



The Apple International Community School

Mobile phone and personal electronic device Policy

2026-2027

POLICY INFORMATION

Policy Written	August 2024
Policy Updated	June 2026
Policy to be reviewed	July 2027
Approved By	Principal- Ms Pretty



Index

Sno	Content
1	Purpose
2	Scope
3	Mobile Phones
4	Use of Personal Electronic Devices
5	VPN and Network Security
6	Exemptions
7	Emergency Communication
8	Responsibility of Students
9	Responsibility of Parents/Guardians
10	Breaches of the Policy
11	Policy Statement
12	Technical Support

1. Purpose

The purpose of this policy is to ensure that mobile phones and personal electronic devices do not interfere with teaching, learning, student wellbeing, safeguarding, or the orderly operation of the school. The school recognises that electronic devices can have educational and practical benefits. However, their use must be appropriately controlled to maintain a focused, safe, and respectful learning environment.

2. Scope

This policy outlines the terms and expectations for all students at The Apple International Community School who use their own devices, such as tablets or laptops, for educational purposes. The policy outlines the acceptable use of personal devices, the school's Wi-Fi network, computer/digital systems, and electronic communications. The policy aims to promote responsible and safe use of technology for teaching and learning purposes. It also protects all users from cyberbullying and guides them to recognize and address it appropriately.

This policy applies to all students and covers personal electronic devices including, but not limited to:

- Mobile phones and smartphones
- iPads and tablets
- Smartwatches and other wearable devices
- Personal laptops and computers
- Gaming devices
- Earbuds and wireless headphones
- Cameras and recording devices
- Any other internet-enabled personal electronic device

3. Mobile Phones

3.1 . AICS Mobile Rules:

1. Students are strictly prohibited from bringing mobiles into school.
2. Use of a mobile is strictly forbidden in all areas throughout the schools.
3. Mobiles must not be used to take photographs/video recordings not even for educational purposes
4. Mobiles must not be used to send images via Bluetooth or other sharing functions.
5. Teachers are authorised and fully expected to enforce the school's mobile rules and will be held accountable if they allow students to have and use mobiles during lessons, in corridors or other areas of the school during the school day.
6. AICS reserves the right to search the content of any mobile on the school premises where there is reasonable suspicion that it may contain undesirable material, violence or bullying.
7. Students are strongly discouraged from bringing mobile phones to school unless there is a genuine need. If a student brings a mobile phone to school, the student must submit the mobile phone to the Section Head upon arrival at school.
8. The Section Head will securely retain the device during the school day.

3.2 Collection of Mobile Phones

Students may collect their submitted mobile phones from the Section Head only at the time of school dispersal, in accordance with the school's dismissal procedures.

Students are not permitted to collect or use their mobile phones during the school day, including during:

- Lessons

- Breaks
- Lunch
- Assemblies
- Examinations
- School activities
- Trips or other supervised activities, unless specifically authorised

3.3 Failure to Submit a Mobile Phone

Any student who brings a mobile phone to school and fails to submit it to the Section Head will be considered to be in breach of this policy.

The school may confiscate the device and apply the appropriate disciplinary consequences in accordance with the school's Behaviour Policy.

4. Use of Personal Electronic Devices

Students may use iPads, tablets, laptops, or other electronic devices during lessons only when specifically permitted or instructed by a teacher for educational purposes.

Devices must be used responsibly and only for the task assigned by the teacher.

Students must not:

- Use devices for gaming or entertainment during lessons
- Access inappropriate or unauthorised websites
- Use social media without explicit teacher permission for an educational activity
- Record, photograph, or video students, staff, visitors, or school activities without appropriate permission
- Use devices to bully, harass, threaten, or intimidate others
- Attempt to bypass school internet or device restrictions
- Access content that is inappropriate, offensive, illegal, or contrary to school expectations

Device Specifications

The device specifications are as follows:

The specific devices permitted within the school are determined by the IT Administrator

iPad/Tablets:

Screen Size	10"-13" preferred; Any iPad or Android/Windows tablets.
Storage	64 GB minimum (128GB preferred).
RAM	4GB minimum (8GB preferred).
Battery Life	4 hours or more.
Wi-Fi	Wi-Fi capable 2.4/5GHz supported (802.11a/b/g/n)
Operating System	iOS version 17.0 or later. Android operating system version 12 or later, Windows 10 or later.
Accessories	Protective bag/case. Headphones during external exams.

