REHOBOTH CHRISTIAN COLLEGE

POLICY AND PROCEDURES MANUAL

ICT Usage and Social Media Policy

CONTENTS

1. OVERVIEW

First created:	4 February 2015
Last reviewed:	11 January 2016
Review cycle:	2 years
Approver:	Senior Leadership Team
Owner:	ICT Manager
Stakeholders:	Students, parents
Child Safety:	National Principles 1-5, 8, 10

Rehoboth Christian College seeks to provide a learning environment in which all students are protected from harm and places the highest possible priority upon the safety and nurture of young people. The College expects all stakeholders to espouse this approach and to be aware of the Child Safe Framework, accessible from the College website.

a) 'So if there is any encouragement in Christ, any comfort from love, any participation in the Spirit, any affection and sympathy, complete my joy by being of the same mind, having the same love, being in full accord and of one mind. Do nothing from selfish ambition or conceit, but in humility count others more significant than yourselves. Let each of you look not only to his own interests, but also to the interests of others' (Philippians 2:1-4).

b) Recent advances in information and communication technologies have radically changed, and will continue to change, the way that Rehoboth Christian College ("the College") interacts with the outside world and provides resources for learning. As we learn to make use of the computer network and travel this electronic highway, maps to find information and rules to keep travelling safely become vital to successfully completing the journey. This document is intended as a guide in helping you to make informed and appropriate decisions about the best use of Rehoboth Christian College's computer resources.

c) This policy documents the College's stance on usage of its computer and network systems and associated devices, as well as the requirements it places on students for fair and proper usage.

d) Any questions about any aspect of this policy or its applicability to a particular situation should be directed to the to the ICT Manager.

2. RATIONALE AND SCOPE

a) This policy applies to students and parents. It should be read prior to signing the Device Loan Agreement.

b) The College believes the educational benefits of a technology-rich learning environment far outweigh any disadvantages of access, such as potential exposure to inappropriate materials. The aim of this policy is therefore to equip students with the knowledge and skills needed to make informed and appropriate decisions when using the College's ICT resources. The purpose of this policy is therefore to outline the expectations and requirements for student usage of those resources, and to provide guidelines for you to be able to meet those requirements.

3. RESOURCES

There are a number of resources available for students and parents in addition to the guidelines provided in this policy, particularly in the areas of cyber safety. Some of these include:

- Australian Government Cybersmart Website
- Australian Communications and Media Authority (ACMA)
- Australian Government NetAlert Parent's Guide to Internet Safety (2007)
  (Available on request from your campus office)
- ACMA Online Social Networking Factsheet
  (Available on request from your campus office)

4. DEFINITIONS

ICT stands for **Information and Communications Technology**. At Rehoboth, this includes all the computer, network, and internet resources currently used, and that we may use in the future. Generally, it does not refer to audiovisual technology such as TVs, projectors, or telephones, though there can be some crossover which you will need to be aware of.

Other key terms in the policy will be defined in their relevant sections.

5. CODES OF CONDUCT FOR ICT ACCESS

5.1 Introduction

Just as you learn and are expected to abide by social, moral, and ethical codes and behaviours that are acceptable in our College, you need to learn the correct procedures and rules for using our network of information services. All students, without exception, are required to obey the guidelines. **If you break any of these rules, you will not be allowed to continue to use the system.**

5.2 Expected Behaviour

a) The network is provided for students to conduct research and process information in connection with their College work. You are expected to use the network to pursue intellectual activities, seek resources, and access other libraries. We want you to explore this new "cyberspace", and discover what is available there which is of real value for learning and for serving God. We encourage you to learn new things and share that newfound knowledge with your friends, your parents and your teachers.

b) Each network or system has its own set of policies and procedures. Actions that are routinely allowed on one network or system may be controlled or even forbidden on other networks that you may access through the Internet. It is the user's responsibility to abide by the policies and procedures of the network or system being used.

c) Remember, the fact that a user **can** perform a particular action does not imply that they **should** take that action. You continue to be a testimony for Jesus Christ in person and on the Internet. As a condition for use of the Rehoboth Christian College computing facilities, all users are expected to:

   i. **Respect the privacy of others.** If a user on the network asks that you no longer send them mail or in any other way contact them, you are obliged to stop all contact immediately. You may feel you have the right to freedom of expression, but others have the right to be free from harassment.

