Yarram Secondary College
86 James Street, Yarram 3971
PO Box 135 Yarram 3971
Telephone: 5182 5522
Email: yarram.sc@education.vic.gov.au
Website: www.yarramsc.vic.edu.au

Yarram Secondary College

Internet and ICT Acceptable Use 2026

Date ratified by Staff: August 2019
Date ratified by School Council: N/A
Review date: June 2027

1. Context

Yarram Secondary College is an innovative, safe school that delivers relevant curriculum and promotes rigour, relationships and lifelong learning and uses a school wide computer network to support effective student learning across the school's curriculum. This network also provides student access to the Internet and email.

It is important that parents, staff, and students are familiar with the guidelines as stated in the accompanying *Internet and Information Communication Technology Acceptable Use Policy.* The Department of Education, Victoria requires that all schools have an ICT Acceptable Use Policy.

2. Rationale

Yarram Secondary College has a vision to be a high-end provider of a Digital Learning program for all students that enables interaction in pedagogical practices to engage students with the curriculum. The program provides a vehicle for a personalised learning program and supports a inquiry approach to creating curriculum.

In keeping with the National Educational Goals for Young Australians, we aim to promote and to lead world's best practice for curriculum delivery and assessment and improve the educational outcomes for all students.

This policy provides direction to staff, students and parents/caregivers on procedures, responsibilities, and expectations regarding the Digital Learning program. The School Council has endorsed the program and approved the financial commitment based on a formal discussions and feedback on parent payment advice.

The student use of their account will / must be in support of, and consistent with, the educational objectives of the School, the School's *Student Engagement and Inclusion Policy* and the *Information Communication Technology Acceptable Use Policy and Agreement*. Failure to follow these will result in the loss of privilege to use these facilities.

Although we have established Acceptable Use policies, please be aware that there may be unacceptable material or communications on the Internet that your child can access. Department of Education Victoria provides a filtered internet feed to all schools and teachers will always exercise their duty of care, however protection against exposure to harmful information on the Internet must depend finally upon responsible use by students.

In summary these refer to -

1. *Purpose of the School network and Internet access.* This gives students the benefit of coordinated networked computers and information technology facilities for educational purposes - their daily classwork as well as for research purposes. The

provision of Internet access provides connections to resources world- wide, as well as facilitating local, regional and world- wide communication through email.

2. *Types of information available and intellectual ownership.* Students may access a range of appropriate information via the Internet as well as use computer software installed on the network. The use of these resources is subject to copyright law.

3. *User responsibilities*. Students are responsible for all activity carried out on their personal network account.

4. *Personal security*. Students are not to disclose personal information - their own or other people's, on the Internet.

5. *Consequences.* Inappropriate use of the network facilities, including the Internet or *email* will incur the loss of access to these facilities.

3. Guidelines

This policy sets out guidelines for the acceptable use of which are provided to students for educational purposes only:

- *the school's computer network facilities*
- *installed computer software*
- *the Internet*
- *e-mail*

Acceptable use issues may be broadly categorized as personal conduct relating to:

- *System security*
- *Legal requirements*
- *Ethical use of Department of Education Victoria's computer network facilities at* Yarram Secondary College*.*
- *Standards of interpersonal communication.*

Benefits to students - Students will have access to

- *A variety of equipment, software and services to support effective learning.*
- *Information sources for research via network facilities and the Internet.*
- *Network facilities before school and during lunch breaks.*

Procedures for use - Students are expected to:

- *Operate all equipment with care. Follow written and oral instructions for room and equipment use. Consult a teacher where necessary.*
- *Ensure personal security of their user account by correctly logging on and off.*

4. Responsibilities

4.1 Students are responsible for all activity carried out on their personal network account.

Students are made aware through this policy and acceptable terms agreement that by receiving and using notebooks, iPad or other devices that they are to abide by the following rules and responsibilities:

