



RANGIORA NEW LIFE SCHOOL

POLICY AND PROCEDURES MANUAL

Providing quality Christian education that equips and inspires all students to reach their life potential in order to serve God's purposes.

Policy 5.3	Health and Safety	Cyber Safety	
Ratification	September 2008	Chairperson	
Last Review	February 2005	Chairperson	

RATIONALE / BIBLICAL MANDATE

This policy is designed to meet the school's statutory obligations to maintain a safe learning environment and to consult with the community. As well, the Board is aware of its responsibilities to be a good employer. The overall goal is to maximise the educational benefits of communication technologies while minimising the risks.

Use of the Internet and other communication technologies at Rangiora New Life School is to be limited to educational and personal usage appropriate in the school environment. Appropriate use also includes staff professional development.

'Other communication technologies' include the mobile phone and technologies associated with Internet use e.g. digital camera and web camera. Included too, are similar technologies still being developed.

The communication technologies at Rangiora New Life School are available to staff and students under certain conditions, as outlined in their signed User Agreements. The school will make basic training available for staff using these technologies. Associated professional development needs will be considered.

Appropriate Cybersafety measures will be put in place and enforced by the school. In order to ensure the safety of the school learning environment, action should be taken if these safety regulations are breached by students or staff.

This Cybersafety Policy applies to all employees of the Board (i.e. teaching, support and ancillary staff) and to all students. It also applies to teacher and other professional trainees assigned to the school from time to time, relief teachers, and staff and students in the Community Education programme.

The Principal will report regularly to the Board on the school implementation of this Board policy.

GUIDELINES

1. All students must read and sign a Computing / Cybersafety Use Agreement. The agreement must also be signed by a parent/caregiver.
2. Students will be supervised while using school facilities; the degree and type of that supervision may vary, dependent on the type of technology concerned, where the equipment is physically situated and whether or not the activity is occurring in the classroom.
3. All staff must sign a Cybersafety Use Agreement which includes details of their professional responsibilities and the limits to their own use of the Internet.
4. Educational material on Cybersafety will be provided by management to staff and students, and to parents/caregivers. As well, additional safety education will be delivered, where relevant, through teaching programmes.
5. Basic training for staff will be made available by management, as will appropriate professional development.
6. The necessary procedures will be put into place by the school to address Cybersafety issues in all venues where the Internet and other communication technologies are accessed by staff or students.
7. The school will provide an effective electronic security system, which is financially practicable. The school will continue to refine methods to improve Cybersafety.
8. The Principal will be responsible for the establishment and regular monitoring of a Cybersafety programme in the school. (The Principal may well delegate that responsibility to a member of the Senior Management Team.)
9. The Board supports the right of the school to check communication technology-related work or data of staff or students at any time, and to carry out a comprehensive investigation of any breaches of the school's Cybersafety policies. Such breaches will be taken seriously and be dealt with through the school's disciplinary and support systems. In such incidents, there will be special attention paid to the need for specific procedures as regards the gathering of evidence. If illegal material or activities are suspected, the matter will be reported to the Police or the Department of Internal Affairs Censorship Compliance.
10. The school will consult with the wider school community and provide opportunities to learn about Cybersafety issues e.g. through Parent Information Evenings.

RANGIORA NEW LIFE SCHOOL CYBERSAFETY MANAGEMENT GUIDELINES

The purpose of these Management Guidelines is to complement Rangiora New Life School's Board Cybersafety Policy by providing the necessary details to put into effect the Board's policy. It should be read in conjunction with that Board policy. The overall goal is to maximise the educational benefits of communication technologies and minimise the risks.

This Management Policy applies to all employees of the Board (i.e. teaching, support and ancillary staff) and all students. It also applies to teacher and other professional trainees assigned to the school from time to time, and staff and students in the Community Education programme.

Use of the Internet and other communication technologies at Rangiora New Life School is at all times to be limited to educational and personal usage appropriate in the school environment. Appropriate use also includes staff professional development.

