YARRA VALLEY
GRAMMAR

POLICIES AND PROCEDURES

Policy Name	**IT Acceptable Use Policy (Students)**
Reviewed / Approved by:	PXC/School Executive
Review:	**Last Review**: 2021, 2023, 2025 **Next Review**: 2027

Statement of Context

Yarra Valley Grammar supports the right of all members of the School community to access safe and inclusive learning and teaching environments, including online spaces. This document outlines the School's roles and responsibilities in supporting safe digital learning as well as the expected behaviours of students when using online spaces.

Digital Learning at Yarra Valley Grammar exists to support our educational mission to be a great school fostering excellence, concern for others and a global outlook.

- Excellence and endeavour
- Community, service and leadership
- Safety and Wellbeing
- Creativity and compassion
- Our Christian ethos and our Anglican tradition

(ref: 2022-2026 YVG Teaching and Learning Plan)

The School provides each student with a network access account, which includes access to:

- A Community Portal and mobile apps for students, staff and families
- A managed email account with mail filtering
- Google Drive Apps for Education
- Microsoft One Drive and Office 365 licensing
- Adobe Creative Cloud Suite (Years 7-12 students)
- Cogniti AI embedded into Canvas courses for students in Year 9-12 from 2026
- A home directory with a limited amount of storage
- Canvas Learning Management System resources
- Filtered and monitored Internet provision
- A variety of additional online learning resources
- Protection against various electronic threats (for example viruses, malware and SPAM) on school owned devices.

Kalinda Road Ringwood Victoria 3134 Australia Telephone +61 3 9262 7700 Facsimile +61 3 9876 1077 Email reception@yvg.vic.edu.au www.yvg.vic.edu.au
ABN 44 004 584 552 CRICOS NO. 00356E

Yarra Valley Grammar provides electronic devices to Junior School students. Depending on the Junior School year level, students may have access to an iPad, desktop or laptop. Student devices in the Junior School remain the property of the School. Students in the Middle School and Senior School participate in a "Bring Your Own Device" (BYOD) program that enables students to use their own device(s) at school.

Digital Citizenship
Internet and network access from both school-owned devices and BYOD devices are governed by the School's rules and policies.

The School has the right and responsibility to ensure a safe environment for the use of ICT and digital devices. At Yarra Valley Grammar, students and staff are expected to develop their understanding and application of ethical principles associated with technology use. This is especially important at a time when the everyday use of Artificial Intelligence is rapidly expanding. Respecting and protecting oneself, others, and intellectual property remain essential components of digital citizenship. Cyber safety and cyber security are essential components of digital citizenship.

This policy is available to students and parents on the Community Portal. The continued access to digital resources is dependent on the student's acceptance of this policy. If students or parents have any objection to accepting this policy, they should contact the School to discuss their concerns before access is granted.

General Conditions

1. Students must follow all instructions from teachers when using digital devices at school.
2. Access is a privilege, not a right, and users are responsible for their behaviour and communications over the Yarra Valley Grammar network.
3. Material such as games, sound files, videos, or images must not be saved in a user's home directory unless it is directly related to schoolwork.
4. Each student bears full responsibility for their own device. Security of the BYOD device is at all times the responsibility of the Student. Students should not access or interfere with another student's device. Students must not access, modify, or delete other users' information without permission.
5. Each student bears full responsibility for their individual network access accounts. Students are not permitted to share their account or password with any other student, misappropriate another person's password/s and must not access another person's account. At the end of each session in a shared computer laboratory, students must log out properly. If a student suspects that someone else is aware of their password, they should immediately contact the IT Department to change it.

Kalinda Road Ringwood Victoria 3134 Australia Telephone +61 3 9262 7700 Facsimile +61 3 9876 1077 Email reception@yvg.vic.edu.au www.yvg.vic.edu.au
ABN 44 004 584 552 CRICOS NO. 00356E

6. Using another person's username and password (e.g. student or staff member) to gain access to the School's network is deemed as serious misconduct.

7. Students must not use another person's image or voice without their express permission. This includes taking, altering, manipulating, sharing, or using someone's image or voice in any form without explicit consent. Any such use without permission is strictly prohibited.

