Robinvale College
"Great Learning for a Thriving Community"

	INTERNET POLICY AND PROCEDURES	
College Council President:		**Date:** 14-5-18
College Principal:		**Date:**
Date ratified:	**Date to be reviewed:**	

I. POLICY STATEMENT

The internet offers a huge potential of benefits for teaching and learning. It offers wonderful opportunities for students and teachers to contribute to the world community on the web. Blogs, social networking spaces such as Facebook and instant messaging tools such as Skype are now part of students' 'life on the web'.

Students can:

- explore the world online
- visit museums and libraries around the world
- access rich information resources to support research and investigations
- communicate and collaborate with people all over the world
- publish to the web
- take part in online activities via APPs

Robinvale College has an important role in preparing students for these 'online communities', even though students may not access some online communities at school (e.g. Facebook).

Before our students start to explore the Internet, it's crucial to make sure everyone understands what they should and shouldn't be doing online.

Behaving safely online means:

- protecting their own privacy and personal information (we used to call it 'stranger danger')
- selecting appropriate spaces to work and contribute
- protecting the privacy of others (this can be sharing personal information or images)
- being proactive in letting someone know if something is 'not quite right' - at home this would be a parent or guardian, at school a teacher

These principles of safety and responsibility are not specific for the web but certainly apply to the use of the internet at school. Just as in the real world, the virtual world of the internet involves some risks. Robinvale College has developed proactive strategies that help to minimise these risks to our students.

2. GUIDELINES

2.1   Use of the school's network to access the Internet and Internet services, including electronic mail and the World Wide Web, will governed by an Acceptable Use Procedures (AUP) for the Internet.

[Version 1.0   Created 28/3/2018]
[Review due 28/3/2019]

2.2 The Acceptable Use Procedures (AUP) is intended to encourage responsible action and to reflect a respect for the ability of its adherents to exercise good judgement.

2.3 Independent student use of the internet will only be permitted where students and their parents/carers provide written acknowledgement that students agree to act in accordance with the standards of conduct established in the Acceptable Use Procedures (see appendix A).

2.4 Students can expect sanctions if they act irresponsibly and disregard their obligations to other users and the school as the provider of their Internet access.

2.5 Students must not use the school network in breach of a law or to commit an offence.

3. PROGRAM

3.1.1 The use of the school's network is subject to the Acceptable Use Procedures (see appendix A). Briefly this means that the school's network can be used only by staff, students and associated individuals (e.g. visiting teachers) and only for, or in connection with the educational or administrative functions of the school.

3.1.2 The Acceptable Use Procedures (AUP) is intended to operate within and be consistent with existing school policies and procedures in areas such as:

- **Anti-bullying (including cyber-bullying) and Anti-harassment**
- **Student Welfare**

3.2.1 Responsibility and accountability for network security is the shared responsibility of all network users. It is the responsibility of the student to protect his/her password and not divulge it to another person. If a student knows or suspects his/her account has been used by another person, the account holder must notify a teacher immediately.

3.2.2 All messages created, sent or retrieved on the school's network are the property of the school, and should be considered public information. The school reserves the right to access and monitor all messages and files on the computer system as deemed necessary and appropriate. Internet messages are public communication and are not private. All communications including text and images can be disclosed to law enforcement and other third parties without prior consent from the sender.

3.3 Independent student use of the internet on the school's network will only be permitted where students and their parents/carers provide written acknowledgement that students agree to act in accordance with the standards of conduct established in this policy document and as set-out in the Acceptable Use Procedures (AUP).

3.4.1 For breaches of the Acceptable Use Procedures students can face a number of consequences depending on the severity of the breach and the context of the situation. More than one consequence 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's discipline policy

3.4.2 Bullying and harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual or group's race' religion, national origin, physical attributes, or sexual preference will be transmitted. Violations of any guidelines listed above may result in disciplinary action.

3.5 While the Internet may be largely a self-regulated environment, the general principles of law and community standards still apply to communication and publishing via the Internet. In addition to school penalties, there are legal sanctions for improper use of the Internet.