- ***Only notebooks purchased via the official school purchase portal are the property of the student / family.*** *All other school issued notebooks remains the property of Yarram Secondary College, which I may use at school for schoolwork.*
- *I will take good care of my device. This includes keeping it in its case, storing it carefully in my bag or locker, placing it safely on my desk or table, storing it in a secure and safe place and being diligent with it at all times.*
- *I will bring my device to school with me every day.*
- *I will not loan my device to anyone else.*
- *I will not give anyone else my login or internet password.*
- *I understand that I am only allowed to access the internet through the school's internet connection whilst I am using my device at school.*
- *I will not use any websites, software or an alternative connection method that bypasses the school's internet filtering system.*
- *I alone will be responsible for backing up my own data by using a USB drive, backing up to my personal drive on the school server, syncing to my Google Drive or using my own alternative form of backup.*
- *I will not try to fix my own device or allow anyone other than the school technician to fix it for me.*
- *If there are any faults found with my device, I must report it to the school technician immediately. I understand that I will be without my device for an undisclosed period while the fault is fixed (this will vary due to the nature of the fault).*
- *I am aware that if my device needs reformatting or reimaging due to any circumstances that any personal data, software or settings will no longer remain on the device when it is returned to me.*
- *My device must be kept in pristine condition whilst in my care and I am not allowed to disassemble my device or remove any stickers from it.*
- *I will not graffiti or put any stickers on any school owned device.*
- *I will keep food and drink well away from my device.*
- *I will not alter any of the software that is already installed on my device.*
- *I will not play any games on my device during class time unless specifically given permission to by my teacher.*
- *I will not install any illegal software or P2P software (e.g. any form of torrent program) on my device.*
- *I will only download and store appropriate material to my device. This means no inappropriate material such as pornographic, obscene, racist, discriminatory, violent or vulgar images, sounds, music, language or materials.*
- *I will not upload or store any pornographic, obscene, racist, discriminatory, violent or vulgar images, sounds, music, language or material on my school or personal Google Drive.*
- *I will not use any generative artificial intelligence (AI) tool to upload or generate images of a student, parent, or teacher*
- *I will not use technology to cheat or steal, and always acknowledge information sourced from others or generated content using AI tools (such as ChatGPT, Google Gemini etc)*
- *I am aware that any user activity on my device can be monitored and logged whilst I am at school.*
- *I will always follow Yarram Secondary College's ICT policy and understand that if I do the wrong thing, that consequences will apply.*

4.2 Parent/Guardian Responsibilities

As a parent/guardian of a student in the notebook program at Yarram Secondary College, I acknowledge that:

- *ALL data stored on ALL student devices can be accessed by the school.*
- *I am responsible for monitoring my child's use of the device whilst it is at home.*
- *I understand that the use of internet at home is totally my responsibility (this includes any financial costs as well as any setup that is required).*

- *I will be responsible for any excess fees in case of the notebook being damaged or lost that is not covered under the warranty terms.*
- *If the device is damaged or not working properly, it must be returned to the Yarram Secondary College technology staff for repairs. I will not attempt repairs myself or contract with any other individual or business for the repair of the device as this may void warranty.*

4.3 School Responsibilities

4.3.1 Cyber Safety

The school will maintain its e-smart credentials and ensure that staff, students and parents/caregivers are familiar with the content of the 2009 document *Cyber-safety: keeping children safe in a connected world: Guidelines for schools and preschools* (available at https://www.vic.gov.au/schools-and-cybersafety).

4.3.2 Internet

The school provides internet connectivity through the Department of Education's Zscaler service, which allow students to join and manage many online tools and environments in a highly controlled and protected environment for student safety.

As part of this protection, the department provides internet traffic inspection to most websites to ensure safety from threats such as viruses, spyware and malware. Please review the FAQ below for more information regarding this.

What is internet traffic inspection?

Internet traffic inspection is a standard cyber security measure to help prevent known cyber security threats. Zscaler will inspect internet traffic on your device to ensure it is safe from known cybersecurity threats such as viruses, spyware and malware. Most websites protect the data travelling between their website and your device and you can tell if the site protects your data if the website link starts with https://.