Laptops:

Screen Size	13" preferred
Processor	Intel® or AMD processor with 64-bit support 8th Gen Intel Core i5; 2 GHz or faster processor Or equivalent such as the new M1 chips from Apple
Storage	128GB minimum
RAM	4GB minimum (8GB preferred).
Battery Life	4 hours or more.
Wi-Fi	Wi-Fi capable 2.4/5GHz supported (802.11a/b/g/n)
Operating System	Windows 10 or later. MacOS 10.14 or above
Accessories	Protective bag/case. Headphones during external exams.

5. VPN and Network Security

Students must not install, download, activate, or use VPN (Virtual Private Network) software or applications on iPads, tablets, laptops, or any other personal electronic devices used during lessons or on the school's network.

VPNs or other applications intended to bypass school network restrictions, filtering, monitoring, or security controls are strictly prohibited.

Students must not attempt to circumvent any school-installed internet safety, filtering, monitoring, or security measures.

Any device found to have an unauthorised VPN or similar bypass application may be removed from classroom use and referred to the Section Head or school leadership for appropriate action.

6. Smartwatches and Wearable Devices

Smartwatches and other internet-enabled wearable devices must not be used for communication, recording, accessing social media, or other unauthorised activities during lessons.

During examinations and assessments, students must follow the specific examination regulations concerning electronic and wearable devices.

7. Photography, Video and Audio Recording

Students must not photograph, video-record, or audio-record other students, staff, visitors, or school premises without appropriate permission.

The use of cameras or recording functions for bullying, intimidation, embarrassment, inappropriate sharing, or any other unauthorised purpose will be treated as a serious breach of school expectations.

8. Teaching and Learning

Where personal electronic devices are permitted for educational purposes:

1. The teacher will determine when and how the device may be used.
2. Students must follow the teacher's instructions at all times.
3. Devices must remain on the assigned application or activity.
4. Students must not use personal devices for unrelated activities.
5. Students must ensure that their devices are appropriately charged when required for learning.
6. Students must not attempt to bypass school security, filtering, or monitoring systems.

6. Exemptions

Exceptions to this policy may be considered in specific circumstances, including:

- Medical requirements
- Additional educational needs
- Accessibility requirements
- Other circumstances specifically approved by the school

Any exemption must be authorised by the school leadership and communicated to the relevant staff members.

7. Emergency Communication

In an emergency, students should not use their personal mobile phones unless instructed to do so by a member of staff.

Parents and guardians should use the school's designated communication channels for contacting students during the school day.

The school will provide appropriate arrangements for urgent communication between students and their parents/guardians.

8. Responsibility of Students

Students are responsible for:

- Following this policy at all times.
- Submitting mobile phones to the Section Head upon arrival if they bring them to school.
- Collecting submitted phones only at dispersal.
- Using permitted electronic devices responsibly.
- Ensuring that devices used for lessons do not contain VPN software or other applications intended to bypass school network controls.
- Respecting the privacy and dignity of others.
- Following all instructions given by teachers and school leadership.
-

9. Responsibility of Parents/Guardians

Parents and guardians are expected to:

- Support the school in implementing this policy.
- Ensure that students understand the rules regarding mobile phones and electronic devices.
- Avoid contacting students directly on their mobile phones during school hours except in exceptional circumstances.
- Use the school's official communication channels when communication with their child is necessary during the school day.

10. Breaches of the Policy

Breaches of this policy will be dealt with in accordance with the school's Behaviour and Discipline Policy.

Depending on the nature and frequency of the breach, consequences may include:

- Verbal reminder or warning
- Confiscation of the device
- Referral to the Section Head
- Parent/guardian notification
- Behavioural or disciplinary action

- Further consequences for repeated or serious breaches

Serious misuse of technology, including cyberbullying, unauthorised recording, accessing inappropriate content, or deliberate attempts to bypass school security systems, may result in more serious disciplinary action.

11. Policy Statement

The school expects all students to use technology responsibly and respectfully. The primary purpose of electronic devices in school is to support learning, communication where authorised, and student wellbeing.

Mobile phones brought to school must be submitted to the Section Head upon arrival and may only be collected at the time of dispersal. Electronic devices used for learning, including iPads and tablets, must not have VPN software installed or activated and must not be used to bypass the school's internet safety, filtering, monitoring, or security measures.

All students, parents, and staff are expected to support the consistent implementation of this policy.

12. Technical Support

As part of the BYOD Program, the school is committed to providing limited technical support to assist students with the following:

1. Connecting to the school's Wi-Fi/internet.
2. Installing recommended applications.
3. User profile management.

Please notify the IT support team at itsupport@applecommunityschool.ae, if:

1. You believe your password has been compromised or if you have been asked to provide your password to another individual.
2. You suspect you have received a phishing email. Each reported instance will be thoroughly investigated by the IT department.

Feedback from students and parents is actively sought to inform the review process.

Please reach out to us for any concerns or suggestions.