4. LINKS AND APPENDICES (including processes related to this policy)

Links which are connected with this policy are:

- https://esafety.gov.au/

- https://fuse.education.vic.gov.au/Resource/LandingPage?ObjectId=86ad26cf-d96a-4b76-8b45-64a7b87f7bf3&SearchScope=All

- legal.services@edumail.vic.gov.au

Appendices which are connected with this policy are:

- The school's Anti-bullying (including cyber-bullying) and Anti-harassment Policy
- The school's Student Welfare Policy
- Appendix A: Acceptable Use Procedures (AUP) for the Internet

5. EVALUATION

This policy will be reviewed annually or more often if necessary due to changes in regulations or circumstances.

[Version 1.0   Created 28/3/2018]
[Review due 28/3/2019]

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 development of staff. Any behaviour that interferes with these primary objectives will be considered an infringement of Acceptable Use.

1.0 General Policies

- use of computer/internet resources is for **educational purposes only**
- access to the Internet must be supervised by a staff member
- appropriate language must be used in **all** communications
- 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: No eating of food while using school laptop or desktop computer

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 (games or other executables)
- 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
- access the internet using netbooks unless instructed by a teacher

2.0 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.

Regardless of the real or supposed levels of understanding, students are NOT authorised to attempt the repair or adjustment of any college hardware or software. Any such attempt will be regarded as a violation of network security. Any problem with equipment or software must be referred to an authorised person.

3.0   Software and Operating Systems

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

Students must 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 unless authorized by a teacher
- 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

4.0   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 T:) 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:

[Version 1.0   Created 28/3/2018]

[Review due 28/3/2019]

o program files (EXE, COM)
o compressed files (ZIP, ARJ, LHZ, ARJ, TAR, etc)
o picture files, video files, music files etc unless they are required for a school task
o obscene material - pictures or text
o obscene filenames
o insulting material
o copyrighted material

- intentionally seek information on, obtain copies of, or modify files, other data or passwords belonging to other users

5.0 Printing

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

6.0 Internet usage

Students must use the internet 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.

6.1 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, 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**
    o messages containing inappropriate content are automatically reported to the Principal

- teachers will set their own guidelines for use of email in class time
- Use capitals in bold format – which constitutes shouting.

Students will not:

- send offensive mail
- send unsolicited mail to multiple recipients ("spam")
- use email for any illegal, immoral or unethical purpose

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

    http://www.smartcopying.edu.au/

[Version 1.0   Created 28/3/2018]
[Review due 28/3/2019]

Robinvale College is required to protect all personal and health information they collect in accordance with the Privacy and Data Protection Act 2014 and health Records Act 2001 (Victoria Privacy Laws). In the event that an online service will collect, use, disclose or store personal information or health information, schools should undertake a privacy impact assessment (PIA) to identify and risks involved.

Privacy Impact Assessment

This is a planning and auditing tool the school will complete when they are preparing to use an online service.

The Link

https://edugate.eduweb.vic.gov.au/Services/legal/Pages/CP%20Information-Sheets.aspx

Online services are commonly referred to as cloud services, apps or SaaS (Software- as-a Service) and are accessed through an internet website portal or by downloading software into the schools digital environment. Examples of online services are Facebook, Twitter, Compass, blogs, Gmails, wikis, Google Apps, Microsoft 356 and iTunes.

6.5   The School Web site

Material placed onto the school web site must:

- Be checked for appropriateness and (as far as possible) accuracy by the principal
- 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.

7.0   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**

[Version 1.0   Created 28/3/2018]
[Review due 28/3/2019]

8.0   The Student and Parent Support Kit

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.

Robinvale College

<div style="background:#5b9bd5">

Return Sheet to Administration Office

See Part C for support Information

</div>

Part A - Agreement to be signed by the student and parent

When I use technology, both at school and at home I have responsibilities and rules 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:

- behave according to the school Code of Conduct when online or using mobile technology
- 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

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

- 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

[Version 1.0   Created 28/3/2018]
[Review due 28/3/2019]

To this end, when using my mobile device as a phone I will:

- keep my phone on silent during class times and place it in the office, only make or answer calls and messages outside of school hours - except for specified learning purposes
- protect the privacy of others and never post private information about another person using SMS messages
- I will not use my own Mobile Internet modem or use my own Mobile Phone as a Wi-Fi hotspot as wireless network, printing and Internet access will be provided.

