

SOCIAL MEDIA DEFAMATION POLICY

POLICY FOR	SOCIAL MEDIA DEFAMATION POLICY
PERSON RESPONSIBLE	Head of Pastoral / Digital Leader / IT Department
REVIEW DATE	October 2026
REVIEWED BY	Assistant Principals and Head of School
APPROVED DATE	October 2026
APPROVED BY	Executive Principal
DATE OF NEXT REVIEW	May 2027
RELATED POLICIES	E-Safety Policy, Anti-Bullying Policy, Child Protection and Safeguarding Policy, Staff Code of Conduct, Student Behaviour Policy, Acceptable Use Policy, BYOD Policy





Executive Principal / CEO
 & Brand Ambassador for GEMS Westminster Schools

Introduction

The Westminster School, Dubai is committed to maintaining a safe, respectful and inclusive learning environment. This policy provides guidance on responsible social media use and addresses defamation, cyberbullying, harassment and misuse of digital platforms.

Purpose

To promote responsible online communication, protect individuals and the school community from reputational harm, establish reporting procedures and support digital citizenship. The Westminster School, Dubai, is committed to maintaining a safe, respectful, inclusive and professionally responsible school community. Social media and digital communication platforms provide valuable opportunities for learning, collaboration and communication. However, misuse can damage reputations, affect wellbeing, undermine professional relationships and compromise the school's reputation.

This policy establishes expectations for responsible social media use and for preventing, identifying and addressing online conduct that may constitute defamation, cyberbullying, harassment, impersonation or unauthorised sharing of information. The policy aims to protect dignity, reputation, privacy and wellbeing; promote respectful online communication; prevent malicious or misleading content; establish clear reporting and response procedures; encourage concerns to be raised through appropriate channels; and promote awareness of legal, professional and safeguarding responsibilities.

Definitions

Social media: Digital platforms and services through which users create, publish, share or exchange information, images, videos, opinions or messages.

Defamation: Communication that may unlawfully harm an identifiable person's or organisation's reputation. Whether a statement constitutes defamation must be assessed in accordance with applicable law.

Slander and libel: Traditional legal terms generally associated with defamatory spoken statements and defamatory statements in permanent or published form. The applicable classification depends on UAE law.

Cyberbullying: Online behaviour intended to intimidate, humiliate, threaten, harass or harm another person, often through repeated or targeted conduct.

Misinformation: False or inaccurate information, whether shared intentionally or unintentionally.

Digital evidence: Relevant screenshots, URLs, messages, timestamps, account details, recordings or other electronic records that may help assess a reported incident.

Official school account: An account or digital communication channel formally authorised to represent GEMS The Westminster School, Dubai.

SCOPE

This policy applies to students from Foundation Stage to Year 13; teaching and non-teaching staff; school leaders; parents and legal guardians; volunteers, contractors, visitors; and individuals managing school-authorized accounts.

It covers public and private social media platforms, messaging applications, online forums, blogs, websites, digital communities, video-sharing platforms and other electronic communication services. It also covers content created, shared, reposted, forwarded, commented on, recorded or generated using digital tools, including artificial intelligence (AI).

The policy applies to school-related online conduct on or off school premises and during or outside school hours where there is a reasonable connection to the school community, student safeguarding, professional responsibilities or school operations. Actions will be proportionate and consistent with applicable laws, safeguarding requirements and GEMS policies.

POLICY STATEMENT

The school expects all members of its community to communicate online respectfully, responsibly and lawfully. No individual may use a digital platform to target, threaten, harass, humiliate, impersonate or unlawfully damage the reputation of a student, parent, staff member, school leader or the school itself.

Reports will be taken seriously and addressed according to the nature, severity and circumstances of the incident. The school recognises that legitimate concerns, constructive criticism, safeguarding disclosures and good-faith complaints must not be confused with defamation. Members of the community may raise genuine concerns through appropriate channels without fear of retaliation.

This policy does not prohibit respectful disagreement, factual reporting, legitimate feedback or responsible expression of opinions. It establishes boundaries against unlawful, abusive, threatening, misleading or otherwise inappropriate online conduct.

Roles and Responsibilities

Students, staff and parents are expected to use social media responsibly, respect privacy and report concerns. School leaders oversee investigations and policy implementation.

Principal and Senior Leadership Team (SLT)

- Oversee implementation of the policy and review serious allegations.

