



ACCEPTABLE USE OF TECHNOLOGY POLICY

2026-2027

POLICY INFORMATION

Policy Written	September 2026
Policy Updated	September 2026
Policy to be Reviewed	June 2026
Approved By	Principal – Ms Pretty



Index

Sno	Content
1	Policy Statement
2	Purpose
3	Scope
4	Legal and Regulatory Framework
5	Guiding Principles
6	Roles and Responsibilities
7	General Acceptable Use of ICT
8	Digital Citizenship and Ethical Code
9	Bring Your Own Device (BYOD) Policy
10	Mobile Phone Regulations

11	Privacy, Data Protection and Security
12	Monitoring and Compliance
13	Consequences of Misuse
14	Reporting Concerns

ICT ACCEPTABLE USE POLICY

1. Policy Statement

The Apple International Community School (AICS) is committed to promoting the safe, responsible, and purposeful use of Information and Communication Technology (ICT) to support and enhance teaching, learning, assessment, and communication. As a British curriculum school operating within the United Arab Emirates, this policy establishes clear expectations and responsibilities for students, staff, parents, and visitors regarding the appropriate and responsible use of ICT within the school community.

The policy safeguards the wellbeing, privacy, and digital citizenship of the whole school community while ensuring full compliance with UAE law, the standards of the relevant local education regulator, and the expectations of British international-school best practice.

2. Purpose

This policy aims to:

- Support effective teaching, learning, and assessment through the appropriate and innovative use of technology.
- Promote responsible, ethical, and safe digital behaviour among all members of the school community.
- Protect students, staff, and the wider school community from online risks, including cyberbullying, exploitation, and exposure to harmful content.
- Ensure compliance with UAE legal and regulatory requirements and with the standards expected of a British curriculum school.
- Provide clear, consistent expectations for the use of school-owned ICT equipment and personally owned devices (BYOD).
- Define the consequences of misuse and the procedures for reporting concerns.

3. Scope

This policy applies to:

- All students, from Foundation Stage through to Year 11.
- All teaching and non-teaching staff, including leadership, administrative, and support personnel.
- School-owned devices, networks, servers, cloud platforms, and learning-management systems.
- Personally owned devices (laptops, tablets, phones, wearables) brought onto the premises or used for school-related activities under the BYOD provisions of this policy.
- All digital platforms, applications, artificial intelligence tools, and online services used for school purposes, on or off site.
- Parents, guardians, governors, and visitors while accessing the school's network or digital resources.

4. Legal and Regulatory Framework

This policy has been developed with reference to, and operates in full alignment with, the following legal and regulatory instruments:

- UAE Federal Law No. 3 of 2016 concerning Child Rights (“Wadeema's Law”).
- UAE Federal Decree-Law No. 34 of 2021 on Combating Rumours and Cybercrimes (the “UAE Cybercrime Law”).
- UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (PDPL).
- Ministry of Education (MoE) Child Protection and Digital Safety Regulations and the MoE Code of Conduct for Educational Professionals.
- The standards and inspection frameworks of the relevant local education regulator (KHDA).
- Principles consistent with UK statutory guidance on online safety and safeguarding in schools (Keeping Children Safe in Education), adapted to the UAE context.
- The school's own Child Protection & Safeguarding Policy, E-Safety Policy, Data Protection Policy, and Behaviour Policy.

Where any provision of this policy appears to conflict with UAE law or the requirements of the relevant local regulator, UAE law and regulatory requirements shall prevail.

5. Guiding Principles

ICT use at The Apple International Community School (AICS) is guided by the following principles:

- Technology enhances learning, engagement, and achievement when used purposefully and under appropriate guidance.
- Digital safety and safeguarding are paramount and take precedence over convenience or preference.
- Respect, responsibility, and integrity apply equally online and offline.
- Every user is accountable for their own digital actions and their consequences.
- ICT use must at all times comply with the school's values, this policy, and the laws of the United Arab Emirates.

6. Roles and Responsibilities

6.1 Senior Leadership and Governors

- Ensure this policy is implemented consistently, reviewed annually, and reflects current legislation and best practice.
- Allocate appropriate resources, training, and IT support to uphold safe and effective ICT use.
- Ensure that all safeguarding concerns arising from ICT misuse are managed in line with the Child Protection & Safeguarding Policy.

6.2 IT Department / Network Manager

- Maintain network security, filtering, and monitoring systems appropriate to the age and needs of students.
- Manage user accounts, access permissions, and password policies.
- Log and escalate technical breaches, attempted security bypasses, or suspected cyber incidents to the Designated Safeguarding Lead and Senior Leadership Team as appropriate.

