Bacchus Marsh Grammar

School POLICY

STUDENT DUTY OF CARE

Student Acceptable Online Usage Policy

Approved by the School Principal: 17 September 2025

Bacchus Marsh Grammar PO Box 214 Bacchus Marsh VIC 3340 **E** school@bmg.vic.edu.au
Maddingley Campus South Maddingley Road, Bacchus Marsh VIC 3340 **P** 03 5366 4800
Woodlea Campus and ELC 111 Frontier Avenue, Aintree VIC 3336 **P** 03 5366 4900

An Independant Ecumenical School for Girls and Boys
Reg. No. 1919
ABN: 24 128 531 078
www.bmg.vic.edu.au

Student Acceptable Online Usage Policy

1 Rationale

Bacchus Marsh Grammar (the School) is committed to providing high quality, relevant educational experiences for all students.

Information and Communication Technologies (ICT), including advanced AI tools, cloud-based learning platforms, and digital collaboration systems have dramatically changed how information is accessed, stored, communicated and used in education.

Due to the rapidly evolving nature of ICT, clear usage guidelines are required to ensure students use digital resources responsibly, do not access inappropriate content and remain safe in an online environment.

The School also acknowledges the increasing risks associated with cybersecurity threats, artificial intelligence (AI), data privacy and online child abuse.

To prevent online child abuse, the School has implemented the following safety strategies:

- Age-appropriate filtering and monitoring systems to restrict access to harmful online content.
- Active monitoring of student accounts, emails, and online communications to detect inappropriate behaviour or risks.
- Restricted access to online platforms (e.g., SchoolBox, Google Workspace, Microsoft 365) with security and privacy protections in place.
- Disabling of device cameras for younger students (Prep – Year 10), unless specifically approved and supervised.
- Supervised use of online learning tools, particularly for Junior School students, with staff oversight in both physical and remote learning settings.
- Staff training to recognise, respond to, and report any suspected online grooming, exploitation, or abuse.
- Education programs for students about safe online behaviour, responsible digital citizenship, and how to seek help if they feel unsafe.
- Alignment with child safety standards and reporting obligations under relevant legislation.

Online services include the School's network and intranet, the internet, email, newsgroups, blogs, the Learning Management System (SchoolBox), social media platforms, cloud storage, artificial intelligence tools and other online communication and collaboration platforms.

2 Rules for Student Use of Online Services

2.1.1 Students must not access, search for, or distribute offensive, pornographic, subversive or dangerous material at any time using any online device, including school computers, personal devices, or other student's devices while on school premises or during remote learning.

2.1.2 During class time students may use school approved devices e.g. Chromebooks and online services solely for academic purposes. The use of ICT resources for gaming, social media, non-school-related applications, or unapproved video/music streaming is prohibited.

2.1.3 Students must NOT use email, social networking, online chat, shared documents, or any other communication services unless explicitly directed by their teacher.

2.1.4 Junior School students using online services must be actively supervised at all times.

2.1.5 Chromebook cameras must only be used for positive educational experiences, ensuring they support student learning and school-related activities in a safe and appropriate manner.

2.1.6 Students must not tamper with, move or alter school ICT equipment, including network connections, wireless devices, and computer hardware. Troubleshooting or fixing malfunctioning school devices must be handled by ICT support staff.

2.1.7 Students must NOT attempt to access any school computer or online service using the credentials of another student or staff member. Students must keep their passwords confidential.

2.1.8 The use of proxy services, VPN's, or any other method to bypass the school's internet filtering system is strictly prohibited.

2.1.9 Students must NOT bring or install unauthorised software, games or non-school related applications onto school devices or networks.

2.1.10 Students must not use or distribute hacking software, malware, or any tools that could compromise network security or the privacy of others.

2.1.11 Students must adhere to the School's Bullying and Harassment Policy and Student Code of Conduct when using online services. Any form of cyberbullying, bullying, harassment, or digital misconduct will be treated in line with the School's Student Discipline Policy.

2.1.12 Students must NOT publish, share or post material online that could damage the reputation of the School, its staff, students or members of the School community.

2.1.13 Personal devices, including smartphones and tablets, must NOT be used to create unauthorised internet hotspots or circumvent school-managed internet access.

2.1.14 Students must NOT engage in online commercial transactions, including buying or selling goods while at school.

2.1.15 File sharing and cloud storage services (e.g. Google Drive and or One Drive) must be used responsibly, and files should only be shared with permission from their teacher.

2.1.16 Online streaming of content must be for educational purposes only.

2.1.17 Students must NOT manipulate, alter, or misuse online content without School approval.

2.1.18 Students must maintain appropriate behaviour and digital etiquette during online classes, adhering to the Student Code of Conduct.

2.1.19 The privacy of staff and students must be respected at all times, including in online learning environments.

2.1.20 Students must regularly maintain their school-provided devices in accordance with School guidelines, including proper cleaning and updating of software.

2.1.21 The use of AI tools (e.g., ChatGPT) must be in accordance with School's Generative Artificial Intelligence Student Usage Policy and Guidelines.