- Ensure reports are handled fairly, confidentially and consistently.
- Coordinate with the Designated Safeguarding Lead (DSL), Human Resources (HR), GEMS Leadership, or other relevant personnel.
- Determine whether external escalation or specialist advice is necessary.
- Ensure decisions and actions are appropriately documented.

Digital Leader / IT Admin

- Promote digital citizenship, online safety and responsible technology use.
- Support awareness sessions and staff training.
- Provide technical guidance for preserving relevant evidence where appropriate and authorised.
- Support management of official digital accounts.
- Refer safeguarding, disciplinary or legal concerns to the appropriate leader rather than independently determining legal liability.

DDSL

- Assess reports involving threats to student safety, exploitation, coercion, harassment or significant emotional harm.
- Manage safeguarding concerns through school procedures.
- Coordinate appropriate support and escalate to external agencies or authorities when required.

Staff

- Maintain professional boundaries in online communication.
- Comply with the Staff Code of Conduct, Acceptable Use Policy, GEMS Safeguarding Policy, and the school's applicable e-safety and digital communication policies.
- Photography and filming: Do not take photographs, record videos, or make audio-visual recordings of students, staff, or school activities anywhere on school premises, including classrooms, corridors, playgrounds, assembly halls, offices, and drop-off and pick-up areas, unless explicitly authorised by the school in accordance with its safeguarding, consent, and data protection procedures.
- Do not use personal devices to photograph or record students or school activities without explicit school authorisation. Do not share school-related images or recordings through personal accounts, social media, messaging groups, or other unauthorised platforms.
- Protect confidential school-related information and do not disclose or share it without proper authorisation.
- Report suspected safeguarding, privacy, or e-safety incidents through the school's established reporting procedures. Do not respond publicly or conduct unauthorised investigations.

Students

- Demonstrate respect, empathy and responsible digital citizenship.
- Avoid posting or forwarding harmful content.
- Report incidents to a trusted teacher, Form Tutor, Head of Year, DSL or designated staff member.
- Cooperate honestly with enquiries and avoid retaliation.
- Avoid posting images taken in school with or without consent.

Parents and Guardians

- Raise concerns respectfully through official school channels.
- Avoid publishing unverified allegations or personal attacks.
- Protect identifiable student information, private correspondence and school-related material.
- Encourage responsible online behaviour and cooperate with reasonable school enquiries.
- Photography and videography: Do not take photographs, videos, or other recordings anywhere on school premises, including classrooms, corridors, playgrounds, assembly halls, reception areas, school events, and drop-off and pick-up areas, unless explicitly authorised by the school in accordance with its approved safeguarding and photography procedures.
- Do not photograph or record other students, parents, or staff members without appropriate authorisation. Do not publish, upload, or circulate images or recordings containing identifiable students or staff through social media, WhatsApp groups, or other digital platforms without the required consent and school authorisation.
- Respect school photography restrictions and follow staff instructions regarding the use of mobile phones, cameras, and recording devices on school premises.
- Encourage responsible online behaviour among children and cooperate respectfully with reasonable school enquiries relating to safeguarding, privacy, e-safety, or breaches of school policy.

Official School Account Administrators

- Publish approved school-related content only.
- Protect account credentials and permissions.
- Obtain necessary permissions before publishing identifiable student information.
- Refer complaints and harmful comments to the appropriate school leader.

Guidelines for Responsible Social Media Use

Communicate respectfully, verify information before sharing, respect confidentiality, obtain consent before sharing images and use official channels to raise concerns.

EXPECTED STANDARDS OF ONLINE CONDUCT

All members of the school community are expected to:

- Communicate respectfully and professionally about students, parents, colleagues, school leaders and the institution.
- Verify information before sharing claims about individuals, school activities, incidents or decisions.
- Avoid publishing unverified allegations, fabricated information or malicious rumours presented as fact.
- Refrain from posting, reposting or circulating content that may unlawfully damage another person's reputation.
- Avoid abusive comments, personal attacks, threats, discriminatory remarks or targeted humiliation.
- Respect confidentiality, including student records, staff information, assessment materials, internal communications and safeguarding matters.
- Obtain appropriate authorisation and consent before publishing identifiable images, videos, recordings or personal information, in accordance with school procedures and applicable law.
- Refrain from creating fake accounts, impersonating others, manipulating digital content or using AI-generated media to misrepresent people or events.
- Avoid sharing private messages, screenshots or internal communications where doing so breaches confidentiality, privacy or other requirements.
- Use designated school communication and complaints procedures to resolve concerns.

