Red Cliffs Secondary College
Council Policy

<table>
<thead>
<tr>
<th>Policy Title:</th>
<th>ICT Use &amp; Internet Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date Ratified by Council:</td>
<td>June 22\textsuperscript{nd}, 2016</td>
</tr>
<tr>
<td>Council President:</td>
<td>Philip Hand</td>
</tr>
<tr>
<td>Principal:</td>
<td>David Browne</td>
</tr>
<tr>
<td>Signature:</td>
<td>\signature</td>
</tr>
</tbody>
</table>

Rationale:
Red Cliffs Secondary College has provided an extensive Information and Communication Technology network to assist users with their studies and school work. The system is backed up daily and is protected by the latest virus protection which is continually updated. It is therefore important that this facility is used responsibly and in a safe manner.

Aims:
- To develop students who understand the importance of the safety of themselves and others whenever they use the College computers or internet.
- To develop students who understand the importance of respect for themselves, others and the equipment whenever they use the College computers or internet.
- To develop students who understand the importance of the management and backing up of their personal data.
- To develop students who are ethically responsible digital citizens.

Implementation:
Access to the College Computer System is given under the condition that all users:
- Use the College computer facilities to assist in class studies only.
- Are responsible for backing up their own data on approved portable media which includes SD cards, USB memory sticks or USB portable hard drives.
- Save files in the provided user home directory or on approved portable media.
- Do not interfere with any computer, screen or network settings in any way.
- Do not install software of any kind on desktop computers
- Do not have any programs (games, executable files or runtime files) in Home Directories or removable media.
- Do not interfere with other students files/directories or log-in details.
- Do not log on using another student’s details.
- Abide with the terms and conditions of the netbook usage agreement

**Access to the College Internet facility is given under the condition that all users:**

- Use the Internet for assisting in class studies only.
- Do not arrange to meet in person someone they have met on the Internet.
- Do not publish personal or private details of themselves or other people.
- Do not access or distribute materials which are pornographic, obscene, upsetting, threatening, racist, sexist or in any way dangerous or harmful.
- Do not use language which is obscene, abusive, upsetting, threatening or disrespectful.
- Do not engage in personal attacks, bullying or harassment.
- Do not violate the wellbeing, rights, privacy, data and property of others.
- Do not present the ideas and work of others as their own.
- Do not attempt to gain unauthorised access to any computer system.
- Do not attempt to damage or disrupt the College system by any physical or electronic means including the spreading of computer viruses.
- Do not waste time, band-width or resources by aimless browsing or downloading large files.
- Do not have at school material which could be used to breach the above rules.

**Evaluation:**

- This policy will be reviewed as part of the school’s four year review cycle.
- This policy will be ratified by College Council at the start of each year.
Appendix-A  Guidelines and Conditions Acceptable Use Procedures for the School’s Internet

The school’s computing facilities are provided primarily for the educational benefit of students and the professional activities of staff. Any behaviour that interferes with these primary objectives will be considered an infringement of Acceptable Use.

1. General Policies

- Use of computer/internet resources is for **educational purposes only**
- Access to the Internet will be supervised by a staff member
- Appropriate language must be used in all communications
- Internet and printing services are both charged against a student’s account.
- Consideration must be given to avoiding inconvenience to other computer users. e.g. use headphones to listen to sound or music; leave computers ready for the next user to log in; do not leave programs running on computers when you leave; do not leave rubbish or paper lying around computers; replace furniture to normal positions when you leave

Summary of conditions

**Students must not:**

- Use abusive or obscene language in any communications
- Steal, or deliberately or carelessly cause damage to any equipment
- Interfere with or change any software settings or other user’s files
- Attempt to get around or reduce network security
- Logon using another user’s account
- Store unauthorised types of files in their own home directories ( e.g. games )
- Send "spam" (bulk and/or unsolicited e-mail)
- Reveal personal information in any communications
- Deliberately enter, or remain in, web sites containing objectionable material
- Knowingly infringe copyright

2. Computer hardware

Computer facilities are expensive and must be treated carefully.

**Students must not:**

- Do anything likely to cause damage to any equipment, whether deliberately or carelessly
- Interfere with networking equipment
- Eat or drink near any School owned computer resources

**Students must not, without permission:**

- Attempt to repair equipment without permission
- Unplug cables or equipment
- Move equipment to another place
- Remove any covers or panels
- Disassemble any equipment
- Disable the operation of any equipment
  Students must also report other people breaking these rules.
Any problem with equipment or software must be reported to a teacher or technician.

