

Digital Learning Policy

1. Purpose

Alphington Grammar School is committed to providing a contemporary, safe and educationally purposeful digital learning environment. This policy outlines:

- The School's approach to digital device programs across Prep–Year 12
- Expectations for responsible and ethical use of technology
- Safeguards to protect students' safety, wellbeing and privacy
- Governance arrangements to ensure compliance with VRQA and Ministerial Order No. 1359

This policy operates in conjunction with the School's **IT Acceptable Use Policy**, Child Safety and Wellbeing Policy, and Student Engagement Policy.

2. Scope

This policy applies to:

- All students (Prep–Year 12)
- Staff and contractors
- Parents/guardians
- Volunteers
- All digital devices used for educational purposes on campus or during school-related activities

3. Digital Learning Model at Alphington Grammar School

Early Years & Junior Primary (Prep – Year 2)

- Students are provided with **school-owned iPads**.
- Devices remain the property of the School.
- Devices are stored, managed and supervised by classroom teachers.
- Usage is developmentally appropriate and integrated into structured learning.

Upper Primary (Years 3 – 6)

- Students participate in a **Bring Your Own Device (BYOD) iPad Program**.
- Devices must meet School technical specifications.
- Devices must be enrolled in the School's Mobile Device Management (MDM) system.
- Parents/guardians are responsible for maintenance and insurance.

Secondary School (Years 7 – 9)

- Students participate in the School's **Laptop Program**.
- Devices must meet required specifications and be registered with the School's IT Department.
- Devices are used across all subject areas to support research, collaboration and digital fluency.

Secondary School (Year 10-12)

- Students participate in the School's **BYOD program**.
- Devices must meet required specifications and be registered with the School's IT Department.
- Devices are used across all subject areas to support research, collaboration and digital fluency.

4. Guiding Principles

The School's digital learning program is underpinned by:

1. Educational enhancement – technology supports and enhances pedagogy.
2. Digital citizenship – students develop ethical and responsible online behaviours.
3. Child safety – digital environments are monitored and safeguarded.
4. Equity and inclusion – access is provided in a fair and inclusive manner.
5. Wellbeing – screen use is balanced and age-appropriate.

5. Child Safety & Online Safety Framework

Digital learning environments are governed by the School's Child Safety and Wellbeing framework and align with Ministerial Order 1359.

The School:

- Implements content filtering and network monitoring systems.
- Supervises student use of devices during school hours.
- Provides explicit digital citizenship education across all year levels.
- Maintains procedures for reporting and responding to online safety incidents.
- Applies behavioural consequences consistent with the Student Engagement Policy.

Online safety education includes:

- Cyberbullying prevention
- Safe communication practices
- Managing digital footprints
- Privacy awareness
- Image-based abuse prevention
- Appropriate use of AI tools

6. Acceptable Use Expectations

All students must:

- Use devices for educational purposes during school hours.
- Protect passwords and personal information.
- Respect the privacy and dignity of others.
- Not photograph or record others without permission.
- Not access, create or share inappropriate content.
- Comply with staff instructions regarding device use.

Breaches are managed in accordance with the School's Behaviour and IT Acceptable Use policies.

7. Roles & Responsibilities

Governing Authority

- Approves and reviews this policy annually.
- Ensures compliance with VRQA and Ministerial Order 1359.
- Monitors risk management processes relating to digital safety.

Principal

- Ensures implementation of the policy.
- Allocates appropriate resources for safe digital infrastructure.
- Reports digital safety matters to the School Board.

IT Department

- Manages network security and device compliance.
- Maintains content filtering and monitoring systems.

- Supports MDM implementation.

Teachers

- Supervise device use.
- Integrate digital citizenship education.
- Report digital safety concerns.

Students

- Comply with the IT Acceptable Use Policy.
- Engage responsibly and respectfully online.

Parents/Guardians

- Support responsible device use at home.
- Ensure BYOD devices meet School specifications.
- Reinforce digital safety expectations.

8. Data Security & Privacy

The School:

- Complies with the Privacy and Data Protection Act 2014 (Vic).
- Ensures secure storage of student data.
- Utilises secure cloud-based learning platforms.
- Restricts access to authorised users only.

Personal information will not be disclosed without lawful authority.

9. Artificial Intelligence (AI) Use

The School recognises emerging AI technologies as educational tools when used responsibly.

Students:

- May use AI tools when authorised by teachers.
- Must acknowledge AI assistance where required.
- Must not submit AI-generated work as their own.

Staff:

- Integrate AI literacy into curriculum where appropriate.
- Monitor for academic integrity breaches.

10. Risk Management

Digital learning risks are identified in the School's Child Safety Risk Register and ICT Risk Register.

Risks addressed include:

- Cyberbullying
- Inappropriate content exposure
- Data breaches
- Online grooming
- Misuse of recording functions
- Academic dishonesty

Mitigation strategies include:

- Filtering software
- Staff supervision
- Digital literacy curriculum
- Clear reporting procedures
- Annual policy review

11. Breach Management

Breaches may result in:

- Temporary or permanent loss of device privileges
- Behavioural consequences
- Parent meetings
- Mandatory reporting where required
- Referral to external authorities if applicable

Serious online safety concerns are managed under the School's Child Safety Reporting Procedures.

12. Implementation & Monitoring

Action	Responsibility	Timeline
Annual policy review	Governing Authority	Annually
Device compliance audit	IT Department	Each Term
Digital citizenship curriculum review	Head of Teaching & Learning	Annually
Staff online safety training	Principal	Annually
Risk Register review	Child Safe Champion	Biannually

13. Communication

This policy is:

- Published on the School website
- Provided in enrolment documentation
- Referenced in student handbooks
- Linked to the IT Acceptable Use Agreement signed annually

14. Policy Review

This policy will be reviewed annually or earlier if:

- Legislative changes occur
- VRQA requirements are updated
- A serious digital safety incident occurs