



The Apple International Community School

Anti Bullying and Cyber Bullying Policy **2026-2027**

POLICY INFORMATION

Policy Written	September 2026
Policy Updated	September 2026
Policy to be Reviewed	September 2027
Approved By	Principal - Ms. Pretty Khosla



Index

Sno	Content
1	Policy Statement
2	Purpose
3	Scope
4	Definitions
5	Bullying and other behaviour
6	Forms of bullying
7	Legal and regulatory framework
8	Guiding principles
9	Prevention and education
10	Digital conduct and personal devices
11	Reporting
12	Immediate response
13	Assessment and fact finding
14	Digital evidence and device access
15	Safeguarding and external reporting
16	Support for a student who has experienced bullying
17	Response to a student alleged or found to have caused harm
18	Consequences and restorative practice
19	Bystanders retaliation and false reports
20	Inclusion and equality
21	Confidentiality records and data protection

22	Roles and responsibilities
23	Training monitoring and review
24	Related policies

1 Policy statement

The Apple International Community School (AICS) is committed to a safe, respectful and inclusive learning environment in which every child is protected from bullying and cyber bullying. Bullying is unacceptable and may constitute child-on-child abuse. Every report will be heard, recorded, assessed and addressed; no student is expected to tolerate harm or manage a serious concern alone.

This single policy governs both face-to-face and technology-assisted bullying. The same safeguarding, fairness, support and accountability principles apply whether conduct occurs on campus, on transport, during a school activity, through a device or platform, or outside school where it affects safety, wellbeing or access to education.

2 Purpose

- prevent bullying through education, supervision, inclusive practice, digital citizenship and early intervention;
- define bullying and distinguish it from conflict, accidents and one-off unkindness;
- provide accessible reporting routes for students, parents and staff;
- set one prompt, child-centred and documented response for bullying and cyber bullying;
- protect students who experience, witness or are alleged to have caused harm;
- preserve digital evidence safely and lawfully; and
- apply proportionate support and consequences under the Student Behaviour and Disciplinary Policy.

3 Scope

This policy applies to students, staff, volunteers, visitors and contractors on school premises, school transport, educational visits, residential activities, sports events, remote learning and all school-organised or school-representative activities. It also applies to off-site and online conduct where there is a clear connection to a student's safety, wellbeing, learning, staff welfare, school systems or the orderly operation of AICS.

4 Definitions

Term	Meaning
Bullying	A deliberate pattern of behaviour, usually repeated over time, involving a real or perceived power imbalance and causing or intending physical, emotional, social or psychological harm.
Cyber bullying	Bullying through digital technology, including messaging, social media, gaming, email, images, recordings, voice, group chats, impersonation or coordinated online activity. A single upload or post may be treated as bullying when it can be repeatedly viewed, copied or shared.
Child-on-child abuse	Abuse by one or more children against another child, including bullying, discriminatory abuse, violence, sexual harassment, harmful sexual behaviour, exploitation, coercion or online abuse.
Power imbalance	A difference in power arising from age, size, status, popularity, group numbers, information, disability, language, vulnerability, access to technology or control of images/accounts.
Discriminatory bullying	Bullying connected to disability, nationality, ethnicity, language, religion, sex, appearance, family circumstances or another personal characteristic.
Bystander or upstander	A bystander sees, hears or knows about bullying. An upstander reports safely, refuses to participate and supports the affected student without taking unsafe action.
Retaliation	Threatening, punishing, excluding or targeting a person for reporting, supporting a report or participating in a review.
Harmful digital content	Content that is abusive, threatening, discriminatory, sexual, exploitative, manipulated, privacy-invading, self-harm related or otherwise unsafe for a child.

5 Bullying and other behaviour

Situation	School interpretation and response
Bullying	A pattern involving harm and power imbalance, or a high-impact digital act with continuing reach. Apply this policy and assess safeguarding risk.
Conflict	A disagreement between students of relatively equal power who can express their views and seek resolution. Provide support and monitor; escalate if harm or imbalance emerges.
One-off unkindness	Address promptly under the behaviour policy. Record and monitor because repetition, targeting, digital persistence or wider impact may establish bullying.
Accident	Unintended harm without reckless or targeted conduct. Provide care, repair harm and review supervision where necessary.
Banter or joking	Not a defence when conduct humiliates, frightens, targets a characteristic, continues after objection or causes foreseeable harm.