Essentially, your data is put inside luggage which is protected by a lock and transported over the internet so you can interact with the website you are browsing. Zscaler opens the luggage to see if there are any known cyber security threats inside, and if not, closes it back up and allows the luggage and its contents to travel on to its destination. Hackers and bad actors are increasingly using these safes to hide viruses, spyware and malware so inspection is an important element to keeping everyone safe.

Why is internet traffic inspection being implemented?

As cyber threats are constantly evolving and getting harder to detect, we need to ensure we are protecting our schools and network. Having internet traffic inspection in place is a basic security measure to keep students and staff in our schools, as well as keeping your data and the Department's network safe.

What is the benefit of internet traffic inspection for staff and students?

The school's network, devices and personal information will be better protected as additional steps are taken to check for cyber security threats. It will also block the use of known circumvention methods that may be used to bypass content filtering to ensure that internet browsing is safe and that the content filtering profile selected by a school can be applied.

Are there any sites that won't be inspected?

Sites that are health or finance sites will not be inspected. This means when you access medical services online or access online banking, this will not be inspected.

What will happen if the site or file I am trying to access doesn't pass the internet traffic inspection?
Your screen will display a notice that the website or file is unsafe, and why.

How is internet traffic inspection keeping staff and students safe if it is looking at encrypted data? Is that safe to do?

Internet traffic inspection doesn't retain or record any data when internet traffic is being inspected. It simply checks there are no viruses, malware or malicious content. It is completely safe and once it is done inspecting internet traffic, if nothing is found, you will be able to open your file, view the website and continue with what you need to do.

Does Zscaler keep records of the internet sites I am browsing?

Zscaler logs of internet sites visited are kept by the department for 12 months. This is different to keeping records of information being sent between a website and your device. When inspecting the traffic, the data will only be inspected at the time you are assessing the website and no inspection data is held by the Department or Zscaler.

What personal information is kept in the Zscaler logs?

Staff using the Zscaler app will have their username and device information captured. Students and staff who do not have the Zscaler app installed will only have device information captured.

Where is the Department's Zscaler data stored?

The Department's Zscaler data is stored in Victoria, Australia and not sent overseas.

Who will have access to the logs?

Full Zscaler log information is available to authorised DE staff administrators, engineers and security analysts. Limited Zscaler logs with personal information removed are available to Service Technicians and Service Delivery Managers for the schools they support.

Will my student device be monitored from home?

Your device will only be monitored when connected to the school network. It will not be monitored from home or any other third-party internet connection (public wi-fi for example).

4.3.3 YSC BYOD (Bring Your Own Device) Agreement

This agreement, in accordance with DET Victoria and the *Education and Training Reform Act 2006* (Sections 2.2.4(1), 2.3.6(1) (c), 2.2.) ensures that Yarram Secondary College provides our students with equitable access to electronic devices such as laptop computers or tablets with our implementation of the 1-to-1 learning programs and seeks financial contributions from parents consistent with the *Parent Payments Policy*.

The YSC BYOD Agreement must be fully read, understood, and signed by both the student and their parents/guardians before any personal device is connected to the college's wireless network.

Minimum Device Specifications

Your device must meet the minimum requirements listed on this page before it is allowed to be connected to the school's wireless network.

Note: devices such as smartphones and music devices (e.g. iPods) are deemed as unsuitable devices by the college and will not be allowed to connect to the school's network.

Windows Laptops

- *Windows 11*
- *8gb RAM or more*
- *128gb hard drive or above*
- *Wireless AC standard or above*
- ***AI/Snapdragon devices not accepted at this stage, as they don't allow us to install all required school software***

Mac Laptops

- *OSX 12 (Monterey) and above*

iPads/Android Tablets/Chromebooks are unsupported at this stage.

