Ringwood Secondary College

Digital Technologies (Internet, Social Media and Digital Devices) Policy

Version No: 1 **Date: October** 2019

Committee: Policy and Education

PURPOSE

To ensure that all students and members of our school community understand:

(a) our commitment to providing students with the opportunity to benefit from digital technologies to support and enhance learning and development at school including our 1-to-1 device program which includes iPads at Years 7 and 8 and Macbooks at Years 9-12
(b) expected student behaviour when using digital technologies including the internet, social media, and digital devices (including computers, laptops and tablets)
(c) the school's commitment to promoting safe, responsible and discerning use of digital technologies, and educating students on appropriate responses to any dangers or threats to wellbeing that they may encounter when using the internet and digital technologies
(d) our school's policies and procedures for responding to inappropriate student behaviour on digital technologies and the internet.

SCOPE

This policy applies to all students at Ringwood Secondary College. This policy is to be read in conjunction with the Ringwood Secondary College Cybersafety and Acceptable Use Agreement – please refer to Annexure A

Staff use of technology is governed by the Department's *Acceptable Use Policy*.

DEFINITIONS

For the purpose of this policy, 'digital technologies' are defined as being any networks, systems, software or hardware including electronic devices and applications which allow a user to access, receive, view, record, store, communicate, copy or send any information such as text, images, audio, or video.

POLICY

Vision for digital technology at our school:

Ringwood Secondary College understands that safe and appropriate use of digital technologies including the internet, apps, computers and tablets provide students with rich opportunities to support learning and development in a range of ways.

Through increased access to digital technologies, students can benefit from enhanced learning that is interactive, collaborative, personalised and engaging. Digital technologies enable our students to interact with and create high quality content, resources and tools. It also enables

personalised learning tailored to students' particular needs and interests and transforms assessment, reporting and feedback, driving new forms of collaboration and communication.

Ringwood Secondary College believes that the use of digital technologies at school allows the development of valuable skills and knowledge and prepares students to thrive in our globalised and inter-connected world. Our school's vision is to empower students to use digital technologies safely and appropriately to reach their personal best and fully equip them to contribute positively to society as happy, healthy young adults.

iPads at Ringwood Secondary College

Classes at Ringwood Secondary College are delivered with the use of iPads. Students must bring a charged iPad to school each day to be used during class time for different learning activities.

Instructions for purchase and delivery of the College iPad is posted on the college website.

Students are required to have their own iPad/Macbook Air that must:

- be brought to school in a protective case
- have at least 10 GB of storage
- operate on the College server and maintain support through ITS
- have access to Microsoft Word, Excel and PowerPoint.

Ringwood Secondary College has in place arrangements to support families who may be experiencing long or short-term hardship to access iPads/Macbooks for schoolwork. We also have a number of spare iPads/Macbooks that can be loaned to students in certain circumstances. Daily hire available and loan devices for insurance work.

Safe and appropriate use of digital technologies:

Digital technology, if not used appropriately, may present risks to users' safety or wellbeing. At Ringwood Secondary College, we are committed to educating all students to be safe, responsible and discerning in the use of digital technologies, equipping them with skills and knowledge to navigate the digital age.

At Ringwood Secondary College, we:

- use online sites and digital tools that support students' learning, and focus our use of digital technologies on being learning-centred
- restrict the use of digital technologies in the classroom to specific uses with targeted educational or developmental aims
- supervise and support students using digital technologies in the classroom
- effectively and responsively address any issues or incidents that have the potential to impact on the wellbeing of our students
- have programs in place to educate our students to be promoting safe, responsible and discerning use of digital technologies, including Cybersafety Training for students, parents and staff
- educate our students about digital issues such as online privacy, intellectual property and copyright, and the importance of maintaining their own privacy online

- actively educate and remind students of our *Student Engagement* policy that outlines our School's values and expected student behaviour, including online behaviours
- have an Acceptable Use Agreement outlining the expectations of students when using digital technology at school
- use clear protocols and procedures to protect students working in online spaces, which includes reviewing the safety and appropriateness of online tools and communities, removing offensive content at earliest opportunity
- educate our students on appropriate responses to any dangers or threats to wellbeing that they may encounter when using the internet and other digital technologies
- provide a filtered internet service to block access to inappropriate content
- refer suspected illegal online acts to the relevant law enforcement authority for investigation
- support parents and carers to understand safe and responsible use of digital technologies and the strategies that can be implemented at home through regular updates in our newsletter and annual information sheets.

Distribution of school owned devices to students and personal student use of digital technologies at school will only be permitted where students and their parents/carers have completed a signed Acceptable Use Agreement.

