Policy For Online Bullying & Cyberbullying

Reviewed in April 2026

Next review April 2027

Reviewed by Principal, Slt's

ONLINE BULLYING AND



(Companion to the E-Safety, Online Protection and Digital Safeguarding Policy)

Prepared by	IT Department: Mrs. Sarah Basit
Status	Session 2026-2027
Document date	11 November 2026

1. Policy Statement

Al Amaal English High School is committed to a safe, respectful and inclusive learning environment, online as well as offline. Online bullying and cyberbullying cause real harm to children — to their safety, their learning, their health and their dignity — even when the messages are sent from outside the school gates.

The school will not tolerate online bullying in any form. Every report will be taken seriously, handled fairly and confidentially, and dealt with proportionately, with the best interests of the child as a primary consideration. A student who reports online bullying will never be treated as an offender merely because they reported it or were subjected to it.

2. Purpose and Objectives

This policy aims to:

- define online bullying clearly, so that students, staff and parents recognise it when it happens;
- prevent online bullying through education, clear rules and a culture of respect;
- give every member of the school community a simple, safe way to report it;
- set out exactly what the school will do when a report is made — and what it cannot do;
- support the student who has been targeted, and work constructively with the student responsible;
- protect evidence, keep proper records, and involve parents and, where required, the competent authorities;
- keep the school within UAE law and Sharjah Private Education Authority (SPEA) requirements.

3. Scope and Applicability

This policy applies to:

- all students from Kindergarten to Grade 12;
- all teachers, administrative, technical, support and contracted staff;
- school leadership, parents and guardians, in so far as their conduct affects a student;
- conduct on school devices, school networks, school email, the school ERP, learning platforms, official class and school groups, and official school social-media accounts;

- conduct on personal devices and personal accounts where it affects school life, a student's safety, or the school community — within the jurisdiction limits set out in Section 5.

Online bullying is not limited to school hours. A message sent at night or at the weekend can still harm a child at school the next morning, and this policy deals with that harm where the school has jurisdiction to act.

4. Definitions

4.1 What online bullying (cyberbullying) is

Online bullying is the use of digital technology — including messaging apps, social media, gaming platforms, email, photos, video and AI tools — to deliberately and repeatedly harm, humiliate, frighten, exclude or control another person. It includes:

- **Harassment.** Repeated hostile, threatening or abusive messages, comments or calls.
- **Humiliation.** Posting or sharing embarrassing, insulting or false material about a person, including edited photos, videos, memes or rumours.
- **Harmful impersonation.** Pretending to be another person online to damage their reputation or relationships, including fake accounts in a student's name.
- **Exclusion.** Deliberately and repeatedly excluding a student from online groups, chats or games in order to isolate or humiliate them.
- **Outing and doxxing.** Sharing someone's private information — such as a phone number, address, photographs or personal secrets — without their permission.
- **Discriminatory abuse.** Abuse targeting a person's nationality, religion, language, appearance, disability, gender or family background.
- **Sexting-related harm.** Pressuring a student to send intimate images, or sharing intimate or sexual images of a child — this is a serious safeguarding matter (see Section 14).
- **AI-generated harm.** Using AI tools to create fake images, videos or voices of a person in order to mock, shame or threaten them ("deepfakes").
- **Group pile-ons.** Several students joining together against one student in a group chat, comment thread or game.
- **Recording harm.** Filming a fight, an assault or a humiliating incident and sharing the recording to mock the person involved.

4.2 A single serious event

Online bullying is often repeated, but repetition is not required. A single serious event — for example, sharing a private or manipulated image, a serious threat, or a harmful impersonation — may warrant urgent safeguarding action on its own.

4.3 What is not online bullying

Not every unkind message or online disagreement is bullying. A one-off falling-out between friends, a single rude comment that is not repeated, or a difference of opinion is not, by itself, online bullying — but it may still need a teacher's attention, and it must be reported if it continues or escalates. Staff will judge each case on its facts, not on labels.

