewhere. This includes graphics and sounds files I use in my own schoolwork.

i The Internet has allowed easy access to a huge range of information which can be incorporated into students' work by simply cutting and pasting. Most of this material is copyrighted, and thus involves intellectual property issues. Also, the value to students' learning is questionable if they have not thought through this information themselves.

24. I will check with the teacher before using school equipment to copy software, music, videos or other files, in case they are copyrighted.

i Any such copying is likely to be restricted by copyright laws. Taradale Intermediate School cannot condone the use of its equipment for these activities.

25. I will not use the internet, mobile phones or any other ICT equipment to be mean, rude, offensive, or to harass any members of the school community like students and staff, while at school or any school-related activity. The same rule applies when using school ICT at any time, whether at school or not.

i The basic principles of politeness and respect extend to the use of information and communication technologies.

The capacity of ICT to increase the scale and scope of misconduct can make an otherwise minor rule infringement into a much more serious matter. For example, name calling often becomes a more serious issue where texting or emailing has been used to facilitate harassment. Cyberbullying can involve a range of misconduct including the creation of abusive websites..

26. If I break these rules, the school may need to talk to my family about what has happened. In very serious cases, the school may take disciplinary action.

i Depending on the seriousness of a particular breach, possible school responses could include one or more of the following: a discussion with the student, informing parents, loss of ICT privileges, the family possibly having responsibility for the cost of ICT repairs or replacement, the school taking disciplinary action

Warning re Bebo / Facebook and the Internet Do you have safe practice protocols in place at home for your child's access to the internet? Have you checked lately? Have you explored the history file? Is your computer controlled by your password? We are hearing some scary things that children are getting up to – using places like Bebo to post nasty things about other children. You have heard of recent happenings in NZ and Australia – I am sure we are not far from seeing the same kind of thing in our community. **BE WARNED, BE AWARE!**



From the NetSafe newsletter

www.netsafe.org.nz - a sit well worth checking out.

NetSafe Newsletter

Social Networking - Is Your Child Doing It Too?

For many young people using social networking sites, their online life is as important to them as their offline life. Read on to find out about this latest online trend for young people.

Increasingly young people are spending significant amounts of time online in websites designed for social networking. MySpace.com, Bebo.com and Facebook.com for example, are websites which provide users with the ability to produce their own webpage, which can also display comments posted by others. While many young people seem to enjoy using these sites, there are some significant risks.

One of those risks has received recent media attention when MySpace.com was used by a child sex offender making contact with and grooming a young person for sexual abuse. Further risks include:

- online bullying and harassment using text and photos
- young people using the sites to express serious concerns like suicide and not getting the proper professional help needed
- easy access to anti-social networks (hate groups, pro anorexia or pro drug use networks) which can normalise inappropriate attitudes, beliefs and behaviours
- the harvesting of personal or family information by burglars and other offenders.

In addition to this, there are often risks when a young person's online relationship/friendship moves very swiftly, especially when both parties may not have accurate information about each other.

Recent international research conducted by the USA based Centre for Missing and Exploited Children and Cox Communications, found that when parents and guardians talk to their teens about Internet safety, their exposure to potential threats decline and they make safer online decisions. This research highlights the importance for caregivers to talk with children and young people about social networking and other online activities to help them to better navigate the risks present.

For more information on talking with your child about online risks take a look at Nathan Gaunt's article '**Of Cyber Birds and Digital Bees**' and Lee Chisholm and John Fenaughty's article '**My Online Life**' in the 'Articles' section of the **NetSafe website**. You can also contact the NetSafe contact centre on 0508 638 723 for further information.

THE INTERNET TODAY

Who could have predicted that a communications system designed to serve scientists and the military would one day help Aunt Sylvia uncover a blue-ribbon cake recipe or help you track down your favorite high-school classmate?

The Internet is an unprecedented gateway to a vast wealth of knowledge and information, and its uses are virtually unlimited. The World Wide Web, although still young, is deeply ingrained in our culture and everyday lives. It's a source of news, facts, and figures; a communication tool that allows millions of us to connect with each other every second of every day; a way to bank, invest, and shop; and an educational and entertainment medium that allows people from all walks of life to learn about the world and have fun doing it.

A Resource for Children

Especially promising are the marvelous advantages that the Internet offers children, including access to educational materials, publications, online friendships, pen pals, subject-matter experts, and information on hobbies, games, and sports. There's no question that many of today's kids benefit enormously from online access—often in ways different from their parents' use of it.

A Darker Side

As indispensable as it is in today's society, however, the Internet is also a reflection of society, good and bad. The easy access to information that makes the Web so special is also at the root of parental and community concerns about children's exposure to inappropriate materials and experiences. Real-world threats like hate speech, religious cults, harassment, and stalking exist in cyberspace. Particularly alarming for many parents are pornography and sexual predators—issues that led to the preparation of Youth, Pornography, and the Internet, the National Academies report on which NetSafeKids.org is based.

It's easy for a parent to think, "Maybe I'll just keep my kids offline entirely." This might be the best guarantee for safety, but is it a practical solution? Children can access the Internet from a number of places outside of the home. In addition, the Internet is such a helpful educational resource that denying children access to it could put them at a disadvantage as they prepare for their own future.

Knowledge Is Power

Whoever said "Ignorance is bliss" probably never raised a child. Parents, ever vigilant, sometimes feel helpless when it comes to guiding their children's Internet use. Yes, it's likely that your kids are more Internet-savvy than you, but that shouldn't interfere with your parenting goals. Don't be intimidated by the apparent complexity of the Web; it's easier to understand than you think. Nevertheless, to prevent problems and still help kids get the most out of the Web, you must understand the threats, learn how unacceptable materials and dangerous people travel on the Web, and plan a strategy to protect your children.

HOW CAN I PROTECT MY CHILD?

You might feel overwhelmed by the idea of trying to protect your kids from something as big, and perhaps unfamiliar, as the Internet. But there are real—and manageable—steps you can take to help your children stay safe.

This section offers parents background information on topics involving Internet guidance and safety—from understanding the maturity level of a child to tips on screening and monitoring content to dealing with an incident of exposure to pornography or predation. You'll also learn how schools, libraries, and other community groups might help contribute to children's Internet safety.

Remember:

Although there's no single answer and certainly no quick-fix solution, there's one critical element in the protection game: the presence of a responsible parent or adult. In their Internet use, as in all areas of life, children need adults to guide them and to intervene when necessary. Even if you can't always be there to supervise your children's online activities, you can still teach them how to use the Internet wisely when they're on their own.

Keep in Mind That Your Efforts Are Likely to Be More Successful If You:

Maintain an open dialogue with your child.

Don't play the blame game, but instead encourage open, honest discussion about what a child has seen or done on the Web.

Respect children's concerns or frustrations over your involvement in their surfing activities.

Balance your concerns about exposure to inappropriate or harmful things on the Internet against the benefits gained from exposure to positive things on the Internet.

[back to top](#)

**After reading and discussing this
Cybersafety Agreement please sign the
Licence page in the Student Diary.**

**Please note that while the heading
states Internet Licence it does apply to
all ICT use and equipment used in the
school environment.**

**This agreement must be signed before
a child is given access to ICT
resources and equipment.**