E-Safety, Online Protection & Digital Safeguarding Policy

Reviewed in April 2026

Next review April 2027

Reviewed by Principal, Slt's



e-SAFETY, ONLINE PROTECTION & DIGITAL SAFEGUARDING POLICY

AL AMAAL ENGLISH HIGH SCHOOL
Sharjah, United Arab Emirates

Academic Year 2026–2027

Policy version	**1.0**
Status	Management Approval
Effective date	Session 2026-2027
Policy owner	Principal
Technical implementation	IT Department
Review date	October 2026

1. Policy Statement

Al Amaal English High School is committed to a safe, secure, respectful and inclusive digital learning environment for students, staff and families. Online learning, connected devices and AI can improve education but can also expose children to cyberbullying, exploitation, inappropriate content, identity theft, misinformation and privacy risks.

The school will not tolerate online abuse, exploitation, intentional privacy violations or malicious misuse of technology. Every concern will be managed fairly, confidentially, proportionately and with the best interests of the child as a primary consideration.

2. Purpose and Objectives

This policy aims to protect learners from digital harm; promote responsible and age-appropriate technology use; protect student and staff information; define rules for school devices, Wi-Fi and personal devices; establish safe AI practices; prevent unauthorised access; provide clear incident reporting procedures; improve digital literacy; and support compliance with relevant UAE legislation and Sharjah education requirements.

3. Scope and Applicability

This policy applies to Kindergarten–Grade 12 students; teachers; administrative, technical, support and contracted staff; school leadership; parents and guardians; visitors; and third-party providers. It covers school-owned and authorised personal devices, networks, email, the school ERP, learning platforms, school communication services and online classes. It also applies to off-campus digital conduct where school systems, school-related communication or student safety are affected.

4. Jurisdiction and Limits of School Responsibility

This section defines the boundaries of the school's authority and responsibility in relation to online incidents, social-media activity and related disputes. It applies to students, staff, parents and all members of the school community.

Incidents within the school's jurisdiction. The school shall take action, in accordance with this policy and the applicable behaviour and safeguarding procedures, where an incident: (a) occurs within the school premises, during school hours, or during a school-organised or school-supervised activity, whether on-site or off-site; or (b) occurs outside the school premises but directly involves an official school social-media account, a school system, a school-managed platform, an official class or school group, or any other school-related communication channel.

Incidents outside the school's jurisdiction. The school shall have no jurisdiction over, and bears no responsibility for, incidents that: (a) occur wholly outside the school premises, outside school hours and outside school-supervised activities; (b) involve only personal social-media accounts, personal IDs, personal devices, or personal messaging groups that are not created, owned, or managed by the school; or (c) arise from personal, family, or community disputes between individuals that are unrelated to the school, to staff acting in their official capacity, or to the school's official channels.

No obligation to intervene. For incidents outside its jurisdiction, the school is not required or expected to investigate, mediate, arbitrate, monitor personal accounts, or take disciplinary action. Such matters are the personal responsibility of the individuals concerned and, in the case of students, of their parents or guardians. Where a matter may involve a criminal offence

or a threat to any person's safety, the parties should report it directly to the competent authorities, such as the police or the relevant cybercrime reporting channels.

Spillover into school. Where an incident that began outside the school's jurisdiction later gives rise to conduct within the school premises or on official school channels — for example, continued harassment at school or on an official school group — the school may take action only in respect of that in-school or school-channel conduct, in accordance with this policy.

Parental responsibility. Parents and guardians remain responsible for supervising their children's use of personal devices, personal accounts and personal social-media activity outside the school, and for resolving personal disputes through the appropriate channels.

Safeguarding exception. Nothing in this section limits the school's duty to act on, or to refer to the competent authorities, any safeguarding concern involving a child — including a concern first identified outside the school premises — where such action or referral is required by UAE law or child-protection procedures.

