

Digital Safeguarding and Acceptable Usage Policy

Academic year 2026–27

Why this policy matters

Digital technology is fundamental to learning, communication and creativity at Arab Unity School (AUS), but it also brings safeguarding, privacy and cybersecurity risks. This single policy sets out how students, staff, parents and visitors use technology safely, ethically and responsibly. It brings together our previous Cybersecurity, Social Media and Online, and Students' AI Usage policies, covers students from FS2 to Year 13, and applies whenever technology is used in connection with the school, on or off site, on school-owned or personal devices.

Our principles

- The safety and welfare of students are paramount, and technology should support learning, not replace effort or responsibility.
- Online behaviour should meet the same standards of respect, honesty and safety as behaviour face to face, and everyone is accountable for activity on their own accounts.
- Digital safeguarding is shared between school, students and families, and concerns should be reported early.

The policy operates within UAE and Dubai law, including Federal Law No. 3 of 2016 on Child Rights and Federal Decree Law No. 34 of 2021 on Combatting Rumours and Cybercrimes.

The risks we address

Area of risk	Examples
Content	Harmful, violent, extremist or inappropriate material, and misinformation.
Contact	Grooming, coercion, exploitation, fake profiles and requests for personal information.
Conduct	Cyberbullying, harassment, impersonation and sharing images without consent.
Commerce	Phishing, scams, fraudulent links and attempts to obtain passwords or payment details.

Acceptable use of school technology

School devices, networks and accounts are for learning and legitimate school business. Users follow staff instructions, use only accounts they are authorised to use, respect copyright and report accidental access to harmful content or unusual account activity straight away. They must not hack or bypass school security, use another person's account, install malicious or pirated software, access or share harmful material, or use school systems for bullying, harassment, fraud or any unlawful activity.

DO	DO NOT
• Use technology for learning and school purposes • Protect passwords and use two-factor authentication • Use official school communication platforms • Think before posting or sending • Check sources and AI outputs critically • Report harmful or suspicious activity quickly	• Share passwords or use another person's account • Bypass filtering or security, or attempt hacking • Access or share illegal or harmful content • Cyberbully, threaten, impersonate or harass • Record or share people without consent • Enter confidential information into unapproved AI tools

Personal devices

Students in FS2 to Year 2 may not use personal digital devices in school unless the school specifically authorises it. Students in Year 3 to Year 13 may bring a personal device only with teacher permission, for an agreed educational purpose, and must use the approved student network. Phones, smartwatches, headphones, cameras and recording functions must not be used without permission, and no one may photograph, film or livestream another person without consent. Misuse may lead to confiscation, restricted access, parent contact or further action.

Accounts, passwords and scams

Users choose strong, unique passwords, never share them and report any suspected compromise at once. Everyone should be alert to phishing by email, message, text or call: check the sender and links before clicking, avoid unexpected attachments, and treat urgent requests for log-in details as suspicious.

Social media and online communication

Online communication connected with AUS must be respectful and lawful. Official school platforms are used for school communication, and routine messaging is avoided between 8:00 p.m. and 7:00 a.m. unless urgent. Photos and videos of students are shared only with the required consent and authorisation. Staff may not message students privately through personal social media or messaging accounts.

Artificial intelligence

AUS supports responsible use of AI where it enhances learning without replacing personal effort or academic integrity. Only AI tools approved by the school may be used for school work. Students must not submit fully AI-generated work as their own, must follow their teacher's guidance, disclose AI help where required and check outputs for errors and bias. Personal, confidential or safeguarding information must never be entered into AI tools. Staff remain fully accountable for anything produced with AI assistance.

Cyberbullying and harmful content

Cyberbullying includes abusive messages, spreading rumours, sharing embarrassing images, impersonation, threats, deliberate exclusion from groups, sexual harassment and hate-based abuse. Anyone who experiences or witnesses it should tell a trusted adult, avoid responding or forwarding the content, and keep evidence such as screenshots. Online harm between students can be a safeguarding concern.

Privacy and school monitoring

Users should share only the minimum personal information needed, never publish addresses, phone numbers or identity documents, and not accept contact from unknown people or arrange to meet someone known only online. The school protects information through secure access controls, filtering, monitoring and security updates. Activity on school-owned devices, accounts and networks may be monitored for safeguarding, security and operational reasons.

Reporting concerns

If you have a concern about...	Please report it to...
A child may be at risk online: grooming, cyberbullying, inappropriate images	Tell a member of staff straight away. Concerns go to the Designated Safeguarding Lead, and safeguarding action always takes priority.
A cybersecurity concern: phishing, hacking or a compromised account	Report immediately to IT and Operations so it can be secured.
Concern about an adult's communication with a student	Report to the Principal or safeguarding team.
Any other misuse of technology	Tell the class teacher or phase leader.

Working together at home

Parents and guardians are essential partners. We encourage four practical actions:

- **Educate:** know the apps and games your child uses and talk about them.
- **Protect:** use age-appropriate parental controls and privacy settings, remembering they are not foolproof.
- **Monitor:** keep open dialogue and age-appropriate oversight, especially for younger children.
- **Support:** make sure your child knows they can tell a trusted adult if something goes wrong, and how to block and report.

Education, consequences and review

AUS teaches digital literacy and online safety from FS2 to Year 13 and provides staff training and parent guidance. Breaches are considered according to seriousness, intent, impact, age and safeguarding risk. For students, responses can include education and support, restricted device privileges, contact with parents, a behaviour contract, suspension or, where required, referral to external authorities. The policy is reviewed annually, and sooner after significant incidents or regulatory change.