BYOD vs School Purchased Laptop Support

	BYOD (Bring Your Own Device)	**School Purchased Laptop**
Access to school wireless/internet	YES	YES
School based technical support*	LIMITED	YES
Access to school printers	YES	YES
Access to school personal drive (P:)**	NO	YES
Access to school purchased software***	NO	YES
Software support	NO	YES
Hardware support	NO	YES
Onsite warranty support	NO	YES
Insurance options	NO	YES

****School based technical support for BYOD machines will only include the following:***

Installing school approved antivirus/antispyware software (does not apply to tablet devices at this stage). Any existing AV software will be removed, and all devices will be fully scanned before being connected to the school network.

Installing AB Tutor for monitoring BYO devices during school hours

Installing SCCM client for partial MDM (Windows devices only)

Connecting the device to the school wireless system and internet

*****Students will not be allowed access to their personal drive (aka P Drive) or any school shared drives from their personal device for security reasons.***

****** Students will have access to DET licenced software (Office 365, Adobe Suite etc), but will not have access to any software purchased directly via the school (unless licencing allows for installs on BYO devices).***

Additional Information & BYOD Policies

- ***One*** *BYO device per student.*
- *Students are allowed to switch personal devices once per year. The original device will be removed from the network before the new one is added.*
- *Devices purchased through the school will receive priority support over student personal devices.*
- *Students/parents may be required to purchase software or apps if needed for a class. School licenced software does not cover student personal devices.*
- *The school is in no way liable for any loss or damage that occurs to the student's personal device on school grounds.*
- *Any software or hardware issues that are not covered in the school's BYOD policy must be taken to the original place of purchase or a 3rd party repair agent to be resolved. Any requests to the school to fix these types of issues will not be met.*
- *The school will not accept payments to fix any software or hardware issues that are not covered in the school's BYOD policy as this is also against Department of Education policy.*
- *The school's IT and network policies also applies to personal student devices (information attached). In the case of any of the policies and/or rules being broken, the student's personal device will be removed from the network for a period of time. The student can then borrow a school machine from the library or will be temporarily assigned a notebook by the IT Department. If any damage occurs to their loan machine, repair fees must be paid before the personal device is connected back to the network.*
- *Any software deemed to be intentionally harmful or break any of the school's IT or network policies can be requested to be removed by any school staff member. The device can be denied access to the school's network until this has been achieved.*
- *Removal of the antivirus or AB Tutor software from applicable personal devices will also result in the device being removed from the network for a period of time.*

Section 1 – Student Responsibilities (BYOD)

As a student, I am aware that by using my personal device on the school network, that I am to abide by the following rules and responsibilities:

- I will take good care of my BYO device. This includes keeping it in its case, storing it carefully in my bag or locker, placing it safely on my desk or table, storing it in a secure and safe place and being diligent with it at all times.
- I will bring my BYO device to school with me every day.
- I will not loan my BYO device to anyone else.
- I will not give anyone else my login or internet password.
- I understand that I am only allowed to access the internet through the school's internet connection whilst I am using my notebook at school.
- I will not use any websites, software or alternative connection methods that bypasses the school's internet filtering system.

- I alone will be responsible for backing up my own data by using a USB drive, backing up to my personal drive on the school server, syncing to my Google Drive or using my own alternative form of backup.
- My BYO device must be kept in pristine condition whilst in my care and I am not allowed to disassemble my notebook or remove any stickers from it
- I will keep food and drink well away from my BYO device.
- I will not play any games on my BYO device during class time
- I will only download and store appropriate material to my BYO device. This means no inappropriate material such as pornographic, obscene, racist, discriminatory, violent or vulgar images, sounds, music, language or materials.
- I will not upload or store any pornographic, obscene, racist, discriminatory, violent or vulgar images, sounds, music, language or material on my school or personal Google Drive.
- I am aware that any user activity on my BYO device can be monitored and logged whilst I am at school.
- I will always follow Yarram Secondary College's ICT policy and understand that if I do the wrong thing that consequences will apply.