6 Forms of bullying

- Physical: hitting, kicking, pushing, spitting, damaging or taking property, blocking movement or intimidation.
- Verbal: insults, threats, humiliating comments, name-calling, sexualised comments, mocking language or repeated teasing.
- Social or relational: deliberate exclusion, rumours, coercing friendships, public humiliation, manipulating groups or encouraging others to isolate a child.
- Discriminatory: targeting disability, language, nationality, religion, culture, sex, appearance, family circumstances or perceived difference.
- Material or coercive: demanding money or property, forcing acts, exploiting vulnerability, blackmail or threats of disclosure.
- Sexual harassment or harmful sexual behaviour: sexualised comments,

images, gestures, pressure or contact. These require immediate safeguarding assessment.

- Cyber bullying: harmful messages or posts, fake accounts, impersonation, doxxing, group-chat exclusion, pile-ons, gaming abuse, harmful polls, non-consensual recordings or images, account misuse, threats, manipulated media or deepfakes.

7 Legal and regulatory framework

This policy is implemented in accordance with the current versions of:

- Federal Law No. 3 of 2016 on Child Rights (Wadeema's Law), as amended, and Cabinet Resolution No. 52 of 2018 concerning its Executive Regulations;
- the UAE National Child Protection Policy in Educational Institutions and applicable mandatory reporting requirements;
- Federal Decree-Law No. 34 of 2021 on Countering Rumours and Cybercrimes, as amended;
- Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data;
- applicable UAE criminal, anti-discrimination, disability, media and telecommunications legislation; and
- current KHDA and Ministry of Education requirements for safeguarding, wellbeing, inclusion, student conduct, suspension and exclusion in Dubai private schools.

Where a legal or regulator requirement changes, the current requirement prevails and this policy will be updated at the earliest review. School staff do not determine criminal liability.

8 Guiding principles

Principle	Required approach
Safety and best interests	Protect the child first and escalate medical, safeguarding or emergency risks without waiting for a disciplinary decision.
No minimisation	Do not dismiss conduct as joking, banter, a private matter or an online issue when harm is reported or foreseeable.
Fairness	Hear children separately, avoid leading questions, consider evidence and record the basis for findings.

Principle	Required approach
No forced confrontation	Do not require a child to face another student, mediate or apologise where safety, consent or power imbalance is unresolved.
Need-to-know confidentiality	Share only what is necessary to protect children, comply with law or manage the response.
Proportionate response	Consider seriousness, impact, repetition, intent, age, evidence, vulnerability and individual need.

9 Prevention and education

- Teach respectful relationships, consent, empathy, conflict resolution, digital citizenship, privacy, safe bystander action and help-seeking through age-appropriate curriculum and assemblies.
- Challenge prejudicial language, humiliation and harmful banter consistently.
- Use active supervision and review hotspots, transition times, transport, toilets, corridors, play areas and online learning spaces.
- Build student voice through surveys, trusted-adult routes, student ambassadors and confidential reporting options.
- Teach students not to like, forward, save or participate in harmful content and how to block, mute and report safely.
- Provide annual staff training and parent awareness on warning signs, reporting, device supervision and digital evidence preservation.
- Use reasonable adjustments and targeted safety plans for vulnerable students, including Students of Determination and students with communication needs.

10 Digital conduct and personal devices

- Student phones and personal devices must remain switched off and securely stored during the school day unless staff authorise a defined educational, accessibility, medical or emergency use.
- No person may photograph, film or record another person during school or a school activity without staff authorisation and appropriate consent.
- Students must not create fake or unofficial accounts that impersonate AICS, staff or another student.

- Users must not publish personal data, location information, confidential school information, defamatory allegations, threats or content identifying a safeguarding case.
- School communication with students uses approved platforms; staff must not use personal social-media accounts or private messaging for one-to-one student communication.
- Off-site online conduct may be addressed when it creates a safeguarding concern or material impact on school wellbeing, learning or operations.

11 Reporting

A student may report to any trusted adult, teacher, counsellor, Head of Section, Head of Inclusion, clinic staff, Anti-Bullying Champion, Principal or Child Protection Officer/Designated Child Protection Lead (CPO/DCPL). A student may ask a friend or parent to help. Anonymous information will be assessed, although it may limit the action available.

Staff must make an immediate verbal alert to the CPO/DCPL where there is a safety or safeguarding concern and complete the approved online incident/reporting form before the end of the working day.

Email or messaging may alert a colleague but must not be the sole or final record.

Parents should report concerns to the class teacher, Head of Section, counsellor or CPO/DCPL and should not confront another child or family. Reports will be acknowledged and next steps explained, subject to confidentiality and safeguarding restrictions.