Prohibited Conduct

Prohibited conduct includes, where it breaches this policy or applicable law:

- Publishing or circulating potentially defamatory allegations about students, parents, staff, school leaders or the school.
- Making or spreading knowingly false allegations intended to damage a person's reputation.
- Posting insulting, threatening, abusive or humiliating content targeting members of the school community.
- Creating or sharing manipulated images, videos, audio or AI-generated material to falsely portray an individual or event.
- Impersonating a student, parent, staff member, school leader or official school account.
- Encouraging others to attack, harass, shame or target an individual online.
- Reposting or forwarding harmful content in a way that further exposes or targets the person concerned.
- Publishing confidential school documents, private correspondence or personal information without appropriate authority.

- Sharing photographs, videos or recordings in breach of consent, privacy, safeguarding or school requirements.
- Using social media to threaten individuals, intimidate witnesses, retaliate against complainants or interfere with an investigation.
- Making unauthorised public statements on behalf of the school or presenting personal opinions as official school positions.
- Using anonymous accounts to evade accountability for prohibited conduct.

Each incident will be assessed on its own facts. A statement, complaint or disagreement is not automatically defamation merely because it is critical or unpopular.

Reporting Procedures

Incidents should be reported immediately to school leadership with supporting screenshots or evidence where available.

Step 1 — Report the incident.

Reports should be made promptly to the relevant contact:

- Student-related incident: Form Tutor, Head of Pastoral/Section, DSL or designated school leader.
- Staff-related incident: Principal, SLT or HR through the appropriate process.
- Parent or community concern: Principal, relevant SLT member or official school channel.
- Official account incident: Account administrator and relevant school leader.
- Immediate safeguarding or threat concern: DSL and, where necessary, the appropriate external authority.

Reports should include the platform, date and approximate time, relevant account/post/message or URL, factual description, available evidence, affected individuals where known, and any immediate safety concern.

Step 2 — Preserve evidence. Where safe and appropriate, preserve relevant screenshots, URLs, messages and timestamps. Handle evidence confidentially and share it only with authorised individuals. Do not access another person's account or obtain private information without authority, or circulate material more widely to collect evidence.

Step 3 — Acknowledge and assess. The receiving leader should record the concern and assess seriousness, urgency and potential impact. Immediate safeguarding risks, credible threats, ongoing harassment and continued public circulation of harmful content should be prioritised.

Step 4 — Refer appropriately. Depending on the circumstances, the matter may be referred to the Principal, SLT, DSL, HR, GEMS leadership, the relevant platform, legal advisers or competent external authorities.

Step 5 — Determine action. Consider the available evidence, relevant policies, age and circumstances of those involved, impact and safeguarding needs. Not every report will result in a finding of misconduct. Unsubstantiated allegations should be recorded appropriately and ongoing concerns addressed.

Investigation and Response

The school may review evidence, meet involved parties, inform parents, request content removal and apply disciplinary procedures when necessary. Reported incidents will be managed fairly, proportionately and confidentially. Depending on the circumstances, the school may review digital evidence; speak separately with those involved and relevant witnesses; inform parents or guardians where appropriate; refer safeguarding concerns to the DSL; request removal, correction or clarification of content; request that further sharing stops; provide education, restorative conversations or mediation where suitable and safe; apply relevant disciplinary procedures; or refer serious matters to GEMS leadership, HR, legal advisers or competent authorities. The details will be recorded on the GUARD.

The school will not require a public apology or public statement where this could cause further harm, compromise privacy or interfere with an external process.

Where a complaint concerns a member of SLT or another person responsible for handling complaints, it should be referred to an appropriate alternative senior authority within GEMS.

DISCIPLINARY CONSEQUENCES

Breaches may result in action under established school procedures and applicable GEMS requirements.

Students: Education or counselling; a formal reminder; parental notification and meeting; formal warning or behaviour sanction; restorative action where appropriate; justified restrictions on school-managed digital services; further action under the Student Behaviour or Anti-Bullying Policy; or referral to the DSL or competent authorities where necessary.

Staff: Guidance or training; a documented warning; referral to HR and the staff disciplinary process; justified restrictions on official account access; further employment-related action in accordance with GEMS requirements and applicable law; or referral to competent authorities where required.