8. Students are not permitted to have any software on their personal device that may be perceived as penetration-testing or network-interrogation tools, as these applications can disrupt the school's network, enable unauthorised access to information, and compromise the safety and privacy of others. If such applications are found on a device, the school will treat the matter as a serious breach of the Acceptable Use Policy and investigate accordingly.

9. Internet access is provided solely for educational use and school related activities only. Content filtering is used to restrict access to inappropriate material. Deliberate attempts to locate or download material that is illegal, inappropriate or offensive are not permitted. Attempts to bypass the content filtering system by using offsite proxies, VPNs or any other methods are not permitted.

10. Students are not permitted to use their mobile phone for hotspotting to their electronic device.

11. Students must not use the network to access or send material which is racist, defamatory, obscene, pornographic or advocates violence or discrimination against other people (hate literature). Deliberately attempting to access or send such material is deemed as serious misconduct. If students find or receive any information that is inappropriate or makes them feel uncomfortable, they should inform a member of staff immediately.

12. It is the responsibility of students to keep backup copies of their work, and they are expected to follow a regular backup procedure. The simplest method is to create a folder on their device and drag and drop to copy it to their Google Drive account. Students may also use Microsoft OneDrive or an external hard drive to back up their work. The School will not be held responsible for any data lost as a result of failing to maintain backups.

13. Parents and students need to be aware that student email and internet searches are scanned for inappropriate language, content and attachments. This scanning also includes student internet searches and students who attempt to bypass the school network. The School reserves the right to review any material in user accounts and devices and take appropriate action during school hours. The School may monitor material sent or received by users and may trace network activities to the network accounts of specific users. Students must not:
    a. Send offensive emails
    b. Send unsolicited emails to multiple recipients (SPAM)

Kalinda Road Ringwood Victoria 3134 Australia Telephone +61 3 9262 7700 Facsimile +61 3 9876 1077 Email reception@yvg.vic.edu.au www.yvg.vic.edu.au
ABN 44 004 584 552 CRICOS NO. 00356E

c. Use email for any illegal, immoral or unethical purpose
d. Attempt to disguise their identity or the true origin of their email

14. Students must not tamper or interfere with or compromise any of the school's computer systems. This includes cabling or peripheral equipment such as keyboards, mice and printers in either classrooms or computer labs.

15. Students must not use the School's network to:
    a. Download, install or distribute illegally copied or unauthorised software, games, videos or music
    b. Change any computer settings
    c. Distribute another individual's password/s.

16. Students must not use their School account or social media channels to bully, offend, harass or discriminate against others. Harassment is defined as the persistent annoyance of another user or interference with another user's work. Harassment includes, but is not limited to:
    a. The sending of unwanted email or texts
    b. Posting anonymous messages
    c. Hiding or damaging facilities or files
    d. Making disparaging statements or opinions about the School, the administration of the School, members of staff or other students

17. Students are not permitted to post their School email address or use it to subscribe to content on a web page external to the School. Furthermore, students must protect their privacy and that of others. This includes full name, telephone number, address, passwords and images. Email and the Internet are not always secure, and messages can be forwarded without one's knowledge. For this reason, students should be very careful about communicating private and confidential information via social media.

Social Media

The School acknowledges that social networking has some benefits and hence endeavours to create a framework in which students can operate safely.

Social media channels include social networks (including but not limited to apps such as Instagram, Snapchat, WhatsApp, Facebook, Twitter, Discord, Reddit, YouTube and Tik Tok), FaceTime, messaging services, chat rooms, online forums and discussion groups, wikis, blogs, micro-blogging tools, and any other websites that facilitate the sharing or publishing of user generated content. Access to anonymous email and all social media sites such as those mentioned above is not permitted at School.
From 10 December 2025, many social media platforms will not be permitted to let Australians under 16 create or keep accounts. While Yarra Valley Grammar already limits access to these platforms on the

school network, the School recognises that the highly engaging features and algorithm-driven feeds used by social media apps can encourage excessive use and impact a teenager's attention, sleep, and overall mental health.