5. Legal and Regulatory Framework

The school shall apply the relevant provisions of UAE Child Rights Law (Federal Law No. 3 of 2016); Federal Decree-Law No. 26 of 2025 on Child Digital Safety; applicable 2026 Cabinet-level rules on children's social-media access; Federal Decree-Law No. 34 of 2021 on combating rumours and cybercrimes; and Federal Decree-Law No. 45 of 2021 on the protection of personal data, subject to its statutory scope and exemptions.

The school shall also follow applicable Ministry of Education child protection guidance, Sharjah Private Education Authority (SPEA) requirements and subsequent official directions. Where binding law or regulatory instructions impose stricter requirements, they shall take precedence. Legal references and operational procedures must be confirmed by school management before publication.

6. Governance and Responsibilities

Principal: approve policy and procedures, assign resources, oversee serious incidents and ensure annual review.

Designated Child Protection Officer (DCPO) and deputy: receive and triage safeguarding reports, prioritise student welfare, maintain confidential safeguarding records, coordinate lawful parent/authority notifications and organise support.

IT Department: operate security controls, protect school systems, investigate technical incidents within its remit, preserve relevant technical evidence and escalate suspected breaches. IT does not independently determine child protection outcomes.

Teachers and staff: supervise technology use, model appropriate conduct, safeguard student records and immediately report concerns.

Students: respect others, protect passwords, use technology for approved learning and seek help when unsafe.

Parents/guardians: promote safe technology use at home, apply age-appropriate controls and cooperate with safeguarding procedures.

7. Acceptable Use of Technology

School internet and resources are primarily for authorised teaching, learning and administrative purposes. Users must not access prohibited or harmful content; bypass filters; use another person's account; install unauthorised software; engage in hacking, phishing, harassment or fraud; distribute malware; or record, share or publish another individual's information without lawful permission.

VPNs, proxies, personal hotspots or similar tools must not be used to circumvent school safeguarding restrictions. Exceptions for legitimate educational or technical needs require prior authorisation.

9. Mobile Phones and Personal Devices

Personal devices may be brought to or used at school only under applicable school and regulator rules. Where authorised for learning, devices must be used at the teacher's direction. Camera or audio recording, gaming, social media and unrelated entertainment are prohibited during instructional time unless specifically authorised for education.

Lost, stolen or compromised devices holding school data must be reported promptly. Any device confiscation or examination must follow lawful, documented and proportionate safeguarding and student-behaviour procedures; private accounts must not be searched without proper authority.

10. Social Media and Online Communication

The school shall not require children to create personal social-media accounts contrary to UAE age restrictions or provider terms. Personal accounts for children under 15 must be addressed in accordance with applicable UAE rules, including any relevant exceptions and implementation requirements.

School communication shall use approved ERP, email or messaging channels. Staff shall not establish inappropriate personal online relationships with students, use private accounts for unauthorised one-to-one student communication, disclose confidential information in private groups or publish student images without appropriate authorisation. Official school accounts shall be managed by authorised staff.

11. Cyberbullying and Online Harassment

Cyberbullying includes electronic threats, humiliating posts, hostile messages, harmful impersonation, malicious rumours, discriminatory abuse, deliberate online exclusion used to harass, and sharing private or manipulated images to cause harm. A single serious event may warrant urgent safeguarding action even without repetition if related to school or any school staff/member included in the incident. Personal disputes arising outside the school premises on personal accounts fall outside the school's jurisdiction (see Section 4), unless an official school account, system or platform is involved.

Reports may be made to any trusted staff member. The discipline committee must assess immediate safety, arrange support, preserve evidence safely, inform parents when appropriate, and coordinate fair investigation and proportionate action. Serious exploitation, threats or suspected offences must be escalated to competent authorities where required. Retaliation for good-faith reporting is prohibited.

12. Artificial Intelligence Safety

School-approved AI may support lesson planning, quizzes, language assistance, supervised learning and administrative productivity. Teachers must check outputs for accuracy, bias, cultural appropriateness and age suitability.