It is the responsibility of all students to protect their own password and not divulge it to another person. If a student or staff member knows or suspects an account has been used by another person, the account holder must notify classroom teacher or co-ordinator, immediately.

All messages created, sent or retrieved on the school's network are the property of the school. The school reserves the right to access and monitor all messages and files on the computer system, as necessary and appropriate. Communications including text and images may be required to be disclosed to law enforcement and other third parties without the consent of the sender.

Student behavioural expectations

When using digital technologies, students are expected to behave in a way that is consistent with Ringwood Secondary College's *Statement of Values, Student Wellbeing and Engagement* policy, and *Bullying Prevention* policy.

When a student acts in breach of the behaviour standards of our school community (including cyberbullying, using digital technologies to harass, threaten or intimidate, or viewing/posting/sharing of inappropriate or unlawful content), Ringwood Secondary College will institute a staged response, consistent with our policies and the Department's *Student Engagement and Inclusion Guidelines*.

Breaches of this policy by students can result in a number of consequences which will depend on the severity of the breach and the context of the situation. This includes:

- removal of network access privileges
- removal of email privileges
- removal of internet access privileges
- removal of printing privileges

- other consequences as outlined in the school's *Student Wellbeing and Engagement* and *Bullying Prevention* policies.

REVIEW CYCLE

This policy was last updated in October 2019 and is scheduled for review in October 2022.

ANNEXURE A: ACCEPTABLE USE AGREEMENT

Acceptable Use Agreement

RINGWOOD SECONDARY COLLEGE

CYBERSAFETY AND ACCEPTABLE USE AGREEMENT FORM FOR STUDENTS

To the student, and the parent/legal guardian/caregiver

1. Please read this page carefully, to check you understand your responsibilities under this agreement
2. Sign the appropriate section on this form
3. Detach and return this form to the College office
4. Keep the document for future reference, as well as the copy of this signed page which the College will provide.

We understand that Ringwood Secondary College will:

- do its best to keep the College cybersafe, by maintaining an effective cybersafety programme. This includes working to restrict access to inappropriate, harmful or illegal material on the Internet or College ICT (Information and Communication Technologies) equipment/devices at College or at College-related activities, and enforcing the cybersafety regulations and responsibilities detailed in use agreements. This also includes protecting the holder of this agreement from external or public sources attempting to access the cybersafe environment within the College
- keep a copy of this signed use agreement form on file
- respond appropriately to any breaches of the use agreements
- provide members of the College community with cybersafety education designed to complement and support the use agreement initiative
- welcome enquiries from students or parents about cybersafety issues.

Student's section

My responsibilities include:

- **I will read** this Cybersafety and Acceptable Use Agreement document carefully
- **I will follow** the cybersafety rules and instructions whenever I use the College's computer network, Internet access facilities, computers and other College ICT equipment/devices
- **I will also follow** the cybersafety rules whenever I am involved with privately-owned ICT devices/equipment on the College site or at any College-related activity, regardless of its location
- **I will avoid** any involvement with material or activities which could put at risk my own safety, or the privacy, safety or security of the College or other members of the College community
- **I will take proper care** of my computer and other College ICT equipment/devices and be responsible for its safe storage. I know that if I have been involved in the damage, loss or theft of ICT equipment/devices, my family may have responsibility for the cost of repairs or replacement

- **I will not** install or use any software (such as peer to peer sharing or VPN applications) in an attempt to bypass or circumvent the College internet filtering system.
- **I will keep** this document somewhere safe so I can refer to it in the future
- **I will ask** the relevant staff member if I am not sure about anything to do with this agreement.
- **I understand** that it is my sole responsibility to regularly back up my work to either the College network and/or an external source, such as USB drive. I understand that the College ICT team is not responsible for backing up. In the extreme event of student work requiring backing up by the College, costs will be charged for time taken.
- **I will abide** by copyright laws. I understand that downloading any music, videos, software etc that I do not own is illegal.
- **I will not** interfere with any laptop/ICT device that belongs to another student or staff member.
- **I understand** that allowing anyone other than myself or college appointed ICT Support team to interfere with or use my laptop/ICT device will void the warranty.

I have read and understand my responsibilities and agree to abide by this Cybersafety and Acceptable Use Agreement.

I know that if I breach this use agreement there may be serious consequences.

Name of student: ..... **Form:** .....

Signature: ..... **Date:** .....