12 Immediate response

1. Stop the behaviour if safe, separate students appropriately and address urgent medical or emotional needs.
2. Listen calmly; record the child's exact words; do not promise secrecy or ask leading questions.
3. Notify the CPO/DCPL immediately where there is abuse, serious harm, sexual behaviour, threats, extortion, discrimination, self-harm, exploitation, grooming or significant online risk.
4. Preserve relevant evidence without forwarding harmful content unnecessarily.
5. Decide interim safety arrangements, including supervision, transport, timetable, online-contact restrictions, device/account controls and a

named trusted adult.

6. Contact parents promptly when safe and lawful. The CPO/DCPL may delay or adapt contact if it could increase risk or conflict with competent-authority direction.

13 Assessment and fact finding

The school will assess each concern promptly, fairly and separately.

Children are not required to confront one another or attend a joint meeting.

The assessment considers:

- what happened, where, when, how often and on which platform;
- impact, intent, reach and whether the harm was foreseeable;
- the power relationship, including age, status, popularity, group size, disability, language, information or control of digital content;
- witness accounts and available physical or digital evidence;
- previous concerns, wider group involvement and possible retaliation;
- safeguarding indicators, including coercion, grooming, exploitation, self-harm or sexual harm; and
- each child's age, development, communication needs and reasonable adjustments.

A report is not dismissed because accounts differ, there is no eyewitness, the incident occurred online or outside school, or the affected child delayed reporting. The school distinguishes confirmed, unsubstantiated and deliberately false reports. An unsubstantiated report is not automatically a false report.

14 Digital evidence and device access

- Record the account name, date, time, platform, URL and context; capture only the minimum necessary screenshot or export.
- Do not edit, annotate or repeatedly forward evidence. Store it only in the approved restricted system.
- Do not ask multiple staff or students to view distressing material.
- For suspected sexual images of a child, do not copy, print, email or upload the content; notify the CPO/DCPL immediately and follow authority instructions.
- Students should not be instructed to retain illegal or sexual imagery on a personal device.

AICS may monitor school-owned or school-managed devices, accounts,

applications and networks for safeguarding, security and compliance purposes. Monitoring must be authorised, proportionate and limited to a defined purpose.

The school does not claim unrestricted access to privately owned devices or personal communications. Content is examined only with valid consent, parent involvement where appropriate, contractual authority, a lawful and proportionate school process, or competent-authority direction. Staff must not demand a student's personal account password or conduct an intimate search or criminal investigation.

15 Safeguarding and external reporting

Immediate safeguarding escalation is required for significant harm, violence, sexual harassment or harmful sexual behaviour, extortion, credible threats, discriminatory abuse, exploitation, grooming, coercive control, self-harm or suicide risk, live-streamed abuse, serious privacy violation, repeated failure of protective measures or inappropriate adult/unknown-person contact.

In immediate danger or medical emergency, call 999. The CPO/DCPL follows the Child Protection and Safeguarding Policy and coordinates referrals to Child Protection, Dubai Police, emergency services, a health authority or another competent body as required. School fact-finding must not delay care or interfere with a statutory investigation.

16 Support for a student who has experienced bullying

- Reassure the student that reporting was right and that they are not responsible for the harm.
- Agree a written safety and support plan with a named adult and review date.
- Offer counselling, clinic, inclusion or licensed external support where appropriate.
- Restore safe access to learning, friendships, activities, transport and digital spaces without placing the burden on the affected student.
- Support safe blocking, platform reporting, account recovery and content-removal requests where appropriate.
- Monitor retaliation, attendance, engagement and wellbeing; update parents within confidentiality limits.

17 Response to a student alleged or found to have caused harm

- Explain the concern and provide an age-appropriate opportunity to respond.
- Maintain appropriate supervision and protect the student from retaliation or public labelling.
- Assess unmet needs, peer dynamics, exposure to harm, additional needs and whether the student may also be at risk.
- Use behaviour teaching, counselling, digital citizenship work, a Behaviour Management and Intervention Plan, family work or specialist referral as indicated.
- Set clear boundaries, consequences, repair actions, account/device controls and monitoring dates.
- Record progress and escalate the response where harmful behaviour continues.

18 Consequences and restorative practice

Consequences are determined under the Student Behaviour and Disciplinary Policy and current KHDA/MoE requirements. They are proportionate to seriousness, repetition, impact, reach, intent, risk, age, evidence and individual need. Options may include education, loss of a specific privilege, restricted technology access, increased supervision, behaviour targets, restorative action, formal warning, detention or another approved consequence.

Suspension or exclusion is not automatic. Any such decision must be evidence-based, procedurally fair and compliant with current KHDA/MoE authorisation, notification, documentation and appeal requirements.