   ii. **Respect the integrity of the College's computing systems.** Users must not intentionally use programs that damage or alter the software on Rehoboth Christian College's network. If you are responsible for a computer becoming infected with malware, you will be held liable. In addition, "hacking" and computer piracy, or any tampering with hardware or software, or any vandalism of computer equipment are serious offences which will result in immediate suspension of all network privileges, together with further disciplinary action up to and including criminal charges if applicable. You may also be required to pay the cost of repairing any damage you cause to equipment or data.

   iii. **Respect the legal protection provided by copyright and licenses.** For example, users must not make unauthorised copies of proprietary software for their own use, even when that software is not physically protected against copying.

iv. **Respect the shared nature of our systems** and our shared Internet pipe. Limit your own use and size of your files and downloads so as not to interfere unreasonably with the activity of others.

v. **Respect the procedures** established to manage the use of the network.

vi. **Report any violation** of these guidelines by any other individual. You are also required to report any flaw in, or bypass of, computer or network security that you may discover while working on the network.

d) All users should be aware that the inappropriate use of electronic information resources could be a violation of local, state, and federal laws. Violations can lead to prosecution.

e) The use of Rehoboth Christian College's computing facilities is **a privilege, not a right**. Inappropriate use will result in suspension or cancellation of those privileges. Each person who is given access to the network will first participate in an orientation course as to proper behaviour on the network.

5.3 Cyber Bullying

a) Using the College systems to defame any person is not permitted. Generally, **defamation** occurs when a person publishes a statement or media that harms or damages the reputation or standing of another person within the community. A statement is **published** once it is accessible to a third person. This includes, but is not limited to:

i. defamatory mobile phone messages

ii. defamatory email messages

iii. defamatory web pages

iv. defamatory use of programs such as Usenet groups, chat rooms, email, Telnet, bulletin boards, etc.

b) Cyber bullying will be dealt with in accordance with the College Bullying Policy. Cyber bullying that takes place outside College hours will almost inevitably continue to impact a targeted student while he or she is at College. The College reserves the right to implement the Bullying Policy in these circumstances.

5.4 Fairness of Use

a) It may seem that there is no limit to the resources on the Internet, but the College network has a limited capacity to handle traffic, and this capacity is shared amongst everyone. This means the more users there are on the network, the more congested the network becomes. If there are too many users at any given time, the traffic on the network grinds to a crawl, just like a traffic jam on a freeway. Some users may even be cut off altogether. If you obey the following rules, it will help avoid 'gridlock'.

b) Do not tie up the network with idle activities.

c) Do not play games with others on the network or on the Internet. The College network is not designed for computer games. Play games on your own time and on your own equipment.

d) Do not download large files where a smaller version will suffice. Do not download unnecessarily; only take the information you need. The best thing to do is get into the Internet, get what you need, and get out. Remember, there are many students who need to use this network.

e) Users are expected to store their data or document files on their own computers or media, not on the College network.

5.5 Moral and Ethical Issues

5.5.1 Inappropriate Material

a) The moral and ethical issues involving the use of worldwide information systems deal with the appropriate access to information, the type of information, and the behaviour of the user. Rehoboth Christian College wants to provide you with a stimulating educational environment, but at the same time we want to protect you from information that is not appropriate for students to use. We want you to use this valuable educational tool, but at the same time we cannot condone the use of inappropriate information on the Internet.

b) We cannot weed out all of the materials that are unacceptable for students, but it should be clearly understood by all students that access to such material in any form is strictly forbidden. The network is designed to achieve and support instructional goals, and any information that does not support classroom learning is to be avoided.

c) Although the actual percentage of unacceptable materials is small, it can cause concern for students and parents if a student stumbles onto the information while doing legitimate research. If you have a question or concern regarding any information you find, contact your teacher or the ICT Manager.