Section for parent/legal guardian/caregiver

My responsibilities include:

- **I will read** this Cybersafety and Acceptable Use Agreement document carefully and discuss it with my son/daughter so we both have a clear understanding of my child's role in the College's work to maintain a cybersafe environment
- **I will ensure** this use agreement is signed by my child and by me, and returned to the College
- **I will encourage** my son/daughter to follow the cybersafety rules and instructions
- **I will contact** the College if there is any aspect of this use agreement I would like to discuss.
- **I will ensure** that my son/daughter understands and follows their legal copyright responsibilities.
- **I understand** that allowing others, beyond immediate family, to access or use my son/daughters laptop/ICT device will void the warranty.

I have read this Cybersafety and Acceptable Use Agreement document and am aware of the College's initiatives to maintain a cybersafe learning environment, including the responsibilities involved.

Parent/Legal Guardian/Caregiver (Please circle which term is applicable.)

Name: .....

Signature: ..... **Date:** .....

CYBERSAFETY AND ACCEPTABLE USE AGREEMENT

FOR ALL RINGWOOD SECONDARY COLLEGE STUDENTS

OCTOBER 2019

This document is comprised of two sections:

Section 1 – Cybersafety in the College Environment

a) Important College cybersafety initiatives
b) General cybersafety rules

Section 2 – Information Specifically For Ringwood Secondary College Students

a) Additional information
b) Additional rules / responsibilities

Instructions for secondary students:

1. You and your parent/legal guardian/caregiver are asked to read Section A 'Cybersafety in the College Environment' and Section B 'Information Specificall for Secondary Students' carefully.
2. If help is needed to understand all the language, or there are any points your family would like to discuss with the College, let the College office know a soon as possible.
3. You and your parent/legal guardian/caregiver should then sign the Student Use Agreement Form at the back of Section B before you return that page t the College.
4. It is important to keep Section 1 and Section 2 for you and your family to read again in the future.

SECTION A – CY COLLEGE ENVIRONMENT

Important terms used in this document:

*(a) The abbreviation **'ICT'** in this document refers to the term 'Information and Communication Technologies'.*

*(b) **'Cybersafety'** refers to the safe use of the Internet and ICT equipment/devices, including mobile phones.*

*(c) **'College ICT'** refers to the College's computer network, Internet access facilities, computers, and other College ICT equipment/devices as outlined in (d) below. This also includes subsidiary or public organisation(s) equipment which may extend and/or be part of the college network infrastructure.*

*(d) The term **'ICT equipment/devices'** used in this document, includes but is not limited to, computers (such as desktops, laptops, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/receivers (such as portable CD and DVD players), and any other, similar, technologies as they come into use.*

IMPORTANT RINGWOOD SECONDARY COLLEGE CYBERSAFETY INITIATIVES

The values promoted by Ringwood Secondary College include establishing positive relationships in a safe and caring environment; cooperation, mutual respect, acceptance and trust; being fair, friendly, supportive and honest; developing and displaying ethics and personal integrity; and respecting the physical environment. The measures to ensure the cybersafety of the College environment which are outlined in this document are based on these core values.

The College's computer network, Internet access facilities, computers and other College ICT equipment/devices, such as student laptops and iPads, bring great benefits to the teaching and learning programmes at Ringwood Secondary College, and to the effective operation of the

College. However, it is essential that the College endeavours to ensure the safe use of ICT within the College community.

Thus Ringwood Secondary College has rigorous cybersafety practices in place, which include cybersafety use agreements for all College staff and students.

Cybersafety use agreement documents include information about obligations, responsibilities, and the nature of possible consequences associated with breaches of the use agreement which undermine the safety of the College environment. The cybersafety education supplied by the College to its learning community is designed to complement and support the use of this agreement. The overall goal of the College in this matter is to create and maintain a cybersafety culture which is in keeping with the values of the College, and legislative and professional obligations. All members of the College community benefit from being party to the use agreement and other aspects of the College cybersafety programme.

1. Cybersafety use agreements

1.1. All staff and students, *whether or not* they make use of the College's computer network, Internet access facilities, computers and other ICT equipment/devices in the College environment, will be issued with a user agreement. They are required to read these pages carefully, and return the signed use agreement form in Section B to the College office for filing. A copy of this signed form will be provided to the user.

1.1. All students *whether or not* they make use of the College's computer network, Internet access facilities, computers and other ICT equipment/devices in the College environment, will be issued with a user agreement. They are required to read these pages carefully, and return the signed use agreement form to the College office for filing. A copy of this signed form will be provided to the user.

1.2. Students are asked to keep the other pages of the agreement for later reference. (If necessary, a replacement copy will be supplied by the College's ICT Management Team).

1.3. The College encourages anyone with a query about the agreement to contact the ICT Management Team as soon as possible.