Section 2 – Parent/Guardian Responsibilities (BYOD)

As a parent/guardian of a student in the BYOD program at Yarram Secondary College, I acknowledge that:

- *ALL data stored on ALL student personal devices can be accessed by the school if required.*
- *I am responsible for monitoring my child's use of the BYO device whilst it is at home.*
- *I understand that the use of internet at home is totally my responsibility (this includes any financial costs as well as any setup that is required).*
- *I will be responsible for organising any software/hardware repairs on the BYO device if it is required.*

4.3.4 Warranty/Insurance/Non-Warranty Charges associated with devices purchased via online school portal

Each notebook purchased via the school portal comes with a 3-year onsite warranty. This means that if the unit has a defect that is not caused by accidental or intentional damage, the unit will be repaired at the school and at no cost to the student/parent.

As part of the new Lenovo education warranty, insurance is now also included for 3 years at no extra cost *. This is an offer that is only available via the school portal and is not available at any other retail stores.

This also means that there are no excess fees to pay. If the unit is damaged beyond repair, a replacement will be provided. **

For devices purchased via the portal that are out of their 3-year warranty/insurance coverage period, we only offer limited repair options via the school (screens, keyboards). ***

**** There is a limit of 3 insurance repairs for the device in the 3-year period.***

***** A new Lenovo education warranty must be purchased with the replacement device. It does not carry over from the existing device.***

***** Replacement parts must be paid for before they can be ordered/fitted. Price includes delivery and GST. Sourced parts may be aftermarket parts that come with a limited warranty.***

5. Agreement Declaration

Student Notebook and Computer Network Use

I have read the agreement document regarding the use of Student Notebook Computers for Yarram Secondary College and agree to abide by the terms and conditions.

Student Agreement

I have read and understand the *Information Communication Technology Acceptable Use Policy and Agreement*.

- I understand that the school's ICT network provides me with access to a range of essential learning tools, including the internet. I understand that the internet can connect me to useful information stored on computers from around the world.
- While I have access to the school's ICT network: I will only use it for educational purposes; I will not undertake or look for anything that is illegal, dangerous, or offensive; and I will not reveal my password or allow anyone else to use my school account.
- Specifically in relation to e-mail and internet usage, I will: clear any offensive pictures or information from my screen; and immediately quietly inform my teacher.
- I will not: reveal home addresses or phone numbers – mine or that of any other person; or use the school's ICT network (including the internet) to annoy or offend anyone else.
- I understand that if the school decides I have broken the rules for using its ICT network, appropriate action will be taken, which may include loss of access to the network (including the internet) for some time.

_____(Student's name) _____(Year Level)

_____(Student's signature)_____(Date)

Parent or Carer Agreement

I have read and understand the *Information Communication Technology Acceptable Use Policy and Agreement*.

- I understand that the school provides my child with access to the school's network (including the internet) for valuable learning experiences. Regarding internet access, I understand that this will give my child access to information on computers from around the world; that the school cannot control what is on those computers; and that a small part of that information can be illegal, dangerous, or offensive.
- I accept that, while teachers will always exercise their duty of care, protection against exposure to harmful information should depend finally upon responsible use by students/my child. Additionally, I will ensure that my child understands and adheres to the school's appropriate behaviour requirements and will not engage in inappropriate use of the school's ICT network.
- I believe_____(name of student) understands this responsibility, and I hereby give my permission for him/her to access and use the school's ICT network (including the internet) under the school rules. I understand that students breaking these rules will be subject to appropriate action by the school. This may include loss of access and usage of the school's ICT network for some time.

_____(Parent/Guardian's name)

_____(Parent/Guardian's signature)_____(Date)

6. Student Logon Details

In this section, the student must write down their username and password.

If the student is new to the college, they must write down their login name (first 4 letters of their first name and first four letters of their last name) and a password to access the notebook/network. The password must have a minimum of **8** characters and numbers and characters can be used.

If the student already has a user account on the school network, they will need to enter their current login information in the fields below. (Please note: if the password given is different to their current network password, the password on this form will replace their current network password.)

Student Username:_____

Student Password:_____