3. Software and operating systems

Computer operating systems and other software are set up properly for computers to be successfully used in the School.

Students will not:

- Change any computer settings (including screen savers, wallpapers, desktops, menus, standard document settings etc)
- Bring or download unauthorised programs, including games, to the college or run them on college computers, online Internet games are banned
- Delete, add or alter any configuration files
- Copy any copyrighted software to or from any computer, or duplicate such software
- Deliberately introduce any virus or program that reduces system security or effectiveness

4. Networks

Network accounts are to be used only by the authorised owner of the account.

It is the responsibility of students to ensure their user account details remain secure and that unauthorised use of their account does not take place.

Students must not:

- Attempt to log into the network with any user name or password that is not their own
- Reveal their password to anyone. Students are responsible for everything done using their accounts, and everything in their home directories. Since passwords must be kept secret, no user may claim that another person entered their home directory and did anything to cause college rules to be broken.
- Use or possess any program designed to reduce network security
- Enter any other person’s home directory (drive F:) or do anything whatsoever to any other person’s files
- Be logged on to the network on different computers at the same time
- Store the following types of files in their home directory:
  - Program files (EXE, COM)
  - Compressed files (ZIP, ARJ, LH2, ARJ, TAR etc)
  - Picture files, video files, music files etc unless they are required for a school task
  - Obscene material – pictures or text
  - Obscene filenames
  - Insulting material
  - Copyrighted material
- Intentionally seek information on, obtain copies of, or modify files, other data or passwords belonging to other users.

5. Printing

Students must minimise printing at all times by print previewing, editing on screen rather than on hard copies and spell-checking before printing.

Students are allocated printing credit as part of their ICT Parent Payment. Once this allocation has been completely used, further allocations may be purchased. Students are not to use another student’s allocation. Students who deliberately waste another student’s allocation will be liable for all costs incurred. Students are charged a fee to print an A4 page of black printing.
6. Internet usage

Internet access is expensive and has been provided to assist students' education. Students must use it only with permission, and not in any unauthorised way. Students are to be supervised by a staff member when using the Internet at all times.

Students are allocated a download credit as part of their ICT Parent Payments. Once this allocation has been completely used, further allocations may be purchased. Students are currently charged for each Mb of download.

The Internet is not intended for entertainment.

Because the Internet is an unsupervised environment, the school has a responsibility to ensure that, as far as possible, material obtained from the Internet is not offensive or inappropriate. To this end, filtering software has been placed on the Internet links. In the end, however, it is the responsibility of individual students to ensure their behaviour does not contravene college rules or rules imposed by parents/carers.

The school is aware that definitions of "offensive" and "inappropriate" will vary considerably between cultures and individuals. The school is also aware that no security system is perfect and that there is always the possibility of inappropriate material, intentionally and unintentionally, being obtained and displayed.

6.2 Email

Electronic mail is a valuable tool for personal and official communication both within the college network and on the Internet. Students and staff are encouraged to use it and take advantage of its special features. As with all privileges its use involves responsibilities.

Throughout the Internet there are accepted practices known as Netiquette, which should be followed. The following points should be noted:

- Use appropriate language and be polite in your messages. Do not be insulting, abusive, swear or use vulgarities.
- Never write hate mail, chain letters, harassment, discriminatory remarks and other antisocial behaviours. Therefore no messages should contain obscene comments, threats, sexually explicit material or expressions of bigotry or hate.
- Do not reveal your personal address or the phone numbers of students or colleagues.
- Note that email is not guaranteed to be private. All college emails are filtered for inappropriate content. Messages containing inappropriate content are automatically reported to the ICT Manager.
- Teachers will set their own guidelines for use of email in class time.

6.3 Chat lines (IRC, MIRC, ICQ etc)

Real-time chat programs (MIRC, ICQ etc) are not to be used by students.

6.4 World Wide Web

The World Wide Web is a vast source of material of all sorts of quality and content. The college will exercise all care in protecting students from offensive material, but the final responsibility must lie with students in not actively seeking out such material. Students will not deliberately enter or remain in any site that has any of the following content:

- Nudity, obscene language or sexual discussion intended to provoke a sexual response
- Violence
- Information on, or encouragement to commit any crime
- Racism
- Information on making or using weapons, booby traps, dangerous practical jokes or "revenge" methods
Any other material that the student's parents or guardians have forbidden them to see
If students encounter any such site, they must immediately turn off the computer monitor (not the computer itself) and notify a teacher. Do not show your friends the site first.
The Internet must not be used for commercial purposes or for profit.
The Internet must not be used for illegal purposes such as spreading computer viruses or distributing/receiving software that is not in the public domain.
It is inappropriate to act as though you intend to break the law e.g. by attempting to guess a password or trying to gain unauthorised access to remote computers. Even if such attempts are not seriously intended to succeed, they will be considered serious offences.
Interactive use of the Internet should ensure that there is no possibility of the transmission of viruses or programs, which are harmful to another user's data or equipment.
Copyright is a complex issue that is not fully resolved as far as the Internet is concerned. It is customary to acknowledge sources of any material quoted directly and it is a breach of copyright to transmit another user's document without their prior knowledge and permission. This includes the use of images and text. It is safest to assume all content on web sites is the legal property of the creator of the page unless otherwise noted by the creator.

6.5 The School Web site
Material placed onto the school web site must:
- Be checked for appropriateness and (as far as possible) accuracy
- Not violate copyright
- Have the written permission of a parent/guardian if the parent or guardian has requested such a veto
- Not contain the home address or home phone number of an individual
- Not contain the e-mail or web address of a student unless specifically required and requested
Links to sites beyond the school site must be checked for appropriate content. It must be recognised that the content of external sites may change after links have been made, and the college cannot be held responsible for the contents of linked sites, but the college must exercise all due care to ensure no objectionable material is directly accessible via links on our site.

7. Penalties

More than one may apply for a given offence. Serious or repeated offences will result in stronger penalties.

- Removal of network access privileges
- Removal of email privileges
- Removal of internet access privileges
- Removal of printing privileges
- Paying to replace damaged equipment
- Other consequences as outlined in the school discipline policy

8. The Student and Parent Support Kit is to be distributed and the Agreement Form is to be signed and returned to school before access to the school’s Information and Technology resources can be granted.
Acceptable use of ICT and the Internet Agreement
(to be signed by the student and parent/carer)

When I use technology, both at school and at home I have responsibilities and protocols to follow. I agree to:

- be a safe user whenever and wherever I use that technology
- be responsible whenever and wherever I use technology and support others by being respectful in how I talk to and work with them and never write or participate in online bullying (this includes forwarding messages and supporting others in harmful, inappropriate or hurtful online behaviour)
- report to an adult if I feel unsafe or uncomfortable online or see a friend being unsafe or being made to feel uncomfortable by others.

When at school I agree to:

- keep myself and my friends safe by not giving out personal details including full names, telephone numbers, addresses and images and protecting my password
- use the technology at school for learning, use the equipment properly and not interfere with the work or data of another student
- not bring or download unauthorised programs or files
- not go looking for rude or offensive sites
- use an ‘online name’ and avatar when sharing my work online
- remember that the content on the web is someone’s property and ask my teacher or parent to help me get permission if I want to use information or pictures
- think carefully about what I read on the internet, question if it is from a reliable source and use the information to help me answer any questions (I should not copy and paste the information as my answer)
- talk to my teacher or another adult if:
  - I need help online
  - I am not sure what I should be doing on the internet
  - I come across sites which are not suitable
  - someone writes something I don’t like, or makes me and my friends feel uncomfortable or asks me to provide information that I know is private
  - I feel that the welfare of other students at the school are being threatened.

If I use my mobile phone, iPod or other mobile device I agree to:

- restrict usage to the conditions outlined in the college mobile phone policy
- use it as requested for learning purposes as directed by my teacher
- be responsible in my use and not use the device to find, create or send information that might be harmful, inappropriate or hurtful to me or anyone else.
- To this end, when using my mobile device, this will be restricted to out of school hours and out of school boundaries use only:
  - I will keep my phone turned off or on silent while at school and store it inside a locked locker.
- protect the privacy of others and never post private information about another person using SMS messages.
• Abide by all state and national laws as they relate to appropriate phone and telecommunications use.

If using my mobile device as a camera I will:

• only take photos and record sound or video when it is part of a class or lesson
• seek permission from individuals involved PRIOR to taking photos, recording sound or videoing them (including teachers).
• seek written permission from individuals involved PRIOR to publishing or sending photos, recorded sound or video to anyone else or to any online space
• be respectful in how I talk to and work with others online and never write or participate in online bullying
• seek teacher permission before uploading any content to websites, blogs or other shared online spaces.
• Abide by all state and national laws as they relate to appropriate phone and telecommunications use.

This Acceptable Use Policy also applies to students during school excursions, camps and extra-curricula activities.

I acknowledge and agree to follow these rules. I understand that my access to the Internet and mobile technology at school will be renegotiated if I do not act responsibly.