AI must not be used to impersonate others, fabricate harmful images or voices, facilitate bullying, generate abusive content, circumvent academic integrity rules or upload confidential student records, photographs or health information into unapproved tools. High-impact decisions about safeguarding, discipline or assessment require human review. Student access shall follow platform age requirements and approved supervision.

13. Student Data Protection and Privacy

Protected information includes identities, admission records, contact details, student images, medical information, assessments, attendance, counselling, staff records and fee/transport details. Access must follow legitimate duties and authorised roles. The school shall use strong authentication, encrypted transmission, secure backups, appropriate logs, controlled sharing, defined retention rules and secure deletion where required.

Suspected personal-data exposure must be escalated promptly for investigation, containment and any legally required notifications. Sensitive information must not be transferred into unapproved AI platforms or third-party applications.

14. School ERP and Digital Services

The school ERP is a sensitive official record system. Individual accounts, server-side authorisation, role-based access, record ownership checks, secure sessions, input validation, encrypted connections, audit logs and tested backups are required. Users must not share credentials or export confidential records to insecure devices.

Parent messaging and WhatsApp integrations must be approved, use verified recipients, enforce access permissions and reduce accidental disclosure. Examination, financial, health, HR and student records shall be available only to appropriately authorised roles.

15. Photography, Video and Digital Media

Student photographs, videos and audio must be collected, stored and published for authorised purposes with required permissions. The school shall respect opt-outs and restrictions, avoid attaching sensitive identifying details, restrict access to media archives and prohibit recording in spaces where privacy is expected.

Suspected intimate, exploitative or abusive images involving a child require immediate safeguarding escalation. Staff and students must not circulate such material.

16. Event Photography, Consent and Individual Responsibility

The school has a total strength of approximately 2,000 persons, comprising more than 120 staff members and over 1,800 students. Given the size of the school community, it is not practically possible for the school's social media administrator to identify, at the time of posting, which individuals have or have not signed the photography consent form, or to verify the consent status of every individual face appearing in group photographs and event coverage.

Voluntary participation constitutes consent. Any staff member or student who voluntarily poses for, participates in, or knowingly remains within a group photograph, event photograph, or video being recorded at a school event or activity shall be deemed to have consented to the publication of that photograph or video on the school's official social-media channels and website.

Submission of photographs constitutes consent. Photographs or videos sent or submitted by any staff member to post — whether directly or through another person — to the school for publication shall be treated as submitted with the consent of the individuals appearing in them.

Duty to remain aside. Any individual who has not signed the photography consent form, or who does not wish to be photographed, filmed, or published, must keep themselves aside from the place where photographs or videos are being taken, and must not position themselves in the centre of group photographs or within the main photography area of any event.

No obligation to delete or re-edit. Where an individual has voluntarily participated in a photograph or video, or has positioned themselves within the photography area of an event, the school and its social media administrator shall bear no responsibility for that individual's appearance in the published material, and shall not be obliged to delete, crop, re-edit, or withdraw the published photograph or video on that ground. Deletion requests on this basis will not be entertained, and no staff member shall contact the social media administrator directly — by telephone call or message — demanding the deletion of such photographs. Any genuine concern must be raised in writing through the Principal.

Incidental appearance. Where an individual who has kept aside in accordance with this section nevertheless appears incidentally in the background of a photograph or video, the school will, where reasonably practicable, crop or obscure that individual before publication.

Individual responsibility. It is the responsibility of every staff member and student to manage their own presence at photographed events in accordance with their consent status. The social media administrator publishes event coverage in good faith, based on participation at the event, and cannot be held responsible for the appearance of individuals who placed themselves within the photography area.

17. Online Learning and Virtual Classrooms

Only school-approved platforms shall be used for online teaching. Teachers shall control meeting access, protect classroom links, supervise conduct and obtain any required recording approvals. Students must join under their authorised identity, behave respectfully, avoid unauthorised recording and report suspicious participation or interactions.