6.3 Teachers and Staff

- Use ICT professionally, responsibly, and only for approved educational or administrative purposes.
- Protect the confidentiality of student data, assessment records, and staff communications at all times.
- Use only school-approved platforms for communication with students and parents.
- Model positive digital citizenship and supervise students' use of technology during lessons and school activities.
- Report any concerns about student or staff online safety immediately to the Designated Safeguarding Lead.

6.4 Students

- Use ICT only under staff direction or for approved learning activities.
- Access only age-appropriate, educational content.
- Communicate respectfully and appropriately in all digital spaces.
- Protect their own and others' personal information, passwords, and account security.
- Obtain permission before recording, photographing, or publishing any content involving other members of the school community.
- Report cyberbullying, harassment, or any online safety concern to a trusted adult without delay.

6.5 Parents and Guardians

- Support the school's approach to responsible technology use by reinforcing expectations at home.
- Engage in regular, open conversations with their children about online activity and digital wellbeing.
- Ensure that any device brought to school under the BYOD provisions meets the requirements set out in Section 9.
- Contact the school office rather than a child's personal device for urgent matters during the school day.

7. General Acceptable Use of ICT

7.1 Educational Purpose

All technology use on the school network or on school premises must primarily support educational objectives. Personal, recreational, or commercial use of ICT during the school day is discouraged and, where it interferes with learning or duties, is not permitted.

7.2 Network and Bandwidth Usage

- Access to network resources is granted according to user role; unauthorised access or attempts to bypass security controls are strictly prohibited.
- Streaming of non-educational content, large unauthorised downloads, and excessive gaming on the school network are not permitted.

7.3 Accessing Approved Content

Students and staff must only visit websites and use applications approved by the school. The school employs content filtering and monitoring appropriate to the age of users; any attempt to circumvent these safeguards is treated as a serious breach of this policy.

7.4 Social Media

- Anyone representing the school online must maintain professionalism, use appropriate language, and share only accurate information.
- Users must adjust privacy settings appropriately and consider carefully the content they share, ensuring it does not compromise the safety, dignity, or reputation of any member of the school community.
- Posting defamatory, offensive, or misleading content about the school, its staff, or its students is strictly prohibited and may result in disciplinary or legal action.

8. Digital Citizenship and Ethical Code

8.1 Academic Integrity

- All assignments, projects, and research must represent the student's own work, with sources properly cited according to an approved referencing style.
- Copying from peers, using unauthorised resources during assessments, or falsifying research data constitutes academic misconduct.
- Online research must draw on credible, accurate, and relevant sources.

8.2 Ethical Use of Artificial Intelligence and Digital Tools

- AI-based tools (for example, generative chatbots, translation tools, or grammar checkers) must be used only in ways explicitly permitted by teachers and in line with the school's Academic Integrity guidance.
- AI must not be used to generate assignments, assessments, or other work submitted for a grade in place of a student's own effort.

- Any AI-assisted work must be clearly acknowledged where required by the teacher.

8.3 Digital Etiquette

- Students and staff must use polite, professional, and appropriate language in all online discussions, emails, and group chats related to school activities.
- Excessive informal language, slang, or emojis should be avoided in formal school communications.
- When attending virtual lessons, students should follow the school's netiquette expectations, including muting microphones when not speaking, dressing appropriately, and maintaining a distraction-free environment.

8.4 Cyberbullying and Harassment

Cyberbullying, harassment, hate speech, or intimidation in any form — including the spreading of false information, derogatory comments, or sharing private content without consent — is strictly prohibited and will be treated as a serious safeguarding matter, managed jointly under this policy, the Anti-Bullying Policy, and the Child Protection & Safeguarding Policy.

8.5 Digital Footprint and Online Reputation

- All users should understand that online actions create a permanent digital footprint that can be retrieved and misused even after deletion.
- Content that could harm a person's or the school's reputation should never be posted.
- Users must verify information before sharing it and must not circulate misinformation, propaganda, or misleading content.

9. Bring Your Own Device (BYOD) Policy

Where the school permits students or staff to bring personally owned devices onto the premises, the following provisions apply in addition to the general acceptable use expectations set out above.

9.1 Eligibility and Registration

- BYOD is permitted only for year groups, roles, or purposes explicitly authorised by the school.
- All personal devices used on the school network must be registered with the IT Department and connected only via the designated guest or student Wi-Fi network.
- Devices must meet minimum operating system and security requirements set by the IT Department, including up-to-date antivirus or security software where applicable.

9.2 Use of Personal Devices

- Personal devices may be used only for approved educational purposes and only when and where a teacher has given explicit permission.
- Devices must remain switched off or in a designated storage area at all other times, in accordance with the Mobile Phone Regulations in Section 10.

- Staff should avoid using personal devices for school-related work (including communicating with students or parents) unless specifically authorised by the administration, and must never store student data on personal devices.