Student Name:.................................................................

Student Signature:...........................................................

Parent Permission
I agree to allow my child to use the internet at school. I have discussed the scenarios, potential problems and responsible use of the internet with him/her as outlined in the internet use kit.

I will contact the school if there is anything here that I do not understand. If there is a situation which concerns me, I will contact either the school or ACMA Australia's Internet safety advisory body on 1800 880 176.

Parent/Guardian Signature :..............................................

Date:.......................................................... ............................

On receipt of the completed and signed Acceptable Use Agreement you will receive your network and internet account details.
Help Your Child to be a Safe User of the Internet

Safe and ethical behaviour online is explicitly taught at our school and support at home is requested.

Please keep this as a resource to use at home

At school the internet is mostly used to support teaching and learning. However, at home it is often used differently. Not only is it a study resource for students, but it is increasingly being used as a social space to meet, play and chat. The internet can be lots of fun.

If you have the internet at home, encourage your child to show you what they are doing online. If not, see if you can make a time to visit the school to see their work and how the school uses the Internet.

Bullying, stranger danger, gossip, telling the wrong people personal information have long been issues for young people growing up. These are all behaviours which now present online. These are not 'virtual' issues. They are real and can harm and hurt.

At home we recommend you:

- make some time to sit with your child to find out how they are using the internet and who else is involved in any online activities
- ask them to give you a tour of their 'space' if they are using a site which allows them to chat, publish photos, play games, etc
- always get them to set their space to 'Private' if they use a social networking site like MySpace, Bebo or Pixo (they are then in control of who can contact them and accesses their information)
- have the computer with internet access set up in a shared place in the house - not your child's bedroom
- negotiate appropriate times for you child's online activities and use of mobile phones
- ask questions when your child shows you what they are doing:
  - How does it work, how do you set it up and can you block out people?
  - Who else is sharing this space or game - did you know them before or 'meet' them online and what do you know about them?
  - Why is this so enjoyable - what makes it fun?
  - Can you see any risks or dangers in the activity - what would you say to warn/inform a younger child who was going to start to use the space?
  - What are you doing to protect yourself or your friends from these potential dangers?
  - When would you inform an adult about an incident that has happened online that concerns you?

Safety Topics and Tips

Protective Behaviour Online

Many young people like to publish information about themselves and their friends in spaces like MySpace, Club Penguin or blogs. This can put them at risk of being approached, groomed, and/or bullied online.
We recommend that they:

- don’t use their own name, but develop an online name and use avatars where available
- don’t share personal details including images of themselves or their friends online
- password protect any spaces or accounts they have and never share that password
- don’t allow anyone they don’t know to join their chat or collaborative space - use the block feature
- are reminded that any image or comment they put on the internet is now public (anyone can see, change or use it)

**Being respectful online and not participating in online bullying or hurtful behaviour.**

The online environment sometimes feels different. The language is different. Sometimes students say things online that they would never say to someone’s face. Being online can make students feel that they are anonymous (even though online interactions can be traced), and often their environment has very few adults.

Not all altercations are examples of bullying, but all unacceptable behaviours need to be addressed.

Participation in bullying or hurtful actions can take many forms in the online world (for example, it can take the form of forwarding messages or directing others to see published images and content which has been deliberately posted to humiliate another person).

Deliberate exclusion of another in an online space is another way some students hurt each other online. It is important that the behaviours are discussed as separate from the technologies.

**Thinking carefully about what is on the internet, questioning if it is from a reliable source and using the information to help answer questions**

Not everything on the internet is true, accurate or unbiased. Copying and pasting information can help organise arguments, ideas, and information, but it is important that your child uses their own thoughts and language to express what they have learnt. If helping with homework ask open-ended questions.

**Encourage them to keep out of rude or offensive sites.**

The internet has some really flashy and tricky ways to lead people into websites they never meant to visit. It is easy for us all to get distracted. We want students to ask for help in locating the information they need, and clarifying the task they have been set. Unfocused clicking through websites can lead to inappropriate content.

Open communication between parents, teachers and young people is the best way to keep them safe. Young people will often share concerns with each other online. It is important that they tell a teacher and or parent when they are feeling uncomfortable or threatened online.

If you have any concerns about this agreement or internet safety contact your school or call 1800 880 176 or visit [http://www.cybersmartkids.com.au/for-parents_tips.htm](http://www.cybersmartkids.com.au/for-parents_tips.htm) or email connect.manager@edumail.vic.gov.au