5.5.2 Plagiarism

a) Plagiarism can be defined as “taking ideas or writings from another person and offering them as your own”. A student who leads readers to believe that what they are reading is the student’s original work when it is not is guilty of plagiarism. Credit must always be given to the person who created the original article or the idea.

b) Be careful when you are using the Internet. Cutting and pasting ideas into your own document is very easy to do, so be sure that you give credit to the author by referencing your work accordingly. That way your

teacher will know which ideas are yours, and you won't be guilty of plagiarism. Bibliographies, reference lists, and citations are all examples of references – **if you are unsure how to prepare a reference, your teacher will be able to help.**

c) Teachers are able to use a variety of tools to automatically scan your work and check it against a variety of sources such as Wikipedia, blogs, websites and other online sources. **It is very easy to uncover plagiarised work.**

d) The penalty for plagiarism is laid down in the College's Fairness in Student Work Policy, which is available from the College office and is issued to all students annually. **You will lose credit for any assessment containing plagiarised material.**

5.5.3 Copyright

a) Copyright is another issue altogether. According to the Copyright Act of 1968, as amended, "Fair Use" means that you may freely use any information that you legally find on the Internet as long as you do so only for scholarly purposes; you may not plagiarise or sell what you find. Suppose, for example, that you find a copy of Photoshop on the Internet. Could you legally copy it? The answer is NO. This is copyrighted software. You have to purchase commercial software packages before you use them legally. Suppose you find an article about the use of Photoshop on the Internet. Can you legally copy it? The answer is yes, as long as you give credit to the author and do not sell the article for profit, but only use it to learn about the use of the program.

b) The same rules apply to music and video files. These may be legally downloaded (from iTunes, for example) but sharing them with others, whether over the Internet, via AirDrop, or other local sharing mechanisms, **is not permitted**. This rule remains in force even where copyright does not directly apply, such as the case of a creative commons license on a media file.

5.5.4 Etiquette and Privacy

a) You are expected to abide by the generally accepted rules of network etiquette in all of your online activity. These rules include (but are not limited to) the following:
   i. Be polite: never send, or encourage others to send, abusive messages.
   ii. Use appropriate language: remember that you are a representative of our Christian College and community. You may be alone with your computer, but what you say and do can be viewed globally. Never swear, use vulgarities, or any other inappropriate language. Illegal activities of any kind are strictly forbidden.
   iii. Maintain privacy: do not reveal your home address or personal phone number, or the addresses and phone numbers of students or colleagues.

iv. Email is not guaranteed to be private. Messages relating to or in support of illegal activities must be reported to the authorities.

v. Disruptions: do not use the network in any way that would disrupt use of the network by others.

b) Other considerations:

i. Be brief. People will be less likely to bother reading a long message.

ii. Minimise spelling errors and make sure your message is easy to understand and read.

iii. Use accurate and descriptive titles for your articles. Tell people what it is about before they read it.

iv. Remember that humour, satire, and sarcasm is very often misinterpreted. Without face-to-face communications your joke may be viewed as criticism or worse.

v. Cite references for any facts or direct quotes you present.

vi. Remember that all network users are human beings. Don't attack correspondents personally; courteously persuade them with fact.

vii. Only capitalise a whole word to highlight an important point or to distinguish a title or heading. *Asterisks* surrounding a word also can be used to make a stronger point.

viii. It is considered extremely rude, and may sometimes be illegal, to forward personal e-mail to mailing lists or Usenet without the original author's permission.

6. NETWORK SECURITY

6.1 Security Principles

a) Security in every aspect is about trading convenience for safety. Just as it is not convenient to put a lock on your front door but you do it to increase your safety, so there are measures necessary to increase your safety online. For example, it is not convenient to have to enter a password to use your computer, but it is safer.

b) Consistency and reliability are paramount for Rehoboth Christian College's computer network to serve you optimally. Therefore, the following guidelines are set out to help you understand our security concerns:

i. Masquerading or pretending to be someone else is forbidden. This includes message forgery, spoofing or impersonation.

ii. Attempts to change desktop or system settings on College PCs are not permitted.

iii. No hacking: attempting to break into or go around any of our security measures is considered a major violation of College rules, whether or not you are actually successful. This includes servers, workstations, networks and other people's resources. Consequences of attempted hacking will be extremely serious.

6.2 Passwords

a) All students with access to the College network will be issued with a password. In addition, many online services that are available to students will secure access with a password. These password guidelines should therefore be followed as closely as possible.

b) Don't give out your passwords to anyone else for any reason. Actions performed by another person using your account will be attributed to you.

c) Use good passwords. Poor passwords are the most common way computer systems are compromised. To help us maintain a properly secure system, please follow these password guidelines:
   i. Use passwords that aren't words in the dictionary
   ii. Use between 5 and 8 characters in your passwords
   iii. Do not use your phone number or home street number as part of your password.
   iv. Use special characters if possible (e.g.: @#$%A*)

d) When you change your password, try not to follow a predictable pattern.

e) Change your password often – especially if you suspect someone else knows it.

f) Don't reuse your password on multiple websites or systems. If one system is compromised then your one password will be known and may be reused by unauthorised persons.

g) Your password should be easy for you to remember. A good way to create this kind of password is to use a sentence that relates to yourself – e.g.: Bill Taylor has 2 cats Ziji and Tiger! So the password for the above sentence would be: BTh2cZaT!