2. Requirements regarding appropriate use of ICT in the College learning environment

In order to meet the College's legislative obligation to maintain a safe physical and emotional learning environment, and be consistent with the values of the College:

2.1. The use of **the College's** computer network, Internet access facilities, computers and other College ICT equipment/devices, including but not limited to iPads and student laptops, on *or* off the College site, is limited to educational purposes appropriate to the College environment. This applies whether or not the ICT equipment is owned/leased either partially or wholly by the College. If any other use is permitted, the user(s) will be informed by the College.

2.2. The College has the right to monitor, access, and review all the use detailed in 2.1. The College will use remote access software to ensure appropriate use of ICT

devices and the College network. This includes personal emails sent and received on the College's computers and/or network facilities, either during or outside College hours.

2.3. The use of any **privately-owned/leased** ICT equipment/devices on the College site, or at any College-related activity must be appropriate to the College environment. This includes any images or material present/stored on privately-owned/leased ICT equipment/devices brought onto the College site, or to any College-related activity.

Such equipment/devices could include a laptop, desktop, PDA, mobile phone, camera, recording device, or portable storage (like a USB or flash memory device). Anyone unsure about whether or not it is appropriate to have a particular device at College or at a College-related activity, or unsure about whether the planned use of a particular device is appropriate, should check with the ICT Management Team.

Note that examples of a **'College-related activity'** include, but are not limited to, a field trip, camp, sporting or cultural event, *wherever its location*.

2.4. **When using a global information system** such as the Internet, it may not always be possible for the College to filter or screen all material. This may include material which is **inappropriate** in the College environment (such as 'legal' pornography), **dangerous** (such as sites for the sale of weapons), or **illegal**.

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

3. Monitoring by the College

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

3.2. The College monitors traffic and material sent and received using the College's ICT infrastructures. This will be examined and analysed to help maintain a cybersafe College environment.

3.3. The College will deploy filtering and/or monitoring software where appropriate to restrict access to certain sites and data, including email. Any attempt to obstruct, bypass of circumvent this software will constitute a breach of this agreement.

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

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

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

4. Ownership

1.1 Laptops/ICT equipment remain the property of the College and remain so until the laptop is purchased at the conclusion of the three year lease. In the event that the student leaves the College before the conclusion of the lease, the student may purchase the laptop/ICT equipment.

1.2 The College reserves the right to confiscate, reimage, delete software and/or modify user privileges on any laptops/ICT equipment due to breaches of this agreement.

5. Audits

5.1. The College will from time to time conduct an internal audit of its computer network, Internet access facilities, computers and other College ICT equipment/devices, or may commission an independent audit. If deemed necessary, auditing of the College computer system will include any stored content, and all aspects of its use, including email. An audit may also include any laptops provided or subsidised by/through the College or subsidised by a College-related source such as the Department of Education and Early Childhood Development.

6. Breaches of the use agreement

6.1. Breaches of the use agreement can undermine the values of the College and the safety of the learning environment, especially when ICT is used to facilitate misconduct.

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

Refer to the document 'Misdemeanours and Recommended Consequences Regarding the Use of Laptops and Related ICT Facilities'.

6.3. If there is a suspected breach of use agreement involving privately-owned ICT on the College site or at a College-related activity, the matter may be investigated by

the College. The College may request permission to audit that equipment/device(s) as part of its investigation into the alleged incident.

6.4. Involvement with **material** which is deemed 'age-restricted', or 'objectionable' (illegal) is a very serious matter, as is involvement in an **activity** which might constitute criminal misconduct, such as harassment. In such situations, it may be necessary to involve law enforcement in addition to any disciplinary response made by the College as a result of its investigation.

7. Other aspects of the College's cybersafety programme

7.1. The Cybersafety and Acceptable Use agreement operates in conjunction with other cybersafety initiatives, such as cybersafety education supplied to the College community. This education plays a significant role in the College's overall cybersafety programme, and also helps keep children, young people and adults cybersafe in all areas of their lives. If more information is required, the ICT Management Team can be contacted.

SECTION 1B - GENERAL CYBERSAFETY RULES

These general rules have been developed to support the 'Important Ringwood Secondary College Cybersafety Initiative's outlined in Section A.

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

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

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

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

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

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

2.3 **Privately-owned ICT.** Use of privately-owned/leased ICT equipment/devices on the College site, or at any College-related activity must be appropriate to the College environment. This includes any images or material present/stored on privately-owned/leased ICT equipment/devices brought onto the College site or to any College-related activity. It also includes the use of mobile phones which must not be used as a hotspot to connect other College owned devices to the internet in a way that bypasses or defeats the College's filtering system.. Any queries should be discussed with the ICT Management Team.

