Rutherglen High School
Sheridan's Bridge Road
Rutherglen, Vic, 3685
Ph 02 60329483
Fax 02 60329185

CYBERSAFETY AND ACCEPTABLE USE FOR ALL RUTHERGLEN HIGH SCHOOL STUDENTS

This document is comprised of two sections:

Section 1 – Cybersafety in the School Environment
- A) Important Rutherglen High School cybersafety initiatives
- B) General cybersafety rules

Section 2 – Information Specifically for Rutherglen High School Students
- A) Additional information
- B) Additional rules / responsibilities

Instructions for secondary students:

1. You and your parent/legal guardian/caregiver are asked to read Section A 'Cybersafety in the School Environment' and Section B 'Information Specifically for High School Students' carefully.
2. If help is needed to understand all the language, or there are any points your family would like to discuss with the School, let the School office know as soon as possible.
3. You and your parent/legal guardian/caregiver should then sign the Student Use Agreement Form at the back of Section B before you return that page to RHS.
4. It is important to keep Section A and Section B for you and your family to read again in the future.

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 RHS ICT equipment/devices as outlined in (d) below. This also includes subsidiary or public organisation(s) equipment which may extend and/or be part of the RHS network infrastructure.*

*(d) The term **'ICT equipment/devices'** used in this document, includes but is not limited to, computers (such as desktops, notebooks, netbooks, 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) The abbreviation **'YLC'** in this document refers to Year Level Coordinators*

*(f) The abbreviation **'RHS'** in this document refers to Rutherglen High School.*

(g) *The ICT Management Team in this document refers to the Principal, Assistant Principal, Network Administrator/Manager and other staff appointed to the team.*

SECTION 1A - IMPORTANT RUTHERGLEN HIGH SCHOOL CYBERSAFETY INITIATIVES

The values promoted by Rutherglen High School include establishing positive relationships in a safe and caring environment; cooperation, mutual respect, acceptance and trust; being fair, friendly, supportive and honest; developing and displaying ethics and personal integrity; and respecting the physical environment. 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, such as student netbooks, bring great benefits to the teaching and learning programs at Rutherglen High School, and to the effective operation of the School. However, it is essential that the School endeavors to ensure the safe use of ICT within the School community.

Rutherglen High School
Sheridan's Bridge Road
Rutherglen, Vic, 3685
Ph 02 60329483
Fax 02 60329185

Thus Rutherglen High 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 of this agreement. 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 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 user 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. Each time a student logs in to a device they are agreeing to the terms and conditions of this document.

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 ICT Management Team or Reception).

1.3. The School encourages anyone with a query about the agreement to contact the ICT Management Team 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, including but not limited to iPod Touches and student netbooks or notebooks, on or off the School site, is limited to educational purposes appropriate to the School environment. 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. The School will use remote access software to ensure appropriate use of ICT devices and the School network. 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** ICT equipment/devices on the School site, or at any School-related activity must be appropriate to the School environment and be approved by the ICT management team or the YLC. 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 netbook, notebook, 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 Management Team prior to using such device.

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**.

However, the expectation is that each individual will make responsible use of such systems. In the event of their use, students must be able to demonstrate their connection to current classroom learning.

Rutherglen High School
Sheridan's Bridge Road
Rutherglen, Vic, 3685
Ph 02 60329483
Fax 02 60329185

3. Monitoring by the School

3.1. Rutherglen High School has an electronic access monitoring system which has the capability to record Internet use, including the user details, time, date, sites visited, and from which computer or device the http traffic was viewed. The ICT Management Team also has the ability to remotely monitor School ICT equipment, via logs and real-time screen viewing, including, but not limited to, student netbooks, notebooks, laptops and Desktops. You must not attempt to prevent the ICT Management Team from remotely monitoring any ICT equipment/device

3.2. The School monitors traffic and material sent and received using the School's ICT infrastructures. This will 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.

3.4. The School holds the right to access/redirect/stop/copy for evidence any type of electronic data and remove inappropriate electronic data without notice.