2.1.22 Students must immediately report to a teacher or trusted staff member any online contact, message, or behaviour that makes them feel unsafe, uncomfortable, or threatened.

2.1.23 Students must not engage in private, unsupervised online communications with adults who are not staff members or verified educational partners.

2.1.24 Students must not share personal information (such as home addresses, phone numbers, or private photos) in online learning environments unless approved for educational purposes and supervised by staff.

2.1.25 The use of video conferencing platforms must follow School guidelines: sessions will be monitored, recordings will be managed according to privacy and child protection policies, and students must not initiate private video calls without teacher approval.

2.1.26 Any suspected online grooming, harassment, or inappropriate contact will be treated as a serious child protection concern and referred to the Principal and relevant authorities.

3 Student Email Account Usage

3.1.1 School-issued email accounts are provided to students for academic purposes only. Personal emails and social communication unrelated to schoolwork should not be conducted via the School's email system.

3.1.2 Email should be used for communication related schoolwork and academic inquiries between staff and students only. For example. A student may request additional help on a homework task, or a teacher may give an absent student some resources missed in class. When communicating with staff, students must maintain a professional and respectful tone, free of personal comments as expected in all student teacher interactions.

3.1.3 Students may only use email within class time with explicit teacher permission. Outside of school hours, school emails should be used solely for academic purposes, including group work or inquiries regarding school tasks.

3.1.4 Personal email accounts (e.g. Hotmail, Gmail) should not be used for school-related communication, not should students communicate with staff through personal email or social media platforms.

3.1.5 All school-issued student email accounts are subject to monitoring. Random checks may be conducted periodically to ensure compliance with this policy.

4 Consequences for Non-compliance with the Usage Rules

4.1.1 For the first violation of the usage rules, the student's access to on-line services will be restricted for two weeks. Parents/guardians will be notified via letter by the appropriate Head of Year or Deputy Principal.

4.1.2 For a second violation, all online usage will be suspended, and an interview will be scheduled with the student's parents / guardians, the appropriate Head of Year and Deputy Principal.

4.1.3 In the case of severe breaches, the Principal may impose sanctions in line with the School's Student Discipline Policy, even for a first violation.

4.1.4 Any incidents involving illegal activity will be reported to the appropriate authorities immediately.

5 Other Information

5.1.1 Students are provided with cloud storage (e.g. Google Drive and/or One Drive) for school-related files. Only school-work should be stored here. Students may also use USB sticks for additional storage, however they remain responsible for backing up their files.

5.1.2 School-provided Chromebook cameras are disabled for students in Years Prep – 10, while Chromebook cameras are enabled for student use in Years 11 and 12. Requests for chromebook camera use for students in Years Prep – 10 must be directed to the Head or Deputy Head of Campus.

5.1.3 The School reserves the right to impose quotas on internet usage, including monitoring of bandwidth consumption, and to apply filtering services to ensure safe and appropriate use.

5.1.4 Student printing will be monitored, and any excessive printing beyond the allocated quota will incur charges, requiring the student to purchase additional printing credits.

5.1.5 Photocopying services are available in the School Libraries, with charges, similar to printing.

5.1.6 By enrolling at the School, parents/guardians agree to ensure their child complies with the School's Acceptable Online Usage Policy.

5.1.7 The School uses a combination of content filtering, user monitoring, and secure logins to protect students from accessing harmful or abusive online material.

5.1.8 The School provides regular student workshops and parent information sessions on online safety, including strategies to prevent cyber abuse and exploitation.

5.1.9 All staff are required to complete mandatory child safety and online protection training to ensure vigilance in detecting and responding to online abuse risks.

5.1.10 Where suspected online abuse occurs, the School will activate its Child Safety Reporting Procedures and work with external agencies, including law enforcement, as required.

5.1.11 This policy will be reviewed and updated regularly to stay current with technological developments.

6 Related Documents

Child Safe Policy
Generative Artificial Intelligence Student Usage Policy and Guidelines
Information & Communication Technology (ICT) Policy (students)
Mandatory Reporting to Child Protection Policy
Mobile Phones (Student Use of) Policy
Privacy Policy

School Community Code of Conduct
Student Bullying and Harassment Policy
Student Code of Conduct
Student Discipline Policy
Student Use of Social Media Policy

7 Authorisation

School Document Name	**Student Acceptable Online Usage Policy**	
Approval Authority	**CEO**	
Approval Signature	Andrew Neal **CEO** **Bacchus Marsh Grammar**	
Administrator	**Company Secretary**	Greg Gough
Approval Date	**17 September 2025**	
Date of Next Review	**17 September 2028**	To be reviewed every three years

8 History

Date	Amendment
29 January 2015	1. New policy
17 October 2019	2. Reviewed and new format
16 April 2020	3. Updated rules to include online learning component
10 August 2022	4. Reviewed with minor changes
7 March 2025	5. Reviewed and updated to align with current technological and security requirements / standards.
17 September 2025	6. Updated to include the procedures and strategies the school has in place to prevent online abuse