This Acceptable Use Policy also applies to students during school excursions, camps and extra-curricular 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: _____

When this Acceptable Use Agreement for the use of the school's internet has been completed and signed please return it to the School.

Please detach this return slip from the *Guidelines and Conditions Acceptable Use Procedures for the school's Internet* document before it is returned to the school.

To be kept by the Parent or Guardian

Part B - The schools' support for responsible and ethical use of technology?

Robinvale College uses the internet as a teaching and learning tool. We see the internet and mobile technology as valuable resources, but acknowledge they must be used responsibly.

Your child has been asked to agree to use the internet and mobile technology responsibly at school. Parents should be aware that the nature of the internet is such that full protection from inappropriate content can never be guaranteed.

At Robinvale College we have a cyber-safe and responsible use program across the school and reinforce the values and behaviours of the school code of conduct when students use technology and the internet.

These may include:

- provide a filtered internet service
- provide access to/only to the DEECD search engine CONNECT (https://fuse.education.vic.gov.au/Primary), which can be used to restrict students to only using websites that have been teacher recommended and reviewed
- provide supervision and direction in internet activities and when using mobile technologies for learning
- have an Information Literacy program
- use mobile technologies for educational purposes (e.g. podcasts or photos from excursions)
- work towards setting tasks that ask your child open questions, so they can't copy and paste all answers from the internet
- provide support to parents to understand this agreement (e.g. language support)
- provide support to parents through information evenings and through the document attached to this agreement

Should your child be found to use the school's Information and Technology resources inappropriately your child will be counseled and some penalties may apply;

These may include:

- 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

Part C - Advice for Parents

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 Facebook (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 your 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?

http://www.education.vic.gov.au/about/programs/bullystoppers/Pages/advicecybersafe.aspx

http://www.education.vic.gov.au/about/programs/bullystoppers/Pages/advicecyberbully.aspx

Support information for parents around the agreement

When I use technology, both at school and at home I have responsibilities and rules to follow.

Robinvale College believes the teaching of cyber-safe and ethical behaviour is essential in the lives of students and is best taught in partnership between home and school.

21st Century students spend increasing amounts of time online learning and socialising. These online communities need cybercitizens who do the right thing by themselves and others online, particularly when no one is watching.

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

It is important to note that some online activities are illegal and as such will be reported to police. This includes harassment of others and publishing of inappropriate images.

Behaving according to school Code of Conduct

The school's Code of Conduct encompasses not only the rules of the school, but also those desired behaviours and values that your school community believes are important for all students.

Not giving out personal details or details of other students including full names, telephone numbers, addresses and images and protecting password details.

Many students like to publish information about themselves and their friends in spaces and Apps like Facebook, Instagram, snapchat etc. 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.

[Version 1.0   Created 28/3/2018]
[Review due 28/3/2019]

Using the technology at school for learning, using the equipment properly and not interfering with the work or data of another student

By just taking care with the equipment, printing and downloading from the internet students can save time, money and the environment. Students often see the internet as 'free', but just looking at a page on the internet is considered a download and the cost is charged somewhere. The repair and support of the school's technology is another issue and as many computers are shared at school, their care is important.

Not bringing or downloading unauthorised programs (including games) to the school or run them on school computers

The school connects all of the computers through a network. The introduction of unknown games or files could introduce viruses etc and these put all school equipment and student work at risk.

Not looking for rude or offensive sites.

Filters block a lot of inappropriate content, but they are not foolproof. Students who deliberately seek out inappropriate content or use technology that bypasses filters will have their internet access reviewed and their parents will be informed immediately.

Using the internet/mobile technology at school to learn.

It is important to realise that there is a time for fun and a time for work (even on the internet). Staying on task will reduce risk of inappropriate access and teach students strategies to use the internet or mobile technologies for their learning.

Asking teacher to help get permission before using information or pictures

Music, information, images and games on the internet are owned by someone. The term copyright is a legal one and there are laws to enforce it.