Learning management systems that allow educators to share course materials, manage assignments and facilitate communication, and which allow students to access classroom resources, submit work and collaborate with peers, will be excluded from the age restrictions.

While these services are often integrated with other tools such as video conferencing, messaging and the ability to post content on the service, if their sole or primary purpose is to support the education of users, the exclusion will apply. Some of these services allow teachers to embed public video content from other platforms onto the learning management system. If the content is publicly available and does not require the student to log into another platform, students will still be able to watch this content.

When using Social Media, students should:

1. Be respectful and kind to others. Do not post information that is untrue or could harm others.

2. Protect the privacy of others by never posting or forwarding their personal details or images without their consent.

3. Not use the School's network to access social media channels unless the access is facilitated and moderated by a teacher for class work.

4. Have regard to the impact of social media postings within the extended school community. Students should think carefully about the content they upload or post online, knowing that this is a personal reflection of who they are and that it can influence what people think of them.

5. Not make disparaging statements or opinions about the School, the administration of the School, members of staff or other students on any social media channels.

6. Not use social media channels to bully, offend, harass, intimidate, masquerade or deliberately exclude other students or staff, whether within or outside of school hours.

7. Be aware that by identifying themselves as Yarra Valley Grammar students (such as images in school uniform) immediately creates an association with the School and may affect the public image and/or reputation of the School.

8. Understand that publication of photos and tagging can reveal information about themselves and others and their location. People have the right to control when and how their image, likeness and voice are shared. Photos, videos or audio taken without consent can be used for exploitation or harassment and may lead to legal consequences.

9. Students should understand that anything published online can be copied, shared, or misused by others, often without their knowledge or control. Online activity creates a permanent digital footprint that can be traced, and content such as images, videos, or audio may be impossible to remove once posted. Students should be aware that there is little to no privacy on the internet.

Students feeling unsafe or intimidated through the effects of social media or seeing others being affected by or participating in inappropriate online behaviour should seek immediate assistance from a member of staff. Students are encouraged to talk to a teacher or a trusted adult if they believe another student is in an unsafe, inappropriate online situation.

Mobile Phones

The use of a mobile phone, smart watch and other personal devices is not permitted during school hours. Students should refer specifically to the current Mobile Phones and other Electronic Devices (Students) Policy.

The use of AI Language Models

There are a small number of AI tools available through the school network that meet requirements for ethical use, privacy, age restrictions, and data protection. The permitted tools offer students protection under the Australian Privacy Principles. Most AI tools are opaque in how they collect, use, and store personal information and are therefore not permitted for use at School by students.

The School may monitor the use of AI tools on the school network to ensure compliance with this policy.

This section should be read in conjunction with the published Yarra Valley Grammar Generative Artificial Intelligence (GenAI) Guidelines.

1. AI must not be used to complete or generate work for assessment unless a teacher has given explicit permission.

2. All permitted AI use must follow the School's guidelines for disclosure and acknowledgement.

Kalinda Road Ringwood Victoria 3134 Australia Telephone +61 3 9262 7700 Facsimile +61 3 9876 1077 Email reception@yvg.vic.edu.au www.yvg.vic.edu.au
ABN 44 004 584 552 CRICOS NO. 00356E

3. Students must not use AI tools to create harmful, misleading, or inappropriate content. This includes fake images, altered audio, impersonations, misinformation, or any content designed to deceive, harass, or disadvantage others.

4. Students must not use AI to replicate, imitate, or manipulate another person's image, likeness, or voice without explicit consent.

   This includes deepfakes, voice clones, generated images, or edited media.

Breach of Policy

Students will be held responsible for their actions while using their network access account and for any breaches caused by allowing another person to use their network access account. The misuse of IT resources, including breach of the School's rules or policies contained in this IT Acceptable Use Policy and elsewhere in the School's policies, may result in the withdrawal of network access and disciplinary action. Students may also be held legally liable for any unauthorised or illegal actions committed using their network access account.

All students agree to abide by the rules set out in this IT Acceptable Use Policy at each login on the School's computer system. This IT Acceptable Use Policy may be amended from time to time.