7. ACCEPTABLE USE POLICY

7.1 Acceptable and Unacceptable Behaviours

a) Students are required to be familiar with this policy as a condition of their network privileges.

b) The College considers unethical and unacceptable behaviour just cause for taking disciplinary action, revoking networking privileges, and/or initiating legal action for any activity through which an individual:
   i. uses the network for illegal, inappropriate, or obscene purposes, or in support of such activities. Illegal activities shall be defined as a violation of local, state, and/or federal laws. Inappropriate use shall be defined as a violation of the intended use and/or purpose and goal of the network.

Obscene activities shall be defined as a violation of generally accepted social standards for use of a publicly-owned and operated communication vehicle;

ii. uses obscene language, harass, insult, or attack others;

iii. sends or receives messages that indicate or suggest pornography, unethical or illegal solicitation, racism, sexism, discrimination, or inappropriate language;

iv. sends or displays offensive messages or pictures;

v. uses the network for any illegal activity, including violation of copyrights or other contracts violating such matters as institutional or third party copyright, licence agreements and other contracts;

vi. intentionally disrupts network traffic or crashes the network and connected systems;

vii. joins to the wireless network any unapproved personal computing devices such as smartphones or gaming devices;

viii. installs any software onto the College computers or network without permission;

ix. degrades, disrupts, or damages equipment or system performance;

x. uses the College computing resources for commercial or financial gain, or fraud;

xi. steals data, equipment, or intellectual property;

xii. gains unauthorised access to others' files, or vandalises the data of another user;

xiii. gains or seeks to gain unauthorised access to resources or entities;

xiv. forges electronic mail messages, or uses an account owned by another user;

xv. wastefully uses finite resources;

xvi. invades the privacy of individuals;

xvii. uses passwords belonging to others;

xviii. trespasses in or open folders or files belonging to others;

xix. posts anonymous messages;

xx. possesses any data that might be considered a violation of these rules in paper, magnetic (disk), or any other form;

xxi. engages in any other activity that may be expressly or implicitly forbidden in this document.

7.2 Consequences of Violation

a) Consequences of violations may include, but are not limited to:

i. suspension or cancellation of internet access;

ii. suspension or cancellation of network privileges;

iii. suspension or cancellation of computer access;

iv. disciplinary penalties not related to use of the computer network;

v. College suspension;

vi. College expulsion;

vii. legal action and prosecution by the authorities.

b) Please note that Section 440A of the WA Criminal Code recognizes the crime of "unlawful operation of a computer system". This includes any use of other people's passwords to gain access to someone's workspace, or any other hacking or misuse of the computers. The police computer crime squad have indicated that they would be prepared to prosecute individuals involved in such activities in schools.

7.3 Remedies and Resources

a) Violations, or allegations of violations, of the expectations for College computer network access, will be dealt with in the first instance by the class teacher or the teacher-librarian, as applicable. Most violations will be reported to the ICT Manager and also to the College Administration, who may take further action. Serious violations may be reported to the College Board and/or the police, if appropriate.

b) If you are accused of any violations of the requirements for using College computer resources, you will have all of the rights and privileges that you would have if you were accused of any other offence in the College, such as vandalism, fighting and so forth.

c) The ICT Manager has the right to restrict or terminate network and Internet access at any time and for any reason. Furthermore, the ICT Manager has the right to monitor network activity in any form that necessary to maintaining the integrity of the network.

8. SOCIAL MEDIA

a) Social media refers to the use of web-based and mobile technologies and associated platforms that allow users to easily publish, share, and discuss content in highly interactive communications. The ever-changing and inherently public nature of these and other forms of online communication present a range of challenges in safeguarding the College community, its staff, and most importantly the safety and security of the College's students.

b) The College recognises the potential value of Social Media as an effective educative and social tool for expressing views, comments, ideas and criticism on a whole range of issues. The College expects students to use Social Media in a respectful and responsible manner. Social Media should not be used to insult, present offensive or inappropriate content or to misrepresent the College or any member of the College community.

c) It is expected that students will uphold the ethos of the College both within and without; this includes the context of all Social Media interactions.

