



The Apple International Community School

DIGITAL SAFEGUARDING POLICY

2026-2027

POLICY INFORMATION

Policy Written	September 2026
Policy Updated	September 2026
Policy to be Reviewed	June 2027
Approved By	Principal – Ms Pretty



Index

Sno	Content
1	Intent
2	Scope
3	Definitions
4	Guidelines

DIGITAL SAFEGUARDING POLICY

1. Intent

The Apple International Community School (AICS) has a statutory obligation to maintain a safe, secure and supportive physical and emotional environment for all members of its school community. The School also recognises its responsibility to promote the safe, responsible and ethical use of the Internet and Information and Communication Technologies (ICT).

The Internet and ICT devices and equipment provide significant benefits to teaching, learning, communication and the effective operation of the School. AICS places a high priority on providing reliable Internet facilities and appropriate ICT resources that enhance learning outcomes, support innovation and improve the efficiency of school operations.

However, the School recognises that the use of these technologies—whether provided by the School or privately owned by staff, students or other members of the school community—can also provide opportunities for access to inappropriate, harmful, anti-social or illegal material and activities.

The school therefore has a dual responsibility to maximise the educational and operational benefits of technology while taking appropriate measures to minimise, manage and respond to associated risks.

This policy provides a framework for maintaining rigorous and effective cyber safety practices across AICS and promoting safe, responsible and respectful use of digital technologies.

Our Vision

Empowering students with values and skills to excel in a dynamic world.

Our Mission

- To deliver high-quality, forward-thinking education that equips every student with the knowledge, skills, attitudes and global competencies required to excel.
- To create a nurturing and inclusive environment where all learners are enabled to contribute meaningfully to their communities and beyond.
- To inspire a passion for discovery and nurture innovative mindsets.
- To develop individuals who embrace every learning experience, build emotional and mental resilience, and develop a growth mindset to navigate challenges confidently.

2. Scope

The Apple International Community School (AICS) will develop, implement and maintain rigorous and effective Cyber Safety practices designed to:

- maximise the benefits of the Internet and ICT devices and equipment for teaching, learning and the effective operation of the School;
- promote safe, responsible, respectful and ethical use of digital technologies;
- minimise and appropriately manage risks associated with the use of the Internet and ICT;
- protect students, staff and other members of the school community from online risks and harm; and
- develop the knowledge, skills and understanding required to participate safely and

responsibly in an increasingly digital world.

This policy applies to all students, staff and other authorised users of the School's Internet facilities, ICT systems and equipment, including the use of personal devices where they are used on School premises or in connection with School-related activities.

3. Definitions

Cyber Safety practices are intended not only to maintain a safe digital environment within the School but also to ensure that students and other members of the school community receive appropriate education and guidance regarding the safe, responsible and ethical use of current and emerging information and communication technologies.

For the purpose of this policy:

1. **ICT** refers to Information and Communication Technologies.
2. **Cyber Safety** refers to the safe, responsible, respectful and ethical use of the Internet and ICT equipment and devices, including mobile phones and other connected technologies.
3. **School ICT** refers to the School's computer network, Internet access facilities, computers, digital platforms, systems and other ICT equipment and devices provided, owned, leased or managed by the School.
4. **ICT equipment/devices** includes, but is not limited to:
 - desktop computers and laptops;
 - tablets and other portable computing devices;
 - storage devices such as USB flash drives and memory cards;
 - cameras, digital cameras, video cameras and webcams;
 - mobile phones and smartphones;
 - audio and video players or receivers;
 - gaming consoles;
 - wearable and connected devices; and
 - any other current or emerging technologies capable of connecting to, storing, accessing or transmitting digital information.

4. Guidelines

AICS recognises that effective Cyber Safety requires a whole-school approach. Related considerations include:

- alignment with the School's annual and strategic development plans;
- appropriate deployment of staff and allocation of responsibilities;
- regular professional development and training for staff;
- integration of Cyber Safety and digital citizenship within the curriculum;
- appropriate education and awareness programmes for students, staff and parents;
- clear procedures for responding to breaches of Cyber Safety;
- appropriate disciplinary and pastoral responses to incidents;
- safeguarding and wellbeing support for students and staff affected by online incidents; and
- consideration of relevant employment, legal and regulatory requirements.

The school delegates to the Principal the responsibility for ensuring the development, implementation and monitoring of appropriate management procedures, practices, technical controls, electronic systems and educational programmes to maintain a safe digital environment.