'Other communication technologies' include the mobile phone and technologies associated with Internet use e.g. digital camera and web cam. Included, too, are similar technologies still in development.

Where communication technologies are used in places other than specialised rooms, specific cybersafety procedures are required there as well; where needed these should be documented and publicised appropriately.

The school reserves the right to check communication technology-related work or data of staff or students at any time, and to carry out a comprehensive investigation of any breaches of the school's Cybersafety Policies. Breaches of the Rangiora New Life School Cybersafety Policies will be treated seriously. Significant breaches could put at risk a student's place at the school, or the employment of a staff member and may also involve reporting the incident to law enforcement. The maintenance of the physical and emotional safety of the learning environment is of paramount concern.

Details

1. On enrolment, all **students** must read and sign the Rangiora New Life School Computing / Cybersafety Use Agreement. This Agreement outlines the regulations and conditions under which computers and communication technologies may be used at school or in any way which affects the safety of the school learning environment. This Use Agreement must also be signed by a parent/caregiver, and is to be handed in to the office where it will be filed. Information is available whereby classroom teachers can access the names of any students who have a signed Use Agreement.

Cybersafety rules and information will be given to the students to retain for future reference. Additional educational information will be provided by the Cybersafety Team e.g. posters and information in school homework diaries.

- 3 At the commencement of their employment, **all Board employees** (teachers, support and ancillary staff, including the caretaker, gardener and such personnel as Teacher Trainees and Relief Teachers) must sign the Rangiora New Life School Cybersafety Use Agreement. For staff working with students, this Agreement includes details of their responsibilities to actively supervise/monitor student Internet use and report any breaches of the Cybersafety Policies to the school Cybersafety Officer. This agreement also informs staff of the limits to their own use of the Internet, and of privacy issues associated with confidential information on the school network. Accompanying cybersafety rules and information should be retained by staff for future reference.
- 4 As some Internet-accessible computers are in the care of subject departments /syndicates, the **Heads of Department** are responsible for departmental/syndicate cybersafety procedures to cover their particular situation if required. This information should be written in the form of a safety policy, disseminated to all relevant staff and students and a copy lodged with the school Cybersafety Officer.
5. Basic **training for staff** in Cybersafety issues and procedures will be addressed by the Cybersafety Team, as will professional development requirements. There will be a special focus on the skills/training of the ICT Manager. Other specific areas which may need to be addressed include the management of the school's website.
6. Any **breaches of Cybersafety** regulations (by staff or students) should be reported to the CO. This includes misconduct facilitated by the use of communication technologies e.g. harassment. Less serious matters should be documented and reported to the CO at a convenient moment.