8.1 Social Media Channels and Platforms

a) There are various forms of social media channels and there are always new forms of social media being developed. Generally, we consider any platform or channel that offers individuals the opportunity to connect with people, create and share information and ideas, and develop relationships through online communities and networks as 'social media'.

b) The main forms of social media may include, but are not limited to:
   i. social networking sites (e.g. Facebook, MySpace, Google+, Foursquare, LinkedIn, Bebo, Friendster, Reddit);
   ii. video and photo sharing sites (e.g. YouTube, Instagram, Pinterest);
   iii. micro-blogging sites (e.g. Twitter, Posterous, Dailybooth);
   iv. blogs, including corporate blogs and personal blogs or blogs hosted by traditional media publications;
   v. podcasts, including corporate podcasts and personal podcasts;
   vi. forums, chat channels, and discussion boards (e.g. local discussion boards such as Whirlpool, Yahoo! Groups or Google Groups, or chat programs such as Discord);
   vii. virtual game worlds (e.g. World of Warcraft, Mnecraft, Roblox);
   viii. virtual social worlds (e.g. Second Life);
   ix. online encyclopaedias (e.g. wikis such as Wikipedia, Geo-wiki, GeoNames and Sidewiki);
   x. any other websites that allow individual users or companies to use simple publishing tools, (collectively called Social Media).

8.2 Procedures and Guidelines

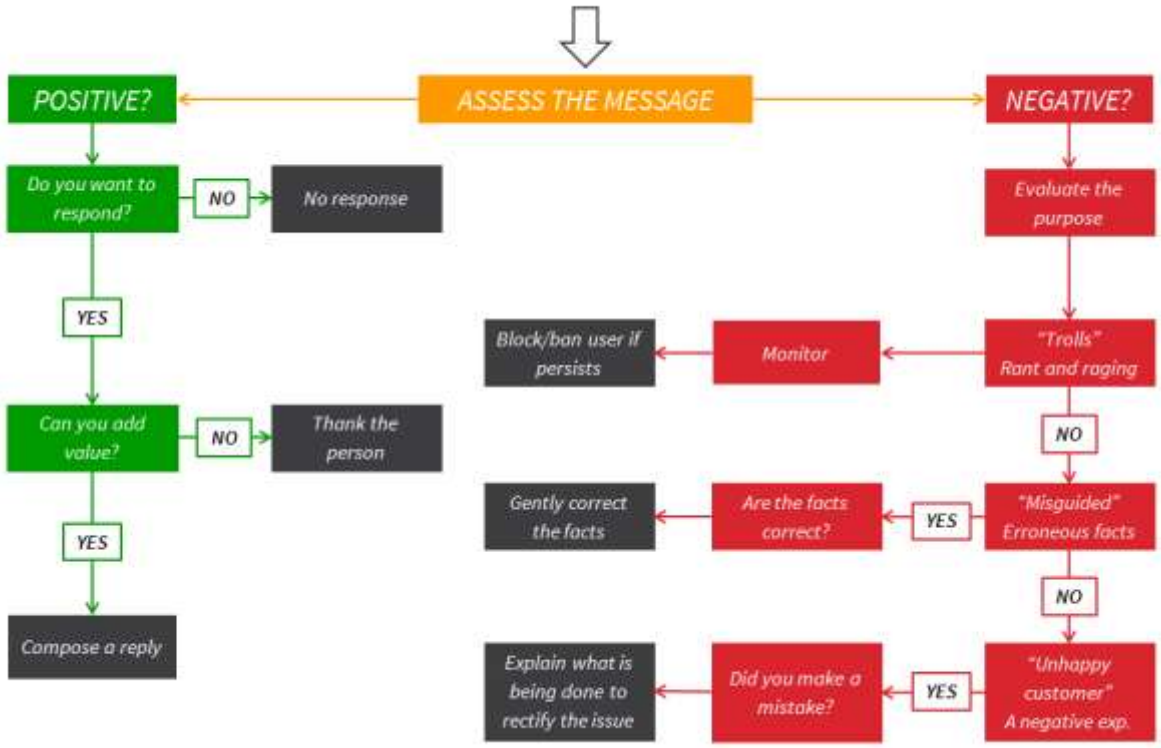
a) Students are expected to show respect to others, including members of the College community. Students are also expected to give due respect to the reputation and good name of the College.