Restorative meetings, apologies or a support-group/no-blame approach may be used only after safeguarding assessment, with informed agreement and where safe. They do not replace fact-finding, consequences, evidence preservation, risk management or mandatory reporting.

19 Bystanders retaliation and false reports

Students are taught to report safely, seek adult help, avoid liking or forwarding harmful content and support the affected student without placing themselves at risk. Retaliation against a reporter, witness or supporter is a separate serious concern. Deliberately fabricated allegations

may be addressed under the behaviour policy, but a report that cannot be substantiated is not treated as malicious without evidence of deliberate fabrication.

20 Inclusion and equality

Students of Determination, students with communication differences, EAL learners and other vulnerable students may face increased risk or difficulty reporting. AICS will provide accessible reporting formats, communication support, reasonable adjustments and tailored safety planning. Additional need does not excuse harmful behaviour, but it must inform assessment, teaching, support and consequence decisions.

21 Confidentiality records and data protection

- Maintain factual, dated, timed and signed records in the approved safeguarding/incident system.
- Restrict access to those who need information to protect children, comply with law or manage the response.
- Do not promise a parent full details of action taken against another child.
- Store digital evidence only in approved restricted systems and do not retain it on personal devices.
- Retain and dispose of records under the school's retention schedule, UAE data-protection law and regulator requirements.
- Monitor anonymised patterns by location, time, platform, type, group and student vulnerability.

22 Roles and responsibilities

Role	Responsibilities
Governing Body	Approve and oversee the policy; assure training, resources, lawful systems, compliance and annual review.
Principal	Overall accountability; ensure fair procedures, protective action and approved disciplinary/regulatory action.
CPO/DCPL and safeguarding team	Lead risk assessment, referrals, evidence safeguards, parent-contact decisions, safety plans and multi-agency follow-up.
Anti-Bullying Champion / Counsellor	Coordinate prevention, student voice, support, monitoring and staff/parent awareness; refer safeguarding concerns immediately.
IT and Data Protection leads	Support authorised evidence preservation, account/system controls, incident containment and secure storage.
Heads of Section and teachers	Supervise, respond, record using the approved form, implement safety plans and monitor classrooms, transitions and online learning.
Inclusion team	Identify vulnerability, provide reasonable adjustments and contribute to support and behaviour planning.
Students	Treat others respectfully, report concerns, protect privacy and accounts, preserve evidence safely and do not retaliate or forward harmful content.
Parents	Report promptly, supervise age-appropriate digital use, preserve evidence, avoid confrontation and cooperate with support and review plans.

23 Training monitoring and review

All staff receive induction and annual refresher training on recognition, immediate response, child-on-child abuse, cyber bullying, digital evidence, the approved reporting form and safeguarding escalation. Students receive

age-appropriate education and parents receive awareness guidance. Senior leaders and the safeguarding team review anonymised trends at least termly. The Governing Body receives an annual assurance report. This policy is reviewed annually, after a serious incident or sooner when law, KHDA/MoE direction, technology or school risk changes.

24 Related policies

Child Protection and Safeguarding Policy; Student Behaviour and Disciplinary Policy; Inclusion Policy; Staff Code of Conduct; Mobile Device Procedure; Photography and Media Consent Procedure; and Educational Visits and Transport procedures.

Appendix A Bullying and cyber bullying response record

Complete the approved online incident form. Use this checklist to ensure the safeguarding record is complete.

Student(s) affected / year / class	
Person(s) alleged to have caused harm	
Reporter / date / time / location or platform	
Exact words and observed facts	
Type frequency impact reach and power imbalance	
Witnesses and evidence preserved	
Immediate medical or emotional action	
CPO/DCPL notified date and time	
IT or Data Protection lead notified if applicable	
Safeguarding risks and referral decision	
Parent contact decision and rationale	
Interim safety and digital account arrangements	
Finding and evidence basis	

Support consequence or restorative action	
Review dates and outcome	
Completed and reviewed by date	

Appendix B Cyber bullying evidence quick guide

Do	Do not
Record the username, platform, date, time, URL and context.	Do not reply, retaliate, like or forward harmful content.
Take one limited screenshot where safe and lawful.	Do not ask several people to view or copy distressing material.
Block or mute where safe and use platform reporting with adult support.	Do not delete accounts or reset devices before advice if serious evidence may be lost.
Tell a trusted adult and submit the approved incident report.	Do not keep suspected sexual or illegal images of a child; notify the CPO/DCPL immediately.
In immediate danger or medical emergency call 999.	Do not confront an alleged offender or arrange an in-person meeting.