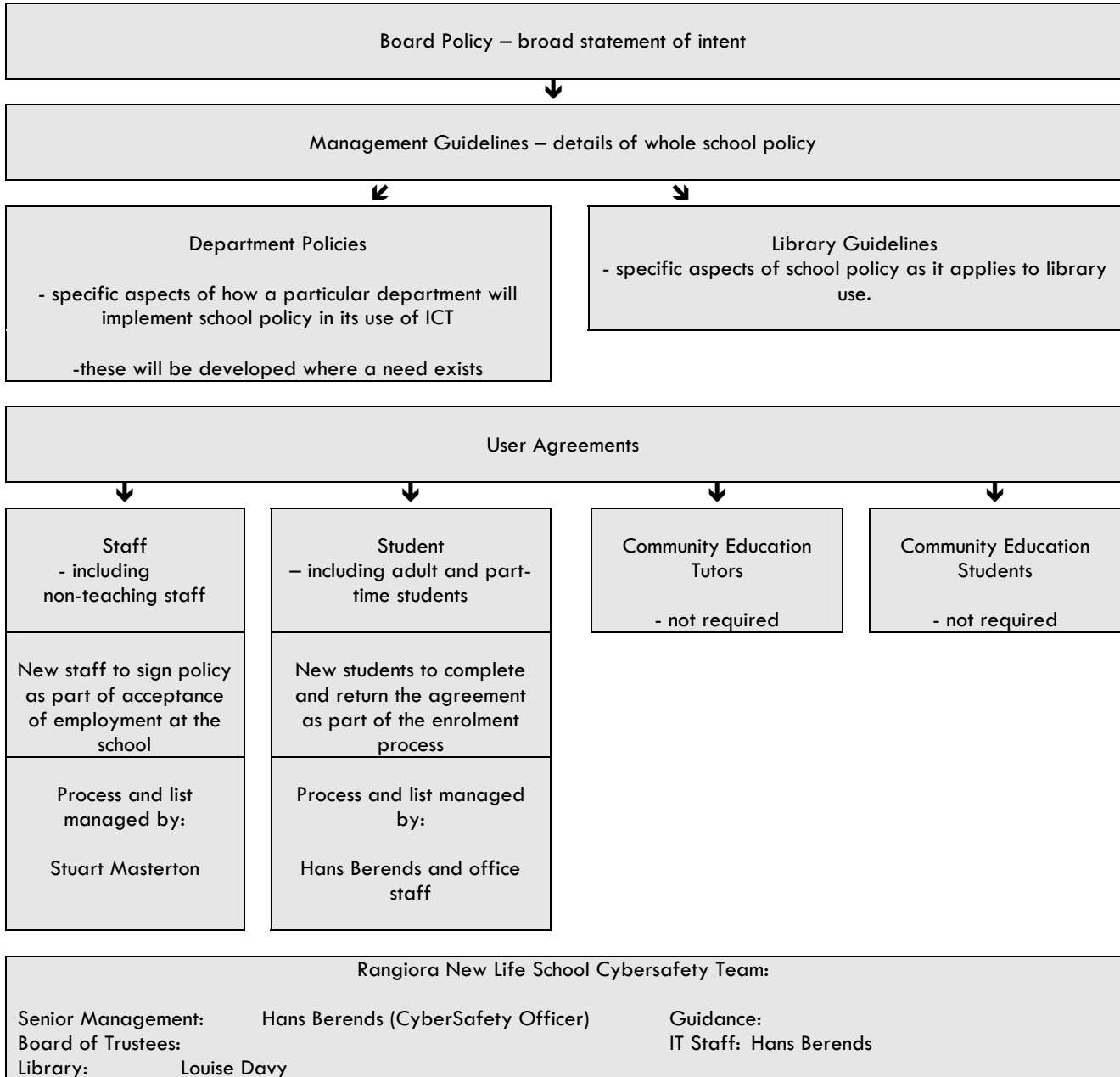
If the matter appears to be serious, that report should be made immediately. If the CO is not available, the report should be made to another member of the Senior Management Team or directly to the Principal. The matter will then be dealt with according to the school's usual disciplinary procedures (including the need to provide counselling and support), with a special focus on Cybersafety issues. The latter could include the vital preservation of the evidentiary trail, appropriate documentation and external consultation. If illegal material or activities are suspected, law enforcement must be informed as soon as possible. In such a case, the Board would also be informed and legal advice would be sought as specified in the school's Cybersafety Protocol for Incidents of Serious Misuse.

7. **Classroom teachers** should be aware of their responsibility to maintain Cybersafety in their classroom. This will include reminding students of Cybersafety rules before starting any unit of work involving use of the Internet or other communication technology, actively supervising student use and checking that the siting of Internet-accessible computers takes into account safety issues. Classroom teachers can help their students develop the skill base to effectively use the Internet as a learning tool. Appropriate preparation for lessons which make use of the Internet can prevent potential problems e.g. a list of suggested sites to visit can keep students on task and avoid conflicts with any filtering system.
8. **Parents/caregivers** will be consulted as part of the school's cybersafety education programme, and offered the opportunity to learn more about Cybersafety.
9. The school will endeavour to keep up to date on Cybersafety issues as they impact on the safety of the school learning environment.