By downloading a freebie you can risk bringing a virus or spyware to the computer or system. These can destroy a computer system or provide hackers with details such as passwords and bank accounts.

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. The school is teaching information literacy skills, which enable students to locate, evaluate, and use information effectively on the internet.

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. For example, if you say to your child, "Tell me about wombats" you might encourage him/her to copy and paste facts and images about the wombat. However, if you ask "What would a day in the life of a wombat be like?" you may encourage your child to think about different aspects of the animal's life and draw together the different pieces of information.

Talking to my teacher or another adult if I need help or see something I don't like online

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 students is the best way to keep students safe. Students 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 or https://esafety.gov.au/about-the-office/contact-us

Questions for teacher/ parent/ student discussion

What can you do?

- You found the car picture online you were searching for, but it includes a naked lady!
- Someone keeps messaging nasty and upsetting comments about you and your friends on your mobile phone and online.
- A person you have met online asks you to give them your full name and phone number and suggests you meet. What if you have chatted with them for a long time?
- You are sent a message which has been forwarded by someone else. It has embarrassing comments /image about someone you know.
- A game online will only let you play it if you give your name, address, phone number, DOB etc
- In an online space/chat someone suggests you all exclude /block a classmate.
- Your friend has an online profile published (not set to private) you can see their personal details and photos. Other people you know are in the photos.
- A friend tells you about a great site where there is 'free' music to download.

Attachment A

Online Services Assessment

General Information

a) *What is the online service called?*

COMPASS

b) *What does the online service provide?*

Student / Teacher access to timetables and classroom resources. Parental access to teacher comments for their child. School communication to the school community.

c) *Who is the service provider?*

COMPASS

d) *Who will administer the technology at the school?*

PRINCIPAL

e) *How will the school be using the online service?*

Student / Teacher access to timetables and classroom resources. Parental access to teacher comments for their child. School communication to the school community.

f) *Where can information about the online service be found?*

https://www.robinvale.vic.edu.au/

Use and Disclosure by School

g) *What information of individuals will the school use and disclose to the service provider?*

https://www.robinvale.vic.edu.au/child-safety-statement

h) *How will the school use the information of individuals?*

https://www.robinvale.vic.edu.au/child-safety-statement

i) *Where will the service provider store the information disclosed to it?*

Victoria, Australia

j) *What school policies will apply to the use of the online service?*

ICT Policy 2018

k) *Will the school be able to access and retrieve all content, including messages or other communications from the online service?*

The school has the capacity to access and retrieve the following list of records that form part of the content of the online service:
- Student medical information
- Parent or carer contact information;
- Teacher entries
- Learning tasks and subject resources

[Version 1.0   Created 28/3/2018]
[Review due 28/3/2019]

l)	*Is there an alternate method of access to information, notifications, communications and transactions enabled through the online service?*	The school Bulletin entitled The Grapevine is issued every 2 weeks. This enables: • parents and carers who do not consent to the use of the online service; • students and parents and carers who do not have access to the online service; • whose use of the online service is affected by the accessibility restrictions of the online services (i.e. does not cater for visual disability.

Collection by Service Provider

m)	*How will the service provider use information of individuals that is collected from the school?*	The service provider will use this information to create a login identification for parents.
n)	*What information of individuals will the service provider collect in the course of the use of the online service?*	None.
o)	*How will the service provider use information collected in the course of an individual's use of the online service?*	Not applicable.

Copyright

p)	*What content or works will individuals share in the course of their use of the online service?*	The student may create work that contains information about them or their family, including: • art work or photographs • video or digital story • comments and insights on information • school projects and assessment materials • podcasts and other streaming outputs • email content • written work, such as assignments, essays or poetry • communication with peers.
p)	*Who will be able to see the content or work?*	School leadership and teachers have general access. Restricted access to students and parents.

q) *Whilst students own copyright in the works they produce, who will have rights to reproduce and/or use the works?*

The school has the rights to reproduce the work in a restricted form.

r) *If the school wants to use and reproduce the works of students, what types of work, how and where will it be used or reproduced?*

General display of works on the school website, social media instruments and school magazine and bulletins.