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

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

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

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

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

Refer to the document 'Misdemeanours and Recommended Consequences Regarding the Use of Laptops and Related ICT Facilities'.

3 Individual password logons (user accounts)

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

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

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

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

4 Disclosure of personal details

4.2 For personal safety, users should be very careful about revealing personal information about themselves, such as home or email addresses, or any phone

numbers including mobile numbers. Nor should such information be passed on about others.

5 Care of ICT equipment/devices

5.2 All College ICT equipment/devices should be cared for in a responsible manner and especially ensuring that laptops are carried in the bags or cases provided.

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

5.4 At school, when laptops are not being used or carried by the individual they should be securely stored in a locked locker

5.5 At the conclusion of the lease, or if the student leaves the College before the conclusion of the lease, the laptop/ICT device must be returned to the College in the same condition as was initially supplied. That is, no stickers, graffiti, white-out, scathes and etchings, cracks, missing keys, discolouration, substances requiring more than light cleaning or any damage beyond normal wear and tear.

6 Wastage

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

7 Connecting software/hardware

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

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

8 Copyright and licensing

8.2 Copyright laws and licensing agreements must be respected. This means no involvement in activities such as illegally copying material in any format, copying software, downloading copyrighted video or audio files, using material accessed on the Internet in order to plagiarise, or illegally using unlicensed products. This means that students are not to have limewire or torrents or any other peer to peer software

on the laptops. It is very clear in the acceptable use agreement which all year 9 to 11 students and a parent have signed. If students are found in breach of these guidelines the laptop will be reimaged immediately. If Peer-to-peer / bittorrent clients or anonymising software is found on any laptop/ICT device, the laptop/ICT device will be reimaged.

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

9 Posting material

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

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

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

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

10 Queries or concerns

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

10.3 Queries or concerns regarding other cybersafety issues should be taken to the ICT Management Team, a Community Leader or the Student Wellbeing Team.

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

SECTION 2A - ADDITIONAL INFORMATION

1. The Student Cybersafety Use Agreement

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

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

2. Use of ICT.

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

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

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

3. Monitoring

3.1. The College reserves the right at any time to check work or data on the College's computer network, Internet access facilities, computers and other College ICT equipment/devices. For example, in order to help make sure that the College stays cybersafe, teachers may at any time check student email or work. The ICT Management Team also has the ability to remotely monitor College ICT equipment,

via logs and real-time screen viewing, including student laptops and iPod Touches. You must not attempt to prevent the ICT Management Team from remotely monitoring any ICT equipment/device

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

4. Consequences.

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

4.2. Where laptops require reimaging due to a breach of this agreement, the laptop/ICT device will not be backed up before reimaging. There will be no opportunity given to the student to back up their work. However, if you wish for work to be backed up, the College ICT Support team will back up work for a fee. A fee $50 will apply on the first occasion and $100 on every occasion thereafter.

4.3. The College reserves the right to confiscate the laptop due to a breach of this agreement.

Refer to the document 'Misdemeanours and Recommended Consequences Regarding the Use of Laptops and Related ICT Facilities'.

SECTION 2B - ADDITIONAL RULES / RESPONSIBILITIES

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

Students are not to connect to any external devices e.g. Phones, USB modems or other

wireless networks while at Ringwood Secondary College. Students found breaching these guidelines will lose access to Ringwood Secondary College's network, and laptops will be reimaged immediately. Deliberate circumvention of school internet filtering, by use of third-party software, external internet connections (such as '3 mobile internet'), or "anonymous proxy" sites will result in the laptop being immediately reimaged, the administrator status of the student will be modified and the student's ability to access the Ringwood Secondary College network will be reviewed.

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

3. **Mobile phones.** Cybersafety rules also apply to mobile phones. You are not permitted to have a phone on in class time unless this is approved by a staff member. Mobile phones must not be used for involvement with inappropriate material or activities, such as:
   - upsetting or harassing students, staff and other members of the College community even as a 'joke'.
   - inappropriately using text, MMS, email, photographs or film, phone messages, web browsing, images or any other functions.
   - during any assessment where such possession or use is specifically prohibited.
   - Mobile phones must not be used as hot spots to connect College owned devices to the internet in a way that bypasses the College internet filtering systems.

4. **Care of the computers and other College ICT equipment/devices, and their appropriate use includes:**
   - You must not damage or steal any equipment, or try to damage the ICT network. If the damage is deliberate, it will be necessary for the College to inform your parent/legal guardian/caregiver who will have responsibility for the cost of repairs or replacement.

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

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

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

This policy was last updated in October 2019 and is due for review in October 2022