4.4 Bullying and the school's photograph rules

Photographs and videos taken at school events are governed by Section 16 of the E-Safety Policy (Event Photography, Consent and Individual Responsibility). A photograph that was taken and published with consent under that section is not bullying. But using any photograph — consented or not — to mock, shame, threaten or exclude a student is online bullying, and is dealt with under this policy, not under the photograph rules.

5. Jurisdiction and Limits of School Responsibility

This section mirrors Section 4 of the E-Safety Policy. It defines the boundaries of the school's authority and responsibility, and it applies to students, staff and parents alike.

5.1 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.

5.2 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.

5.3 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.

5.4 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.

5.5 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.

5.6 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.

6. 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.

Under Article 44 of Federal Decree-Law No. 34 of 2021, taking photographs of third parties in any public or private place, or copying, keeping or publishing them using information systems, without the person's consent, is a criminal offence punishable by imprisonment of at least six months and/or a fine of AED 150,000 to AED 500,000. Online bullying that involves threats, defamation, extortion, unauthorised access, or the sharing of private or intimate images may also constitute a criminal offence under the same law. The school will refer suspected offences to the competent authorities where required.

7. Roles and Responsibilities

Each person does the part only they can do. Nothing in this policy asks anyone to do work they are not positioned to do.

Role	Responsibility
Principal / Management	Approve this policy; give the final decision in any dispute or se ious c ensure the Designated Child Protection Officer (DCPO), the dis cipline committee and the IT Department have the support and reso rces t ensure parents are informed where required.
Designated Child Protection Officer (DCPO) and deputy	Receive and triage safeguarding reports; prioritise student wel fare; r confidential safeguarding records; coordinate lawful parent an d auth notifications; organise support for the students involved; own safegu triage and case management.

Discipline Committee	Assess immediate safety, arrange support, preserve evidence safely, parents when appropriate, and coordinate fair investigation and proportionate action in cases within the school's jurisdiction.
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 or decide discipline. The IT / Social Media Admin cannot identify students or staff by face and therefore cannot verify identities in photos — identification of individuals in images sits with the class teacher, head of charge or DCPO.
Teachers and staff	Supervise technology use; model respectful online conduct; watch for warning signs; take every report seriously; record key facts and refer promptly to the DCPO; never promise a child absolute secrecy; never conduct an informal investigation that could compromise evidence.
Students	Treat others with respect online; protect passwords and personal information; do not forward, share or comment on bullying material; report online concerns to a trusted adult — reporting is an act of courage, not of telling tales; support a classmate who is being targeted by not joining in.
Parents / guardians	Supervise children's personal devices and accounts at home; apply age-appropriate controls; talk with children about online life in a supportive, non-punitive way; report concerns to the school through the proper routes; cooperate with safeguarding and disciplinary procedures; preserve evidence at home as set out in Annex B.

8. Prevention and Education

- **Digital citizenship lessons.** Developmentally appropriate instruction on privacy, passwords, digital footprints, respectful communication, cyberbullying, misinformation, AI literacy and reporting unsafe experiences — at least one structured digital safety activity per academic term, alongside assemblies and classroom reminders.
- **Age-appropriate rules.** Class rules on device use, group chats and online behaviour, explained to students in language they understand, and repeated at the start of each term.
- **Staff training.** Induction and refresher training for all staff covering digital safeguarding, cyberbullying and exploitation warning signs, privacy, professional online boundaries, reporting and evidence handling. The DCPO and IT administrators receive role-specific training.
- **Parent guidance.** Practical parent guidance through notices, awareness sessions and approved channels — covering device supervision, age restrictions, parental controls, privacy settings, healthy online habits and reporting routes (see Annex C).
- **Positive culture.** The school promotes kindness, inclusion and respect online as well as offline, and recognises students who stand up for others.

9. Reporting Online Bullying

Any student, parent, or staff member may report online bullying. A report may be made to any trusted staff member, to the class teacher, to the DCPO, or to the Principal. Parents may report in writing to the school office. Reports may also be made using the form in Annex A.