Rangiora New Life School Cybersafety Overview

All policies and agreements in this overview follow closely those recommended by the Internet Safety Group Netsafe. Netsafe is supported by the NZ Police and the Ministry of Education. The Education Review Office (ERO) expects all schools to have Cybersafety Policies and User Agreements in place.

For more information go to: www.netsafe.org.nz



STAFF

Use of the Internet and other communication technologies at RNLS by staff and students is to be limited to educational and personal usage appropriate in the school environment. Appropriate use also includes staff professional development.

Staff need to be aware that any incident involving material which is deemed 'objectionable' under the Films, Videos and Publications Classification Act 1993 could constitute criminal misconduct necessitating the involvement of law enforcement. As well, involvement with any material which, while not illegal under the Act, is nonetheless detrimental to the safety of the school environment or is not in line with the special character of the school, may constitute professional misconduct serious enough to require disciplinary response by the school.

A Staff use

1. **All staff** (teaching and ancillary) must read and sign this staff Cybersafety Policy and Use Agreement and return the Agreement portion of the document to the Cybersafety Officer. The Policy pages should be retained for later reference.
2. All staff wishing to access the network on school equipment will be provided with an individual login user name and password. This needs to be kept confidential and not shared with anyone else; any illegal and/or inappropriate use of the RNLS computer facilities can be traced to the perpetrator by means of this login information.
3. Staff will be provided with individual Internet e-mail accounts.
4. Links to appropriate websites can be placed on School Zone to provide quick access to particular sites.
5. Staff need to be aware of confidentiality and privacy issues when accessing student or staff information via the school network. Be aware that unauthorized persons could read information left on an unattended computer screen.
6. If a staff member ever wishes his/her own child to make use of the school Internet equipment, the same prohibition of misuse applies as for student use. In particular, note that the parent must be present at all times and is fully responsible for the conduct of his/her child, who would use the parent's login.
7. If the Internet and other communication technologies (e.g. mobile phone) are used to facilitate misconduct such as harassment or involvement with inappropriate or illegal material, the matter will be taken very seriously by the school and could result in disciplinary action. Illegal material or activities will also necessitate the involvement of law enforcement.

B Staff responsibilities when using the Internet with students (not for ancillary staff)

1. Before ANY student can make use of the computer network:
 - An RNLS Computing/Cybersafety Use Agreement (obtainable from the office) must be filled in and signed by both student and caregivers.
 - This form should be returned to the school office where it will be processed and recorded on the network in the student database and filed with the student's records.
 - As this permission form needs to be completed only once in a student's time at school, the cyber safety officer will on request print off a list for staff so that it is clear which students do not yet have permission to use the Internet.
 - UNDER NO CIRCUMSTANCES may a staff member permit a student to use the Internet unless that staff member has sighted official proof that the school has on record a Use Agreement signed by both the child and a parent/caregiver.
 - It is the staff member's responsibility to ensure that this condition is met.
2. Staff who are not confident of their Internet skills could request help from the ICT Manager. Staff may supervise student use of the Internet only if they are confident they have basic Internet Safety Skills. (See Box 1 last page)
3. It is recommended that only one Window is to be used with the Browser at any one time, and that the taskbar must be visible at all times.
4. The staff member must be in the room, remain there and actively supervise while the students are using the Internet. No students may be sent to a computer unsupervised to use the Internet, in or out of class time.
5. Students should be regularly reminded of the contents of the Use Agreement they have signed and that there are can be serious penalties (including possible involvement of law enforcement) for significant breaches of this agreement.
6. If students are permitted email accounts (or accessing accounts outside of school) staff will be advised as to what is appropriate.
7. Students need to be directed to places on the Internet, rather than be permitted to surf. The teacher will need to have gained experience using the Internet before permitting students access.
8. Students may access the Internet only when a staff member is in the room and aware of the activity. This includes use in places like the Library and the Cantatech room as well as teaching classrooms.
9. Inappropriate use of the Internet or any other communication technologies by a student must be reported immediately to the Cybersafety Officer. If the CO is absent, then another senior member of staff should be notified.