b) When using Social Media, students are expected to ensure that they:
   i. respect the rights and confidentiality of others;
   ii. do not impersonate or falsely represent another person;
   iii. do not bully, intimidate, abuse, harass or threaten others;
   iv. do not make defamatory comments;
   v. do not use offensive or threatening language or resort to personal abuse towards each other or members of the College community;
   vi. do not post content that is hateful, threatening, pornographic, or incites violence against others;
   vii. do not harm the reputation and good standing of Rehoboth Christian College or those within its community;

viii. do not film, photograph or record members of the College community without permission of the College or use film, photographs or recordings without permission of the College.

c) A breach of this policy will be considered by the Principal or his/her delegate, such as Deputy Principal or Head of Department and will be dealt with on a case-by-case basis. All reports of cyber bullying and other technology misuses will be investigated fully and may result in a notification to Police where the College is obliged to do so. Sanctions may include, but are not limited to, the loss of computer privileges, detention, suspension, or expulsion from the College. Students and Parents must be aware that in certain circumstances where a crime has been committed, they may be subject to a criminal investigation by Police over which the College will have no control.

8.3 Responding on Social Media



The Australian Communication and Media Authority (ACMA) Online Social Networking Factsheet also provides further tips and useful information on managing your online identity. A copy of this is available on request from your campus office.

9. CYBER SAFETY

a) Cyber safety refers to the safe usage of the Internet and ICT equipment/devices. Many if not all of the previous sections have touched on this already, as it should rightly be involved in every action we take online.

b) So that you can stay up to date on this issue, the College will run an annual Cyber Smart course, which you will be expected to attend. There are some specific aspects of Cyber-Safety that are always good to know and which we will now examine.

9.1 User Vigilance

When you are using the Internet to communicate with others, keep the following in mind:

- You cannot see them;
- You cannot tell how old they are or even what gender they are;
- They can tell you anything, and you cannot always be sure what they are telling you is true;
- Absolute privacy cannot be guaranteed in a network environment, so you need to think carefully about what you say and how you say it.
- For your own safety and for the safety of others, remember to exercise caution when you are communicating with people in the outside world. Do not give out your home phone number or your address to anyone. They do not need to have that information.
- If you feel there is a problem or if you feel uncomfortable with the information someone is giving you, tell your teacher or the ICT Manager immediately.

9.2 Filtering policies

a) As part of our cyber safety plan, the College applies filtering to all on site connections. Although this can never be 100% effective, the policies are based on the fact that, to the greatest degree within our power, we desire to:
   i. protect our students from accidental or intended viewing of inappropriate content;
   ii. protect our students from malicious outside influence;
   iii. prevent time wasting and maintain a focus on learning;
   iv. prevent malware infection and maintain a secure network.

b) Although these filters may be overridden under the supervision of a teacher in class and in order to support specific learning outcomes, our filtering normally aims to prevent access to the following types of content:
   i. sites that promote or sell alcohol;
   ii. activities that violate human rights including murder, sabotage, bomb-building, etc.;