- **What to include.** Who is involved, what happened, when it happened, where it happened (which app, group or platform), and any evidence — see Annex B.
- **Anonymous reports.** A report may be made without giving a name. The school will act on it as far as it can, but anonymous reports are harder to investigate, and the school may not be able to give feedback on the outcome.
- **No retaliation.** Retaliation against any person for making a good-faith report, or for cooperating with an investigation, is prohibited and will itself be dealt with as a disciplinary matter.
- **Confidentiality.** Reports are handled confidentially and shared only with those who need to know in order to protect the child and deal with the case. A student who reports will be told who will be informed and why.
- **No promise of secrecy.** Staff must not promise a child absolute secrecy. If a child is at risk, the member of staff must share the information with the DCPO.
- **Staff duty.** Any member of staff who receives a report, or who sees signs of online bullying, must record the key facts and refer promptly to the DCPO the same day. A report must never be left unrecorded.
- **Out of jurisdiction.** If the report concerns conduct outside the school's jurisdiction (Section 5.2), the school will explain this to the reporter, give the safeguarding advice that applies, and — where a criminal offence or a threat to safety may be involved — direct the family to the competent authorities.

10. Responding to a Report — Procedure

When a report is received, the school will follow these stages. The DCPO leads safeguarding cases; the Discipline Committee leads disciplinary cases within the school's jurisdiction. Both work together where a case involves both.

Stage 1 — Record and refer (same day)

The receiving staff member records the key facts (who, what, when, where, evidence) and promptly refers safeguarding concerns to the DCPO. Technical matters are also sent to IT. The report is entered in the confidential incident register.

Stage 2 — Assess (same day)

The DCPO determines the immediate child-safety risk: is the child safe now, is the bullying continuing, and does anything need to happen immediately (for example, separating students, contacting parents, or removing harmful content from a school platform)? IT assesses and contains any technical threat on school systems.

Stage 3 — Protect

Arrange medical, pastoral, security or emergency support as necessary. Where the bullying is happening on an official school group or platform, the harmful content is removed and the

offending account's access is restricted while the case is dealt with. The targeted student is given a named adult to go to.

Stage 4 — Preserve evidence

Securely retain relevant, lawfully obtained evidence with access restrictions — see Annex B. Screenshots must show the content, the sender, the date and time, and the platform. Do not download, forward or circulate suspected intimate or sexual images of a child; report them immediately to the DCPO.

Stage 5 — Investigate fairly

The investigation is normally completed within five school days of the report. Both sides are heard separately; witnesses are spoken to; parents of the students involved are informed where appropriate. The student responsible is told what is alleged and given a fair chance to respond. No finding is made on the basis of a screenshot alone without checking its context.

Stage 6 — Decide and act

The DCPO and the Discipline Committee decide, on the facts, whether online bullying took place, how serious it is, and what action follows (Sections 11–13). Parents are informed of the outcome as far as confidentiality allows. The decision and the reasons are recorded.

Stage 7 — Follow up and review

The DCPO checks in with the targeted student after one week and again after one month, to confirm the bullying has stopped. Outcomes are documented, support is adjusted if needed, and lessons are folded into the next policy review. Internal targets must never delay legally required reporting.

Imminent threats, suspected grooming, sexual exploitation, extortion, threats of violence and similarly serious harm require immediate attention under Section 21 of the E-Safety Policy: prioritise the child's safety, contact emergency services when necessary, inform safeguarding leadership and cooperate with authorised agencies.

11. Support for the Student Who Has Been Targeted

- The student is believed, listened to, and told what will happen next.
- A named trusted adult is assigned, and the student is told how to reach them quickly.
- A safety plan is agreed with the student (and their parents): what to do if it happens again, who to tell, and how to block or report on the platform.
- Pastoral or counselling support is offered; where the school cannot provide it, the family is signposted to appropriate services.
- The student's routine at school is protected — they are not moved, excluded or disadvantaged because they reported.
- Check-ins after one week and one month confirm the bullying has stopped; if it has not, the case is reopened and escalated.
- The student is never blamed for the bullying, and is never punished for reporting it or for being targeted.