3.5. The School holds the right to lock/disable/remove/modify domain/local computer accounts in the event of a threat to the School ICT. This includes any electronic devices which are on the premises of the School.

However, as noted in 2.4, the expectation is that each individual will be responsible in their use of ICT.

4. Ownership

4.1 Netbooks remain the property of the School. Students may not purchase netbooks.

4.2.1 **If in the netbook program:** - When exiting enrolment from the School the netbook must be returned with all parts and in a reasonable condition on the day of exit. Failure to do so will result in the device being reported stolen to the police.

5. Audits

5.1. 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 netbooks, notebooks or other ICT devices provided by/through the School.

6. Breaches of the Use Agreement

6.1. 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.

6.2. Such a breach which is deemed harmful to the safety of the School, such as involvement with inappropriate or illegal material, anti-social activities such as harassment and bullying and possession of Peer-to-Peer software such as Limewire or BitTorrent, will constitute a significant breach of discipline and result in serious consequences. A breach of this agreement will result in the netbook, or ICT device being reimaged. Any further breaches of this nature will result in changes to the management of the netbook, or ICT device. The ICT Manager and/or year level coordinator will respond and take appropriate action regarding consequences of all breaches.

Refer to the document **'Rutherglen High School - Computer User Agreement'**

6.3. If there is a suspected breach of the 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.

6.4. Involvement with **material** which is deemed 'age-restricted' or 'objectionable' (illegal) 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.

Rutherglen High School
Sheridan's Bridge Road
Rutherglen, Vic, 3685
Ph 02 60329483
Fax 02 60329185

6.5. Any damage or loss caused to a netbook issued to a student by the School which is not covered by warranty, is the student's responsibility.
Note: Failure to use the approved carry cases (See ICT Management Team) will Void the warranty and insurance. All repair costs will be passed onto the student.

6.5.1 An insurance excess will apply for any accidental loss or damage.

6.5.2 Any damage or loss deemed deliberate will not be covered by insurance and the full repair or replacement cost will be the student's responsibility. This includes the failure to use an approved carry case

6.5.3 Insurance excess will be charged at the following rate, 1st offence $100, 2nd Offence $175, Subsequence offences $250 each. Insurance excess needs to be paid before access to the RHS ICT network and equipment is restored.

7. Other aspects of the School's cybersafety programme

7.1. The Cybersafety and Acceptable Use Agreement operates 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 ICT Management Team, Principal and Assistant Principal can be contacted.

SECTION 1B - GENERAL CYBERSAFETY RULES

These general rules have been developed to support the 'Important Rutherglen High School Cybersafety Initiative's outlined in Section A.

1. Staff and students are required to sign use agreements with the School

1.1 Please sign the first page of this agreement and return it to the School office.

NB The entire document should be kept to refer to later, including a copy of the signed form.

2. Use of any ICT must be appropriate to the School environment

2.1 For **educational purposes only.** The School's computer network, Internet access facilities, computers and other School ICT equipment/devices can be used only for educational purposes appropriate to the School environment. This rule applies to use on *or* off the School site. If any other use is permitted, the School will inform the user/s concerned.

2.2 **Permitting someone else to use School ICT.** Any staff member or student who has a signed use agreement with the School and allows another person who does not have a signed use agreement as per point 1 (above) to use the School ICT, is responsible for that use.

2.3 **Privately-owned ICT.** Use of 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. It also includes the use of mobile phones, which are prohibited during school hours. Any queries should be discussed with the ICT Management Team, the Principal, Asssistant Principal or any Year Level Coordinator (YLC).

2.4 **Responsibilities regarding access of inappropriate or illegal material.**
When using School ICT or privately-owned ICT on the School site or at any School-related activity, users must not:

- initiate access to inappropriate or illegal material – including but not limited to adult content, online gaming sites, gambling sites, social networking and chat sites such as MySpace and Facebook etc. The use of Peer-to-Peer software is also prohibited
- save or distribute such material by copying, storing or printing.