4.1 Acceptable Use Agreements

No student may use the School's Internet facilities or School-owned, leased or managed ICT devices and equipment unless the appropriate Acceptable Use Agreement has been completed and, where applicable, signed and returned to the School.

Acceptable Use Agreements may also apply to privately owned or leased ICT devices used on School premises or during any School-related activity, regardless of location. This includes access to School networks, systems or resources from School-owned or privately owned devices.

4.2 Authorised Users

AICS Acceptable Use Agreements and Cyber Safety requirements apply to all authorised users of the School's Internet facilities and ICT systems. This includes:

- students;
- teaching and non-teaching staff;
- tutors and external providers;
- contractors;
- volunteers;
- visitors; and
- other individuals authorised by the School to access its Internet facilities, networks or ICT resources.

4.3 Appropriate Use

The use of the Internet and ICT devices and equipment by staff, students and other authorised users must be appropriate to the School environment and consistent with the relevant Acceptable Use Agreement.

Use should support:

- teaching and learning;
- professional development;
- approved School activities and operations; and
- limited personal use where permitted by the School and where such use is appropriate, responsible and does not interfere with School activities or compromise security.

4.4 Monitoring and Review

The School reserves the right, in accordance with applicable laws, regulations and School procedures, to monitor, access and review the use of its Internet facilities, networks, systems and ICT equipment.

This may include monitoring electronic communications and activity conducted using School-owned or School-managed devices, systems and network facilities.

Users should have no expectation of personal privacy when using School-owned systems, devices or network facilities, subject to applicable legal and regulatory requirements.

4.5 Auditing of Devices and Equipment

The School reserves the right to audit or inspect material stored on School-owned, leased or managed equipment and systems where there is a legitimate safeguarding, security, disciplinary or operational reason to do so.

Where permitted by applicable laws, regulations and School procedures, the School may also request access to privately owned ICT devices used on School premises or during School-related activities where there is a reasonable concern relating to Cyber Safety, safeguarding or a potential breach of School policy.

4.6 Confidentiality and Data Protection

All matters relating to confidentiality, privacy and the protection of personal information must be handled in accordance with the School's relevant policies, procedures and applicable UAE legislation and regulatory requirements.

This includes:

- the collection and use of student and staff information;
- the purpose for which personal data is collected;
- the secure storage and handling of personal information;
- the appropriate use and storage of photographs and images;
- access to confidential information; and
- the secure transmission and disposal of digital information.

All members of the school community are expected to protect confidential information and use personal data responsibly.

4.7 Reporting and Responding to Incidents

The safety and wellbeing of students and staff is of paramount importance. Any suspected or actual breach of Cyber Safety will be taken seriously and dealt with in accordance with the School's established procedures.

Responses to individual incidents will be proportionate to the nature and seriousness of the incident and may include:

- investigation and evidence gathering;
- safeguarding measures;
- pastoral support;
- parental communication where appropriate;
- disciplinary action in accordance with School procedures; and
- referral to appropriate external agencies where required.

In serious or complex cases, the School may seek advice from an appropriate specialist, including legal or safeguarding professionals.

Particular care will be taken to preserve and secure relevant digital evidence in potentially serious cases.

Where illegal material or activity is suspected, the School may report the matter to the appropriate law enforcement or regulatory authorities in accordance with applicable UAE legislation and School procedures.

4.8 Harmful, Inappropriate or Illegal Content

Where the School has reasonable grounds to believe that a device, account, application, online platform or digital communication contains or has been used to access or distribute material relating to:

- bullying or cyberbullying;
- sexual or exploitative content;
- discriminatory or racist content;
- violent or threatening material;
- harassment or intimidation;
- illegal activities;
- material that poses a safeguarding risk; or
- content that could bring the School or members of its community into serious disrepute, the School reserves the right, in accordance with applicable laws, regulations and School procedures, to investigate and take appropriate action.

Where appropriate and legally permissible, authorised members of staff may inspect School-owned devices and, where there are legitimate safeguarding or disciplinary grounds, may require the inspection of personal devices brought onto School premises or used for School-related activities.

Such devices may include, but are not limited to:

- mobile phones;
- tablets;
- laptops;
- cameras;
- video recording devices; and
- other digital or connected devices.

This review may also include social media profiles that are publicly visible.