12. Working with the Student Responsible

- The student is told clearly what behaviour must stop and why it is harmful.
- Where appropriate, a restorative conversation is held — the student hears the impact of their actions and agrees how to make it right (for example, a genuine apology and deleting the harmful content).
- Parents are involved from the start, and a behaviour plan may be agreed, with clear expectations and a review date.
- The student is offered support to understand their behaviour — including, where relevant, counselling or guidance on empathy, anger and online conduct.
- The focus is on stopping the behaviour and preventing a repeat, not only on punishment. But where the behaviour continues, sanctions under Section 13 apply.

13. Sanctions and Disciplinary Measures

Sanctions are proportionate, and consider the seriousness of the behaviour, the age of the learner, safeguarding needs, the evidence, and the school's behaviour policy. The same act may attract a different response for a KG student and for a Grade 12 student.

Level	**Response**
Minor / first incident	Education and warning; restorative conversation; apology and removal of the harmful content; parents informed; record kept.
Repeated or more serious	Parent meeting; written warning; behaviour plan with review date; temporary restriction of access to school devices, school Wi-Fi or official school groups; loss of privileges as set out in the behaviour policy.
Serious or persistent	Suspension in accordance with the school behaviour policy and SPEA rules; referral of the case to the Principal; where a criminal offence may be involved, referral to the competent authorities (police / cybercrime reporting channels).
Severe (threats, extortion, intimate images, hate-based abuse)	Immediate safeguarding escalation; suspension pending investigation where the behaviour policy allows; mandatory referral to the competent authorities; the school will cooperate fully with any police investigation.

Sanctions are never applied to the targeted student for having reported, or for having been the victim of online bullying. Where both students have behaved badly, each case is judged on its own facts.

14. Online Bullying Involving Images, Video and AI

- Photographs of a student used to mock, shame or threaten them are online bullying, even if the photograph itself was taken with consent (see Section 4.4).
- Suspected intimate, sexual or exploitative images involving a child require immediate safeguarding escalation to the DCPO. Staff and students must not download, forward, share or circulate such material — doing so may itself be a criminal offence.

- AI-generated fake images, videos or voices of a person (deepfakes) used to mock, shame or threaten them are treated as a serious form of online bullying, and may be referred to the competent authorities.
- Where harmful content appears on an official school account or group, the IT Department will remove it and preserve a copy as evidence. Where it appears on a personal account outside the school's jurisdiction, the school will advise the family on reporting it to the platform and to the competent authorities.
- Requests to delete photographs published under Section 16 of the E-Safety Policy are dealt with under that section (in writing through the Principal). A deletion request does not stop a bullying investigation.

15. Online Bullying of Staff

Staff can also be targets of online bullying — by students, by parents, or by other staff. The same reporting routes apply: a staff member may report to the Principal, the DCPO, or their line manager. The school will take the report seriously, support the staff member, and deal with the case under this policy and the staff conduct procedures. No member of staff will be asked to investigate a case in which they are themselves the target.

16. Parents and Guardians

- The school will inform parents promptly where their child is involved in a case within the school's jurisdiction — as the targeted student or as the student responsible — and will tell them what action is being taken, as far as confidentiality allows.
- Where the matter is outside the school's jurisdiction, the school will explain why it cannot investigate, give practical advice (Annex C), and direct the family to the competent authorities where a criminal offence or a threat to safety may be involved.
- Parents are asked not to confront another child or another family directly, and not to post about the incident on social media while a case is being dealt with — this can prejudice an investigation and can itself amount to online harassment.
- Parents who disagree with a decision may raise it in writing with the Principal.

17. Record-Keeping, Monitoring and Review

- Every report, investigation, decision and follow-up is recorded in the confidential incident register, held by the DCPO. Access is restricted to those who need it for safeguarding or disciplinary purposes.
- Records are kept in accordance with the school's data protection and retention rules, and are never shared outside the school except where the law requires it or where it is necessary to protect a child.
- The DCPO reports the number and nature of incidents (without names) to the Principal each term, so that patterns — for example, a particular platform, year group or time of day — can be addressed.