9.3 Security and Data Protection on Personal Devices

- Users are responsible for the physical security of their own devices; the school accepts no liability for loss, theft, or damage to personal devices brought onto the premises.
- Personal devices must not be used to store, process, or transmit confidential school data, including student records, assessment data, or staff communications, except through school-approved, secured platforms.
- Any lost or stolen device that may have contained school data must be reported to the IT Department and the Data Protection Officer immediately.

9.4 Software and Applications

- Only applications relevant to learning may be installed and used on a personal device while connected to the school network.
- Downloading, sharing, or using pirated or unlicensed software on the school premises or network is prohibited.

10. Mobile Phone Regulations

Reflecting the emphasis of UAE education regulators on minimising distraction and promoting effective learning environments, the following mobile phone regulations apply.

10.1 Students

- Mobile phone use by students is strictly prohibited during school hours, including breaks and extracurricular activities, unless explicit teacher permission has been granted for an approved educational purpose.
- Where students are permitted to bring a mobile phone to school (for example, due to independent travel arrangements), the phone must be handed over to the Head of Section immediately on arrival and returned at the end of the school day.
- A signed parental consent form is required before any student is permitted to carry a mobile phone on school premises.
- Any student found with an unauthorised mobile phone will have it confiscated immediately; the device will be returned only following a meeting with the student's parents.

10.2 Staff

- Teachers must not use mobile phones during lessons, supervision duties, or other assigned responsibilities, and must never bring a student's phone into the classroom.
- Personal mobile phone use by staff during instructional time must not interfere with professional responsibilities.

10.3 Parental Communication

Parents are asked to contact the school office for urgent matters rather than contacting a child's personal device directly during the school day. Parents or family members wishing to meet a student in person must register at the school reception.

11. Privacy, Data Protection and Security

11.1 Passwords and Account Security

- Passwords must be at least eight characters, combining letters, numbers, and special characters.
- Passwords must never be shared, written down insecurely, or reused across unrelated accounts.
- Multi-factor authentication (MFA) must be enabled on school platforms where it is available.
- Users must log out of shared or public devices immediately after use.

11.2 Confidentiality of School Data

Students, teachers, and staff must maintain the confidentiality of sensitive school information, including examination papers, student records, safeguarding information, and staff communications. Such information must be stored, shared, and transmitted only through school-approved, secured systems, consistent with the UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data.

11.3 Protection Against Cyber Threats

Users must not click on suspicious links, download unverified files, or engage in any activity that could introduce malware or compromise the security of the school network. Suspected phishing or cyber-security incidents must be reported to the IT Department immediately.

11.4 Copyright and Intellectual Property

- Users must respect copyright law and give proper credit to the sources of any digital content they use.
- Plagiarism, including the unauthorised copying of text, images, video, or software, is strictly prohibited.
- Only authorised and licensed software may be installed on school devices.

12. Monitoring and Compliance

The school reserves the right to monitor the use of its network, devices, and platforms, including internet browsing history, email, and messages sent through school-approved systems, to ensure compliance with this policy and to safeguard the wellbeing of students and staff. Monitoring is conducted proportionately and in accordance with the school's Data Protection Policy and applicable UAE law.

Any attempt to alter network settings, disable filtering or monitoring systems, or otherwise disrupt the school's IT infrastructure will result in disciplinary action and may be reported to the relevant authorities.

13. Consequences of Misuse

Breaches of this policy will be addressed in accordance with the school's Behaviour Policy and, where relevant, the Child Protection & Safeguarding Policy. The table below illustrates indicative categories of misuse; the school retains discretion to determine the appropriate response based on the circumstances of each case.

Category	Example Behaviour	Indicative Response
Minor	Inappropriate website access, excessive personal device use, unauthorised app use	Verbal warning, counselling, temporary restrictions from devices or internet access
Moderate	Disrespectful online behaviour, unauthorised social media posts, academic dishonesty	Written warning, parental notification, loss of network or platform access for a specified period
Severe	Cyberbullying, hacking, data breaches, sharing explicit or harmful content, safeguarding violations	Suspension or expulsion in line with regulatory requirements; referral to relevant UAE authorities where the offence may be criminal

The relevant UAE education regulator enforces a zero-tolerance approach to abusive conduct involving ICT or mobile devices that could be deemed criminal or culturally insensitive. Such incidents will be reported promptly to the appropriate authorities.

14. Reporting Concerns

Any member of the school community who becomes aware of a breach of this policy, an online safety risk, or a safeguarding concern arising from ICT use must report it immediately to the Designated Safeguarding Lead, a class teacher, or a member of the Senior Leadership Team. Concerns may also be raised confidentially with the school's IT Department where they relate to network security.