Parents, Guardians and Other Adults: Request for removal or correction; a formal meeting; justified and permitted restrictions on school communication channels; proportionate arrangements for future communication or site access; or referral to GEMS leadership, legal advisers or competent authorities. Any restriction affecting essential school communication or safeguarding matters must be proportionate and follow school procedures.

Serious or repeated incidents: These may be escalated to school leadership, GEMS or competent external authorities. The school will not impose a predetermined penalty solely because an allegation has been made. Decisions will be based on the circumstances, available evidence and relevant procedures.

CONFIDENTIALITY, PRIVACY AND RECORD KEEPING

Reports and investigations shall be handled on a need-to-know basis. The school shall maintain appropriate records of reports, evidence, decisions and actions; protect personal and sensitive information in accordance with applicable UAE data protection requirements and GEMS procedures; restrict access to authorised personnel; avoid unnecessary circulation of screenshots and allegations; and retain and dispose of records under approved retention procedures. Safeguarding records shall be managed through the designated safeguarding process.

Confidentiality cannot be guaranteed where disclosure is necessary for safeguarding, a fair investigation, compliance with law or referral to competent authorities. Necessary disclosure shall be handled appropriately.

SAFEGUARDING AND SUPPORT

The school recognises that online allegations and reputational attacks can cause distress, anxiety, isolation and harm to wellbeing. Where necessary, appropriate pastoral, counselling, safeguarding or HR support will be arranged.

Students should seek help promptly and should not feel responsible for resolving serious online abuse independently. Retaliation against a person who raises a genuine concern, provides evidence or participates honestly in an investigation is not permitted and may be addressed under the relevant policy.

Where an allegation is unsubstantiated, the school will consider whether support, clarification or other proportionate action is needed.

AWARENESS, TRAINING AND PREVENTION

The school shall promote awareness through age- and role-appropriate measures, including digital citizenship and online reputation lessons; staff induction and periodic refresher training; parent communications; guidance on respectful online communication, privacy and confidentiality; training on reporting and safeguarding; e-safety activities and assemblies; and guidance on responsible AI-generated content and digital media. These measures may be incorporated into existing digital citizenship, e-safety, anti-bullying and professional development programmes.

LEGAL AND REGULATORY COMPLIANCE

This policy shall be implemented in accordance with applicable UAE legislation, relevant education and safeguarding requirements, and GEMS policies and procedures. Relevant legislation includes, as applicable:

- Federal Decree-Law No. 34 of 2021 on Countering Rumors and Cybercrimes.
- Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data.
- Other applicable UAE legislation relating to privacy, reputation, online conduct, child protection and information security.

Official references:

UAE Government — Media Regulation: <https://u.ae/en/Media/Media-In-The-UAE/Media-regulation>

UAE Government — Cyber Safety and Digital Security: <https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security>

UAE Legislation — Federal Decree-Law No. 34 of 2021: <https://uaelegislation.gov.ae/en/legislations/1526>

This policy does not replace legislation, GEMS requirements or professional legal advice. The application of any law to a particular incident must be determined by reference to the relevant facts and legal requirements.

MONITORING AND IMPLEMENTATION

The Principal and designated policy owner shall oversee implementation. Monitoring may include reviewing reported incidents and recurring concerns; evaluating reporting and response procedures; reviewing relevant safeguarding, behaviour and digital citizenship records; monitoring required awareness and training; identifying improvements to prevention; and reviewing stakeholder feedback and emerging digital risks. The school shall maintain appropriate evidence of communication, awareness and implementation.

POLICY REVIEW AND APPROVAL

This policy shall be reviewed annually or earlier if significant changes occur in UAE legislation, GEMS requirements, school procedures, safeguarding expectations or the digital environment. Revisions shall be reviewed by the designated policy owner and approved by the appropriate school leadership authority before publication. Approved revisions shall be communicated to relevant stakeholders and the latest authorised version maintained in the designated policy repository.

Consequences of Breach

Students, staff and parents may face appropriate actions under school policies and, where necessary, referral to authorities.

Awareness and Education

The school will provide ongoing digital citizenship, e-safety and responsible social media awareness programmes.

Confidentiality

All reports will be handled confidentially and shared only on a need-to-know basis.

Monitoring and Evaluation

The policy will be reviewed annually and updated to reflect legal, safeguarding and technological developments.