- 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.

18. Approval and Authorisation

Prepared by	Mrs. Sarah Basit — date: 11 November 2026
Reviewed by	Health & Safety In-charge Mrs. Kar
Approved by	Principal:

Prepared by: _Mrs. Sarah Basit IT Administrator_____

Reviewed by: _Vice Principal Mr. Qaid-ur-Rehman_____

Principal's Name: ___Mr. Bakht Biland_____

Principal Signature: _____

ANNEX A — ONLINE BULLYING REPORT FORM

Complete as much as you can. This form can also be submitted online at https://alamaalschool.com/page/cyber-complaint (the same form is available on our school website)
Or sent by email to the school social worker, Ms Maryam ***(maryamhammadi@alamaalschool.com),*** *or to the school at* ***studentsupport@alamaalschool.com****. A paper copy may be given to any trusted staff member, the class teacher, the DCPO, or the school office. A student may ask a trusted adult to help fill it in.*

Name of student reporting (leave blank for an anonymous report):

_____

Class / Grade: _____ Date of report: _____

Name of the student(s) being targeted (if different from above):

_____

Name(s) of the student(s) believed responsible (if known):

_____

What happened? (describe in your own words):

_____

_____

_____

When did it happen? (date(s) and time(s)):

_____

Where did it happen? (which app, website, game, group or platform):

_____

Is it still happening? Yes / No Has it happened before? Yes / No

Evidence attached (screenshots, links, messages): Yes / No — describe:

_____

Have you told anyone else? (parent, teacher, friend):

_____

What would help you feel safe now?

_____

Received by (staff name): _____ Date: _____ Referred to DCPO: Yes / No

ANNEX B — EVIDENCE PRESERVATION CHECKLIST

Good evidence is what turns a report into a case that can be acted on. Follow these steps as soon as you see the bullying:

- **Screenshot everything.** Capture the full message, post or image — including the sender's name or username, the date and time, and the name of the app or platform. On a phone, include the status bar so the time is visible.
- **Save the original.** Do not edit, crop or alter the screenshot. Keep the original message in the app where possible; do not delete the conversation.
- **Save links and usernames.** Note the exact link (URL) to a post or profile, and the username of every account involved.

- **Do not reply in anger.** Do not answer the bully, and do not forward the material to others — forwarding can spread the harm and can damage the evidence.
- **Do not delete.** Do not delete messages, posts or accounts involved until the school or the authorities have said it is safe to do so.
- **Block and report on the platform.** After saving the evidence, use the platform's own block and report functions.
- **Intimate or sexual images of a child.** Do NOT download, screenshot, forward or share them. Report immediately to the DCPO or the police.
- **Hand it over.** Give the evidence to the DCPO or the staff member handling the report, and keep a copy for yourself.

ANNEX C — PARENT GUIDE: IF YOUR CHILD IS BULLIED ONLINE

A short guide for parents and guardians. The school can share this as a notice or in a parent session.

- **Stay calm and listen.** Thank your child for telling you. Do not blame them, and do not take their device away as a punishment — that stops them telling you next time.
- **Save the evidence.** Follow Annex B: screenshot everything with names, dates and times, and do not delete anything.
- **Report it.** Tell the school through the class teacher, the DCPO or the school office (Annex A), and report the account or content to the platform. If the content involves threats, extortion, or intimate images, report it to the police or the cybercrime reporting channels as well.
- **Block, don't engage.** Help your child block the account and stop replying. Do not contact the other child or their family directly, and do not post about it on social media.
- **Support your child.** Keep their routine normal, watch for changes in mood, sleep or appetite, and ask the school about pastoral or counselling support if you are worried.
- **Check the settings.** Review privacy settings together, turn off location sharing, and check who can message or follow your child. Agree age-appropriate rules for devices and apps.
- **Know the school's limits.** The school can act where the bullying happens at school or on official school channels. Where it happens wholly outside school on personal accounts, the school cannot investigate — but it will still advise you, and it will always act on a safeguarding concern involving a child.