February 2005 update: Copyrighted NetSafe® Sample Cybersafety Use Agreements
FOR YEAR 0-3 STUDENTS

(Note that use agreements for students at year levels 4-8 and 9-13 are on two separate documents)

The Internet Safety Group (ISG) would like to thank those key agencies and professional bodies which took part in the extensive consultation process central to the development of these updated NetSafe® use agreements for schools, as well as express much appreciation for the time and expertise kindly contributed by individual ICT and legal specialists.

Comprehensive use agreements play a vital role in developing an effective school cybersafety programme which helps the school maintain a safe physical and emotional learning environment. The ISG's NetSafe® model for a school cybersafety programme is detailed in the 2003 *NetSafe Kit for Schools*, and is endorsed by the Ministry of Education, the New Zealand Police, and other agencies.

This model focuses on a '3-legged stool' comprising of:
   (a) an infrastructure of policies, procedures and signed use agreements, which are rigorously enforced
   (b) an effective electronic security system
   (c) a comprehensive cybersafety education programme for the school community.   (This education programme includes information and resources, such as NetSafe brochures and posters for staff, students and parents, as well as ongoing school professional development, such as attendance of key personnel at the NetSafe® Training Modules.)

The updating of the 2003 kit use agreements has been necessary in order to help schools address cybersafety and security issues and incidents about which schools need to set clear and appropriate guidelines. The focus of these issues and incidents includes the variety and proliferation of ICT equipment/devices present in schools, the use made of privately-owned ICT on the school site and at school-related activities, and the need for the school community to be aware of what constitutes appropriate use of school ICT. The use of mobile phones can also be of concern. As noted in the paragraph above, it is important that information and education about these matters is provided for all members of the school community. For this reason, the updated use agreements include comprehensive information on obligations and responsibilities, as well as valuable educative material, which staff, and students/parents, are encouraged to refer to as an ongoing guide to the appropriate use of ICT at your school. By providing information on cybersafety initiatives taken by the school, as well as the school's expectations of staff, students and their parents, the use agreements emphasise the role played by *the whole school community* in the maintenance of a cybersafe school environment.

As a New Zealand school, you are invited to modify and personalise this copyrighted NetSafe® document. Your Cybersafety Team should be tasked with customising this use agreement, and organising the process by which it is put into place. This would include:

- modifying the appropriate information within the [square brackets]
- ensuring the agreements are consistent with your own school values, and with your individual circumstances, policies and protocols, including those related to networking capabilities, electronic monitoring systems, and access protocols
- deciding which use agreement (year levels '0-3', or '4-8') is more appropriate for a particular year level, class or individual student. (Although the two use agreements are designated 0-3 and 4-8, it is as a guide only. The school is free to adjust the range of year levels covered under each agreement, to fit individual situations and requirements; this may require a change of title e.g. '0-3' may become 0-4')
- deciding whether it is appropriate for students at some or all levels covered by this 0-3 use agreement, to sign the agreement form themselves. (The year 4-8 agreement form could be used as a template)
- ensuring parents receive a photocopy of the signed use agreement form on the last page
- retaining the default footer on the use agreement pages, as requested by the ISG
- checking that in the event of concern about a particular circumstance, specific advice is obtained
- instructing staff to endeavour to check that all students in their care understand the requirements of the student use agreement
- developing additional safety procedures/rules if the school has involvement in distance learning, a boarding facility, or is in any other situation involving a wider responsibility for the provision of a cybersafe environment. This includes schools which offer students remote access to the school network
- scheduling an annual review by the Cybersafety Team of the school's cybersafety programme, in addition to a review held following any cybersafety incident of significance. A review should include checking the NetSafe website (www.netsafe.org.nz) for updated documents, information and resources.

CYBERSAFETY AT

PUKEPOTO SCHOOL

CYBERSAFETY USE AGREEMENT
YEAR 0-3 STUDENTS
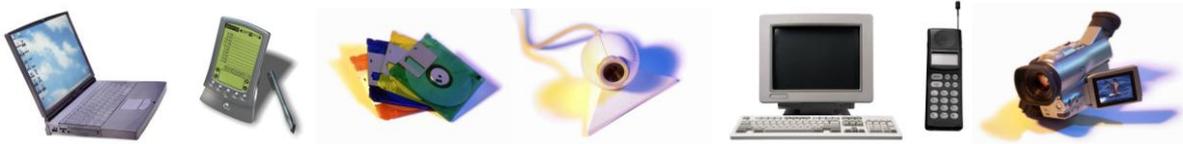
The document is comprised of this cover page and two sections:

Section A
- The Role of Use Agreements in the Pukepoto School Cybersafety Programme
- Cybersafety Rules for Year 0-3 Students, including explanatory notes for Parents*/Legal Guardians/Caregivers

Section B
- Cybersafety Use Agreement Form

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 0-3 Students with your child.
3. Sign the Use Agreement (Section B) and return that page to the school office.
4. Please keep Section A 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.