In the event of accidental access of such material, users should:

1. not show others
2. close or minimise the window
3. report the incident
   - Students should report to a teacher immediately
   - Staff should report such access as soon as practicable to the ICT Management Team.

2.5 **Misuse of ICT**. Under no circumstances should ICT be used to facilitate behaviour which is either inappropriate in the School environment or illegal.

Refer to the document '**Rutherglen High School - Computer User Agreement**'.

3 Individual password logons (user accounts)

3.1 **Individual user name and password.** If access is required to the School computer network, computers and Internet access using School facilities, it is necessary to obtain a personal user account from the School.

3.2 **Confidentiality of passwords**. It is important to keep passwords confidential and not shared with anyone else.

3.3 **Access by another person.** Users should not allow another person access to any equipment/device logged in under their own user account, unless with special permission from ICT Management Team (Any inappropriate or illegal use of the Rutherglen High School computer facilities and other School ICT equipment/devices may be traced by means of this login information.)

3.4 **Appropriate use of email.** Those provided with individual, class or group e-mail accounts are expected to use them in a responsible manner and in accordance with this Use Agreement. This includes ensuring that no electronic communication could cause offence to others or harass or harm them, put the owner of the user account at potential risk, or in any other way be inappropriate in the School environment.

4 Disclosure of personal details

4.1 For personal safety, users should be very careful about revealing personal information about themselves, such as home or email addresses, or any phone numbers including mobile numbers. Nor should such information be passed on about others.

5 Care of ICT equipment/devices

5.1 All School ICT equipment/devices should be cared for in a responsible manner and especially ensuring that netbooks or notebooks are carried in the bags or cases provided and in an appropriate manner.

5.2 Any damage, loss or theft must be reported immediately to the ICT Management Team**.** In the event of theft, a police statement must be made as soon as practically possible.

5.3 At school, when netbooks or notebooks are not being used or carried by the individual they should be securely stored in a locked locker.

5.4 When a student who has received a netbook leaves the School the device must be returned to the School in the same condition as when initially supplied. That is, no stickers, graffiti, white-out, scratches and etchings, cracks, missing keys, discolouration, substances requiring more than light cleaning or any damage beyond normal wear and tear.

6 Wastage

6.1 All users are expected to practice sensible use to limit wastage of computer resources or bandwidth. This includes unnecessary Internet access, uploads or downloads.

Rutherglen High School
Sheridan's Bridge Road
Rutherglen, Vic, 3685
Ph 02 60329483
Fax 02 60329185

7 Connecting software/hardware

7.1 Users must not attempt to download, install or connect any unauthorised software or hardware onto School ICT equipment, including but not limited to student netbooks, notebooks, other School ICT devices, or devices such as mobile phones or iPod Touches or utilise such software/hardware. This includes use of such technologies as Bluetooth, infrared, and wireless, mobile broadband internet, and any other similar technologies which may be developed. Any user with a query or a concern about this issue should speak with the ICT Manager.

7.2 In a special case where permission has been given by the ICT Manager to connect or install privately-owned equipment/devices or software, it is with the understanding that the School may scan this equipment/device/software at any time thereafter as part of a regular or targeted security check, such as for viruses.

8 Copyright and licensing

8.1 Copyright laws and licensing agreements must be respected. This means that there can be no involvement in activities such as illegally copying material in any format, copying software, downloading copyrighted video or audio files, using material accessed on the Internet in order to plagiarise, or illegally using unlicensed products. This means that students are not to have Limewire or torrents or any other peer to peer software on the devices. If students are found to be in breach of these guidelines the netbook or notebook/ICT device will be reimaged immediately and YLC's notified.

8.2 The School will provide software which is in accordance with the copyright laws and must only be installed on School leased or owned equipment. Once equipment ownership transfers outside of the School it is only legal to have installed the software which originally came with the computer and copyright laws and licensing agreements become the responsibility of the equipment holder.