C School Website

This will be an on-going project. A number of important reasons exist for having a website, including providing information about the school and publishing student work. See the ICT Manager for further information.

D Monitoring

- Staff and students need to be aware that with the current systems set up to access the Internet, a record is kept of which sites are visited, how often and from which terminal.
- Filtering software will be deployed where appropriate to restrict access to certain sites.
- If deemed necessary, auditing of the school computer system could include all aspects of its use e.g. personal network storage folders and e-mail accounts.
- Staff and student Internet usage will be randomly audited once a month.

E Cybersafety Use Agreement for staff

Please fill in and sign the attached sheet regarding Student Safety, Professional Development, and your agreement to the school's Policy.

The sheet should be returned to the School's Cybersafety Officer (CO).

(The present CO is Hans Berends)

RNLS Cybersafety Use Agreement for Staff

Student Safety (teaching staff to tick one – ancillary staff leave blank)

I have the appropriate knowledge to safely supervise student Internet use and have read the student use policy. (T:\Department Files\Computer Studies\Policies)

I need training in basic Cybersafety issues before I supervise student Internet use.

Staff Professional Development (tick one or more)

No professional development on Internet use is required at present.

I would like additional training in Internet use.

I would like training in the following areas:

I understand and agree to follow the attached Cybersafety Use Policy as it applies to use of Internet and other communication technologies by staff, and by students under the direction of staff.

Name:

Preferred Password:

Date:

Signature:

STUDENTS & THEIR FAMILIES

I understand that:

- I cannot use the Internet at school without signing and handing in this Use Agreement.
- I may only log on as myself and will not divulge my password to others.
- Computers and other communication technology equipment that belongs to Rangiora New Life School are intended for educational purposes. Any other communication technology equipment that I use within the school environment (e.g. mobile phone) will be used in accordance with the school regulations.
- 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 which is inappropriate, (e.g. legal pornography), dangerous, (e.g. bomb designs), or illegal (e.g. child pornography or stolen credit card numbers). It is therefore **each student's responsibility** not to initiate access to such material, to distribute such material by copying, storing or printing, or have any involvement with such activity.
- When using the email facilities at school, it may not be possible for the school to monitor or filter all messages; it is therefore **each student's responsibility** to ensure that any electronic correspondence will not cause offence or be otherwise inappropriate.
- The school will view seriously involvement in any incident in which communication technologies are used to facilitate misconduct e.g. harassment, bullying, plagiarism, exam cheating etc.
- The school reserves the right to check at any time, work or data related to communication technologies in the school environment.

I will take care of information technology resources, including:

- I will not damage computer equipment or furniture and will use the resources with due care.
- I will not use any school computers for arcade-style games.
- I will not attempt to breach copyright (e.g. by illegally copying software).
- I will not bring software from home to use on a Rangiora New Life computer.
- I will not plagiarise by illegally copying text without referencing the source.

I will be considerate to other users, including:

- I will not monopolise equipment.
- I will not deliberately waste computer resources (e.g. unnecessary printing).
- I will not intentionally disrupt the smooth running of any computer or the school's network.
- I will not scan or display graphics, record or play sounds, or type messages that could cause offence to others.
- If I accidentally encounter inappropriate, dangerous or illegal material I will immediately remove it from the screen/turn off the screen and notify a supervising teacher without disclosing the material to any other student.

I will respect the need for privacy and security, including:

- I will not reveal home addresses or phone numbers, mine or anyone else's, in cyberspace.
- I will use disks only after checking with the School's computer supervisor.
- I will not attempt to upload or create computer viruses or be involved with other forms of electronic vandalism.
- I will immediately report any cybersafety problems to a class teacher or Head of Department.

I accept that:

Breaching this agreement (or any involvement in such a breach) may result in my access to the Computing and Communication Technology resources at Rangiora New Life School being withdrawn, which could make me ineligible to continue studying a particular subject. I also understand it could result in disciplinary action by the School.

(If not collected at enrolment, return the Use Agreement to the school office after it has been signed.)