- *THE ROLE OF USE AGREEMENTS IN THE PUKEPOTO SCHOOL CYBERSAFETY PROGRAMME -*

The values promoted by Pukepoto School 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 Pukepoto School and to the effective operation of the school. (Examples of what is meant by 'ICT equipment/devices' can be found on the cover page.) However, it is essential that the school endeavours to ensure the safe use of ICT within the school community.

Thus Pukepoto 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 and 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 help keep the school community cybersafe by creating and maintaining a cybersafety culture which is in keeping with the values of the school, as well as 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.

Some of the information in this section is less likely to apply to young children while at school, however it is helpful for parents to be aware of the scope of this important, school-wide, cybersafety initiative. It also provides parents with valuable educative material to assist them in their efforts to keep their children cybersafe.

1. **Cybersafety use agreements**

   1.1. All staff and students, whether or not they presently make use of school ICT, will be issued with a use agreement. Parents 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.

   1.2. Parents 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. The school encourages anyone with a query about the agreement to contact the Cybersafety Manager or 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 ICT Manager, or with the Cybersafety Manager. For students, it is appropriate they check with their teacher.

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. Pukepoto School 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. 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 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 0-3 STUDENTS -

Note for Parents/Legal Guardians/Caregivers:

The sections marked 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 know I cannot use the school ICT equipment until my use agreement has been signed by my parent or the adult who looks after me.**

   All students, regardless of age or ability, must have a use agreement signed by their parent. Year 4-8 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.**

   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.**

   This helps children 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 child to work through an issue, and so avoid the child 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 not use ICT to do anything naughty, unkind, or dangerous, even if my friends are doing it.**

   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 find mean or rude or dangerous things on the computer or any other ICT equipment, I will tell the teacher straight away, without showing any other children.**

   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 the student 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.**

   Pukepoto 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 tell my password to anyone.**

   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.**

   Logging off or shutting down, stops others from using a computer under your child's username.

10. **If I am sharing a computer that I have logged on to, I am responsible for how it is used. I will tell the teacher straight away if there is a problem.**

    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 his/her own sensible use of the computer at all times, and tells the teacher if there is any concern.

11. **I will not tell anyone things like my name, home/email address or telephone number, or anyone else's, when using the Internet or a mobile phone, unless the teacher says it is okay.**

    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.

12. **I will be careful with school ICT equipment, and not play around with it.**

13. **If I have anything to do with damaging, losing or stealing school ICT equipment, the school may need to talk to my family about what should happen.**

14. **I will ask the teacher before changing any settings like screensavers or backgrounds.**

15. **I will tell a teacher if I break or damage any equipment.**

16. **I will tell a teacher if I find something broken when I start to use it.**

17. **I will have nothing to do with making or sending viruses (such as worms) on purpose.**

18. **I will ask a teacher before printing anything.**

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 or programmes (such as games or music) without the teacher's permission.**

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.**

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. NB Parents should be mindful of the school's specific policy regarding students and mobile phones on the school site, and at school-related activities. Any students bringing such devices from home are also asked to use them sensibly.

You could 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 I bring from home (including all disks, memory storage devices, media players, cameras and mobile phones), before I use it with school equipment.**

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 copy something somebody else made or wrote, and pretend it is mine.**

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 the information themselves.

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

Installing software from home may cause conflicts with the software installed by the school. Pukepoto 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.

24. **I will not use school equipment to copy any music, videos, or programmes.**

Any such copying is likely to be restricted by copyright laws. Pukepoto 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, or annoying to, or about, any other person in the school community, like students or staff.**

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, my family may have to be told, and there might be consequences.**

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.

5

SECTION B –PUKEPOTO SCHOOL CYBERSAFETY USE AGREEMENT FOR YEAR 0–3 STUDENTS

To the Parent/Legal Guardian/Caregiver:

1. Please read this page carefully as it includes information about your responsibilities under this agreement.
2. Complete and sign the bottom of the page.
3. Detach and return this section to the school office (a copy will be returned to you).
4. Keep **Section A** for your future reference.

Pukepoto School will:

- do its best to enhance learning through the safe use of ICT. This includes working to restrict access to inappropriate, illegal or harmful material on the Internet or school ICT equipment/devices at school or at school-related activities

- work 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 help keep themselves safe in cyberspace

- keep a copy of this signed use agreement form on file

- respond to any breaches in an appropriate manner

- welcome enquiries from parents or students about cybersafety issues.

My responsibilities include:

- **I will read** this School Cybersafety Use Agreement document carefully

- **I will go over** the information with my child and explain why it is important

- **I will ensure** this use agreement is signed by me, and returned to the school, so my child may make use of these important technologies

- **I will retain** Section A for future reference

- **I will support** the school's cybersafety programme by encouraging my child to follow the cybersafety rules, and to always ask the teacher if they are unsure about any use of ICT

- **I will contact** the Principal to discuss any aspect of this use agreement which I might want to learn more about. I know I am welcome to do this at any time.

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.

Name of student: .... **Room:** ....

My Name: ....

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

Signature: .... **Date:** ....