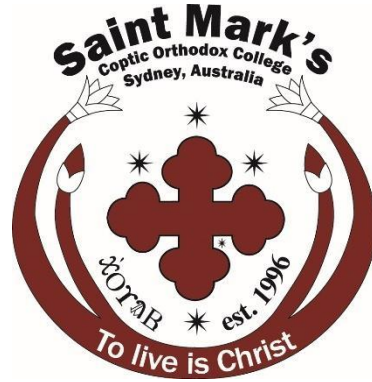




Year 5-12 BYOD Policy

St Mark's Coptic Orthodox College

Master Copy Location:	College Google Drive	
Last Updated:	By Whom:	Authorised by:
13 March 2025	Anthony Deans	Head of College

Rationale

Saint Mark's Coptic Orthodox College values the importance of technology in assisting students with their learning. The use of digital technologies is fundamental to the College's educational philosophies and by implementing Bring Your Own Device (BYOD); Saint Mark's College will assist students in developing digital literacy, fluency, and citizenship while preparing them for the high-tech world in which they will live, learn and work. It will empower students and give them direct involvement in the way they use technology in their learning. It will also allow teachers to continue to employ technology in the classroom while building on the experiences gained in the previously supported model.

Scope

This policy applies to all Saint Mark's Students Year 5 – 12 students and parents/guardians.

Guiding Principles

- The following principles guide how this policy will operate in practice:
- Equity and access to technology should be provided for all Saint Mark's students.
- Saint Mark's College will endeavour to provide a safe and secure online environment for all learning activities.
- The integration of ICT is to support and enhance contemporary, authentic learning in the College.

BYO Device Requirements

Hardware

- The device must support both 2.4 GHz and 5 GHz wireless networks.
- The device must support the 802.11n wireless protocol.
- It is recommended that the device should support the 802.11ac wireless protocol.
- The device should have a battery life of a minimum of 8 hours.

Operating System

- Year 5-9: Chromebook / Chrome OS
- Year 10-12: Laptop (Windows, Mac or Chromebook)

Security & Responsibility

- Use the recommended device for each year group.
- Ensure the device is in good working order with an updated OS.
- Install the latest antivirus and anti-malware software if appropriate.
- No "hacking" software allowed.
- Keep the device secure at all times.
- The College is not liable for damage or theft.
- Install all required College apps.
- Do not use the device while commuting, before school, recess, lunch and after school, unless supervised by a parent or teacher unless supervised.
- Users should ensure that the device is kept in a safe environment, free from excessive heat, moisture, or impact.
- Fault diagnosis, warranty claims and hardware and software repairs are not the responsibility of the College.

Usage & Classroom Expectations

- Bring the device daily, charged and ready for use.
- Devices should only connect to the College's secure Wi-Fi network.
- The College does not provide technical support for personal devices.

- Printing is allowed only via online or flash-drive methods. Direct connection of the device to the network is not permitted. It is the student's responsibility to have a suitable data-transfer device. It is best that a student prints at home.
- Devices must be used strictly for learning; misuse may result in restrictions.
- Device use during lessons is at the teacher's discretion.

Monitoring & Compliance

- Do not connect personal devices to college-owned equipment without permission.
- The College has permission to monitor and audit devices.
- The College may record device serial numbers and MAC addresses.

The College maintains the right to monitor and inspect any BYOD device suspected of containing material that is deemed inappropriate, offensive, or contrary to the values and ethos of the College. If reasonable suspicion arises that a student is storing, accessing, or distributing such material on their device, the College may take the following actions:

Confiscation

The device may be temporarily impounded for inspection by authorised staff.

Investigation

A formal review will be conducted, and the student may be required to provide access to the device. If necessary, parents/guardians will be informed.

Disciplinary Action

Consequences may range from warnings and restrictions on device use to suspension of BYOD privileges. Serious violations, including those involving illegal or harmful material, may lead to further disciplinary actions, up to and including the withdrawal of the student's enrolment in accordance with the College's policies.

Legal and External Involvement: In cases involving illegal content or activities, the College reserves the right to refer the matter to law enforcement or other appropriate authorities.

Review

This policy will be reviewed annually to ensure ongoing relevance and effectiveness. *Effective Date: March 2026.* For any inquiries related to this policy, please contact the College IT department.