9 Posting material

9.1 All material submitted for publication on the School Internet/Intranet should be appropriate to the School environment.

9.2 Such material can be posted only by those given the authority to do so by the ICT Management Team.

9.3 The ICT Management Team should be consulted regarding links to appropriate websites being placed on the School Internet/Intranet (or browser homepages) to provide quick access to particular sites.

9.4 There is only one official website relating to the School with which there should be involvement unless approval has been given by the ICT Management Team.

10 Queries or concerns

10.1 Staff and students should take any queries or concerns regarding technical matters to the ICT Manager.

10.2 Queries or concerns regarding other cybersafety issues should be taken to the ICT Management Team.

In the event of a serious incident which occurs when the ICT Management Team and the Principal are not available, another member of Principal Class Team should be notified immediately.

SECTION 2A - ADDITIONAL INFORMATION

1. The Student Cybersafety Use Agreement

1.1. A teacher will go over this use agreement with you and answer any questions. If you have any more questions later, you should ask staff, including the ICT Management Team. If your parent/legal guardian/caregiver would like to discuss any School cybersafety issue, the ICT Management Team will be happy to discuss this with them.

1.2. You cannot use the School's computer network, Internet access facilities, computers and other Rutherglen High School ICT equipment/devices until this Cybersafety and Acceptable Use Agreement has been signed by a parent/legal guardian/caregiver and signed by you, and the agreement has been returned to the School Office.

2. Use of ICT.

2.1. While at School or a School-related activity, you must not have involvement with any material or activity which might put yourself at risk. The use of social networking sites, including but not limited to MySpace and Facebook is therefore prohibited. As well, you must not at any time use ICT to upset, harass, or harm anyone else in the School community, or the School itself, even if it is meant as a 'joke'.

Unacceptable use could include acts of a malicious or nuisance nature, invasion of privacy, harassment, bullying, hacking, altering the settings on any ICT device or equipment without authorisation, plagiarism, gaming, impersonation/identity theft, spoofing, gambling, fraud, copyright infringement, or cheating in an examination. Behaviour the School may need to respond to also include the use of websites to facilitate misconduct which puts at risk the safety of the School environment.

2.2. If any privately-owned ICT equipment/device, such as a, notebook, netbook or desktop, PDA, mobile phone, camera, or recording device, portable storage (like a USB or flash memory device), is brought to School or a School-related activity, the School cybersafety rules apply to that device. **If you are not sure whether it is appropriate to have a particular device at School or at a School-related activity, you are expected to check with the relevant teacher before bringing it to the School.**

3. Monitoring

3.1. The School reserves the right at any time to check work or data on the School's computer network, Internet access facilities, computers and other School ICT equipment/devices. For example, in order to help make sure that the School stays cybersafe, teachers may at any time check student email or work. The ICT Management Team also has the ability to remotely monitor School ICT equipment, via logs and real-time screen viewing, including student netbooks, notebooks and desktops. You must not attempt to prevent the ICT Management Team from remotely monitoring any ICT equipment/device

3.2. If there is a suspected breach of use agreement involving privately-owned ICT, the matter may be investigated by the School. The School may ask to check or audit that ICT equipment/device as part of its investigation into the alleged incident.

4. Consequences.

4.1. Depending on the seriousness of a particular breach of the use agreement, an appropriate response will be made by the School. Possible responses could include one or more of the following: a discussion with the student, informing parents/legal guardian/caregiver, reimaging of the device, loss of administrator access to devices, loss of student access to School ICT, taking disciplinary action (suspension). If illegal material or activities are involved, it may be necessary for the School to inform the police and/or other government departments.

4.2. Where netbook, notebooks or other devices require reimaging due to a breach of this agreement, the device will not be backed up before reimaging. There will be no opportunity given to the student to back up their work. However, if users request that their work be backed up, the School ICT Support team will do this work for a fee. A fee of $50 will apply on the first occasion and $100 on every occasion thereafter.