18. Digital Wellbeing

Teaching shall promote age-appropriate screen use, breaks, physical activity, healthy posture, sleep, balanced routines and student wellbeing. Students shall receive guidance on excessive gaming, harmful online comparisons, peer pressure and misinformation. Technology should support—not replace—human interaction and healthy learning habits.

19. Digital Citizenship Education

The school shall provide developmentally appropriate instruction on privacy, passwords, digital footprints, phishing, scams, cyberbullying, misinformation, copyright, respectful communication,

AI literacy and reporting unsafe experiences. At least one structured digital safety activity should be conducted per academic term, alongside assemblies and classroom reminders.

20. Safeguarding and Cyber Incident Reporting inside the school premises.

Stage 1 — Record and refer: the receiving staff member records key facts and promptly refers safeguarding concerns to the concerned person; technical events are also sent to IT.

Stage 2 — Assess: the concerned person determines immediate child-safety risk; IT assesses and contains technical threats.

Stage 3 — Protect: arrange medical, pastoral, security or emergency support as necessary.

Stage 4 — Preserve: securely retain relevant, lawfully obtained evidence with access restrictions. Do not download or circulate suspected child sexual abuse material.

Stage 5 — Escalate: inform the Principal and competent authorities whenever law or safeguarding procedures require.

Stage 6 — Follow up: document outcomes, support students and improve controls. Internal targets must never delay legally required reporting.

21. Emergency and High-Risk Incidents

Imminent threats, suspected grooming, sexual exploitation, extortion, threats of violence and similarly serious harm require immediate attention. Prioritise the child's safety, contact emergency services when necessary, inform safeguarding leadership and cooperate with authorised agencies. Staff must not conduct informal investigations that compromise evidence or promise absolute secrecy to a child reporting abuse.

22. Staff Training and Conduct

Induction and refresher training shall cover digital safeguarding, cyberbullying, exploitation warning signs, privacy, phishing, secure ERP practices, responsible AI, professional online boundaries, reporting and evidence handling. The DCPO and IT administrators shall receive role-specific training.

23. Parental Engagement

The school shall issue practical parent guidance through notices, awareness sessions and approved channels. Guidance should cover device supervision, age restrictions, parental controls, privacy settings, healthy online habits and reporting routes. Parents should be encouraged to communicate with children in a supportive and non-punitive manner about online concerns.

24. Monitoring and Compliance

Authorised monitoring may include school-device security status, network logs, ERP access and change logs, intrusion alerts and formally reported misuse. Monitoring must be necessary, proportionate, purpose-limited and privacy-respecting. This policy does not permit unrestricted surveillance or unauthorised access to private communications.

25. Breaches and Disciplinary Procedures

Responses shall consider the seriousness of behaviour, age of the learner, safeguarding needs, evidence and applicable behaviour policies. Measures may include education,

counselling, parent meetings, proportionate access restrictions, restorative measures, disciplinary action or referral to authorities. Victims must not be treated as offenders merely because they reported or were subjected to online abuse.

26. Implementation and Accountability

Management shall appoint the DCPO and deputy, publish confidential reporting routes, brief staff, students and parents, maintain incident registers, ensure training, review filtering and cybersecurity, check approved platform age suitability, review photo permissions and assess policy effectiveness. IT shall maintain technical security controls; the DCPO shall own safeguarding triage and case management.

27. Policy Review

This policy shall be reviewed at least annually, and sooner following changes to UAE law or SPEA guidance, significant safeguarding events, technology changes, audit findings or emerging threats. Amendments must be approved and logged by management.

28. School Community Commitment

Students: use technology responsibly, respect others, protect personal information and report unsafe experiences.

Staff: model professional conduct, safeguard data and respond promptly to concerns.

Parents: cooperate in age-appropriate online protection and healthy device habits.

Management: provide clear accountability, secure systems and ongoing improvement.

29. Approval and Authorisation

Prepared by: IT Department - Mrs. Sarah Basit

Reviewed by: SLTs & Principal

Approved by: SLTs & Principal

Principal's Signature: _____