iii. information about illegal manipulation of electronic devices, encryption, misuse, and fraud;
iv. sites that promote relationships and dating;
v. gambling, lottery, casinos, online poker, and betting agencies;
vi. use or information on drugs, misuse of prescription drugs, and other compounds, including, but not limited to:
    - sites giving non-clinic descriptions or stories about being high;
    - sites on legalising marijuana;
vii. sites with adult content, including, but not limited to:
    - sites that discuss sex and sexuality, pregnancy, and abortion;
    - sites that use profanity or are offensive, disgusting, or tasteless.
    - sites with pornographic or nude imagery;
viii. sites containing instructions on how to commit violence, including, but not limited to:
    - militancy, torture, crime scene photos, descriptions, or pictures of a gory nature;
    - sites that promote violence or sedition;
    - guns and weapons;
ix. sites that exist primarily for users to chat to each other in real-time;
x. sites used to send text messages to phones.
xi. sites dedicated to forums, newsgroups, or bulletin boards.
xii. warez and other illegal software or copy-protected content.
xiii. download sites such as such as peer-to-peer (P2P) and BitTorrent sites, and any site with a repository of downloadable items such as software, screen savers, web templates, ringtones, etc;
xiv. sites about TV, movies, celebrity gossip, and entertainment, including, but not limited to:
    - sites devoted to video content and download;
    - in-browser clips, shows, or movies.
xv. computer games and related sites, including massive multiplayer, flash, and other forms of online gaming;
xvi. politically extreme right/left-wing groups, sexist or racial remarks, religious hate, or the promotion of bigoted views;
xvii. portal sites and parked domains that contain no information of their own;
xviii. social networking and related websites, which are designed with the purpose of giving users a public space to talk about themselves, upload media, and link to their friends;
xix. sites responsible for hosting online advertisements, including advertising graphics, banners, and pop-up content;
xx. proxies and anonymisers for accessing web-based content, including any site that can be used to bypass filtering;
xxi. sites that have been compromised by someone other than the site owner, including, but not limited to:
    - sites that are vulnerable to particular high-risk attacks;
    - sites that contain malware, infected images, or that have been defaced;

xxii. manipulated websites and emails for fraudulent purposes (phishing), including sites that impersonate other sites with the intent of stealing information from visitors;
xxiii. websites found inside junk messages;
xxiv. sites hosting software that installs on a computer with the intent of collecting information or making system changes without user consent;
xxv. sites that attempt to trick users or exploit browser vulnerabilities in order to install software automatically.

c) Any queries about the nature of these filters should be directed in the first instance to the ICT Manager.

9.3 Predatory Behaviour and Child Protection

a) Safe usage of the internet involves a whole range of issues to consider, and many have been covered already. However, the issue of paedophilia and other predatory behaviours in online environments is an important one for students and parents to be aware of, even if it is unpleasant to talk about.

b) Below are some Australian Government NetAlert guidelines worth remembering while online:
   i. Paedophiles can socialise together, trawl for inappropriate content (such as child pornography), and easily make collections of this that can be distributed to others.
   ii. They can pretend to be people other than themselves and they find a sense of security by operating from the confines of their homes.
   iii. Grooming children online with the intention to meet them in real life is an activity many undertake.
   iv. They often set up bogus email accounts and handles (a nickname a person may adopt while on the Internet) to protect their identity online.
   v. Students need to think carefully about the handles they choose for themselves. Handles such as ‘Angel-Babe’, ‘Sweet-Sixteen’, or ‘SexyKid’ may appear harmless on the surface; however, they can attract the wrong attention. Paedophiles are often attracted to people with these types of names.
   vi. Paedophiles may also erase the history of what they have done online from their personal computers, making it a lengthy task for authorities to charge them with an offence.
   vii. Paedophiles conduct numerous activities online, including:
      - swapping pornographic images of children in chat rooms, through email, or via P2P networks;
      - swapping personal information of children that they have collected;
      - participating in online communities with the intention of grooming children for personal sexual gratification or to meet them in person;
      - forming networks with other paedophiles;
      - trading techniques on how to avoid the authorities.

c) The WA Police, in conjunction with AISWA, the Department of Education and Training, and the Catholic Education Office have formed the Internet Safety Working Party. The aim of the working party is to implement strategies through schools and community networks to educate students and parents on safe internet behaviours.

d) The working party has produced a DVD titled Keeping Safe on the Internet. The DVD features two presentations – one aimed at students aged 12 to 16, and the other specifically for parents.

9.4 Platform Security and Student-Owned Equipment

a) The platform used to access the College network will vary depending on circumstances. This may include one or more of the following:
   i. College-owned Mac or PC;
   ii. College-owned iPad or tablet;
   iii. College-owned netbook

b) Where the equipment used is College-owned and used on the College network, the College will assume responsibility for security and filtering. Where the equipment is parent-owned, security and filtering will be the responsibility of parents. The College will assist parents in this role with the provision of instruction, support, resources, and where applicable, direct advice from the ICT Manager.

10. DEVICE LOAN PROGRAM

a) Before a device will be issued to a student, parents and students must have read and completed the ICT Student Device Loan Program Agreement. This agreement contains the terms and conditions for the loan.

b) When signed by the student and their parent/guardian, the Agreement t becomes a legally binding contract. Any questions or concerns about the Agreement should be directed to the ICT Manager.