**Rangiora New Life School Computing / Cybersafety
Student Use Agreement**

Student:

I understand and will abide by the conditions and rules as set out in the school's Computing / Cybersafety Use Agreement. I further understand that there may be consequences (including the possible loss of access and even disciplinary action) if I should commit any breach of these conditions.

Surname: _____

First Name: _____ Year Level: _____ Signed: _____ Password: _____
(at least 5 characters or more)

First Name: _____ Year Level: _____ Signed: _____ Password: _____
(at least 5 characters or more)

First Name: _____ Year Level: _____ Signed: _____ Password: _____
(at least 5 characters or more)

First Name: _____ Year Level: _____ Signed: _____ Password: _____
(at least 5 characters or more)

Parents or Guardian:

General use of computing/communication technology resources:

As the parent or guardian of this student, I have read the Computing / Cybersafety Use Agreement. I believe my child has read the document and understands his/her obligations. I understand that the computer/communication technology resources at Rangiora New Life School are designed for educational purposes and that any breach of the rules and conditions as set out in this agreement can lead to loss of privileges or disciplinary action. I understand if my child steals or damages equipment this could result in a bill for the cost of replacement parts or repairs. I also understand this agreement applies to communication technologies my child brings into the school environment.

Access to cyberspace:

As the parent or guardian of this student, I understand that it is may not be possible for the school to fully restrict exposure to inappropriate material in cyberspace, accessed through such means as the Internet, email or text messaging. I also understand that while the school will take appropriate measures to limit access to illegal, dangerous or inappropriate material, ultimately it is each student's responsibility not to initiate access to, or have any involvement with, such material.

I hereby give my permission for _____ to be given access to computing and communication technologies such as the Internet.

Signed: _____ Date: _____
Parent / Guardian Signature

SCHOOL LIBRARY

The school Library is an information centre and educational resource for both staff and students. Because of the important role it plays in supporting student learning, the Library views the provision of Internet access as part of its service to students. In line with the Board Cybersafety Policy, the Library aims to provide this Internet access in a cybersafe environment.

Guidelines

1. The Teacher Librarian and any other Library staff will work together to set up cybersafe procedures and systems.
2. The Internet will be available to students for educational purposes only.
3. Only students who have a signed Computer Use Agreement on file may use the Library Internet-accessible computers.
4. Computers which are Internet-accessible will be sited so that they can be observed from the Librarian's workstation.
5. Students must use their own login and password. They may not use anyone else's or provide anyone else with their login and password details.
6. Although Library staff will whenever possible endeavour to keep an eye on Internet users, they have many other duties, some of which may take them away from that area of the Library. At all times it is up to individual students to follow the school cybersafety rules they have agreed to. As well, they must follow these specific Library cybersafety procedures which are displayed around the Library. Accepting responsibility for their own actions is particularly important for students in out-of-class time spent in the Library i.e. before class, at interval, lunchtime and after school.
7. Classroom teachers need to be aware that when they bring a class down to the Library it is their responsibility to supervise any Internet use by their students; it is not the responsibility of Library staff.
8. If a class teacher wishes to send a student, or a small group of students, to the Library in class-time in order to use the Internet it is preferable that this is arranged beforehand. If no such arrangement has been made, the students could be sent with a signed note from the teacher which specifies exactly what use is to be made of the Internet. If there is no Internet-accessible computer free, the students will be sent back to class immediately.
9. Any student who is found to have disobeyed school and Library cybersafety rules will immediately be reported to the school Cybersafety Officer (CO), or in his/her absence, to another member of the senior management team. Information on exactly what occurred, plus any evidence available should be given to the CO as soon as possible. Action taken against that student may include being denied future access to Library Internet facilities (or even to the Library itself), and could also result in disciplinary action taken by the school.
10. The Librarian will liaise with the Cybersafety Officer and ICT Manager over all matters pertaining to cybersafety in the Library.
11. A copy of this Library Cybersafety Policy will be distributed to all members of staff.