Refer to the document 'Misdemeanors' and Recommended Consequences Regarding the Use of Netbooks, Notebooks and Related ICT Facilities'.

SECTION 2B - ADDITIONAL RULES / RESPONSIBILITIES

1. Accessing the Internet at School on School ICT. The only time you can access the internet at the School or on a School computer of any kind during class is when a teacher gives permission and there is staff supervision. If other Internet access outside of class on the School site or at a School-related activity is permitted, for example, during a study period via a netbook, privately-owned notebook, leased notebook , mobile phone or any other ICT device, it must be in accordance with the cybersafety rules in this agreement. While at school, students are only to use the school student internet connection.

Students are not to connect to any external devices e.g. Phones, USB modems or other wireless networks while at Rutherglen High School. Students found breaching these guidelines will lose access to Rutherglen High School's network, and netbooks or notebooks will be reimaged immediately. Deliberate circumvention of school internet filtering, by use of third-party software, external internet connections (such as '3 mobile internet'), or "anonymous proxy" sites will result in the devices being immediately reimaged, the administrator status of the student will be modified and the student's ability to access the Rutherglen High School network will be reviewed.

Rutherglen High School
Sheridan's Bridge Road
Rutherglen, Vic, 3685
Ph 02 60329483
Fax 02 60329185

2. **Borrowing School ICT.** ***If you have permission to use School ICT equipment at home or anywhere else away from School, that equipment must not be given to anyone else to use unless at the direction of a staff member. The School ICT is to be used only for the purpose it was lent, and you should explain this to your family or whoever else you are with. If a problem occurs, you must report it to the relevant teacher straight away.***

3. **Care of netbooks, notebooks, computers and other School ICT equipment/devices, and their appropriate use includes**:

- You must not damage or steal any equipment, or try to damage the ICT network. If the damage is deliberate, it will be necessary for the School to inform your parent/legal guardian/caregiver who will have responsibility for the cost of repairs or replacement.
- Students are not to bring cords and chargers to school, if a student needs to charge a netbook they must book a power point and charger through the library, there will be a limited supply available. Students will only be able to access these before school, rece ss, lunch and after school. Students will not be able to charge netbooks in class.

4. **Students need permission from staff to**:
   - use storage devices to back-up work or to take work home or bring work back to School. (It is preferred, for the safety of the School, that data which has been saved from a device which is not under lease or owned by the School not be placed onto the School network or computers)
   - print material when in the classroom situation. Any material printed out of class must be appropriate in the School environment.
   - contribute material to the School Internet/Intranet site. As well, there should be no student involvement in any unofficial School Internet/Intranet site which purports to be representative of the School or of official School opinion.
   - send email to groups of users which are available on School e-mail/exchange server(s). Only email to individual students and staff according to the e-mail agreements are to be sent.

5. **Students must be considerate of other users. This includes**:
   - sharing with other users and not monopolising equipment.
   - avoiding deliberate wastage of ICT-related resources including bandwidth, through actions such as unnecessary printing, and unnecessary Internet access, uploads or downloads.
   - no intentional disruption of the smooth running of any computer or the School network.
   - avoiding involvement in any incident in which ICT is used to send or display messages/communications which might cause offence to others. Examples include text messaging, email messages, or creating, displaying or sending inappropriate graphics, and recording or playing inappropriate audio or video files.
   - obtaining permission from any individual before photographing, videoing or recording them.

6. **Respect for privacy, safety and security when using the Internet and ICT includes**:

- if you accidentally access inappropriate, dangerous or illegal material you should:
  1. not show others
  2. close or minimise the window
  3. report the incident to a teacher immediately.
- you should use data storage devices such as USB and flash memory devices, only in accordance with School regulations. This includes other portable devices such as USB hard drives.
- you must have no involvement in any activity which could put at risk the security of the School computer network or environment. For example, there must be no involvement with malware such as viruses or involvement with any form of electronic vandalism or theft. This includes `hacking' and any other physical or electronic activities that provide unauthorised access to the School ICT.