



KGS Social Media Policy

Revised July 2026

Approved by KGS Board

Responsible Officer	Principal
Review Cycle	Annual
Next Review	July 2027

Karachi Grammar School

Social Media Policy

Social media is recognised as an important means of communication, learning, creativity and community engagement. Karachi Grammar School seeks to educate students to use digital technologies responsibly rather than simply restricting their use. The School adopts an educational, safeguarding and restorative approach wherever appropriate while maintaining high expectations of conduct.

1. Purpose

Social media refers to any digital platform that allows users to create, share, or interact with content or communicate with others online.

This policy sets out expectations for responsible, respectful, and safe use of social media by students. Karachi Grammar School recognises that its reputation, values, and duty of care extend beyond the physical campus and into online spaces, particularly where the School's name, uniform, or community members are identifiable in such spaces.

Students are expected to ensure that their online behaviour reflects the School's core values of Integrity, Respect, Responsibility, Excellence, Intellectual Curiosity, and Compassion, both on and off campus.

Students must also respect the privacy and personal data of others at all times and must not share, distribute, or use personal information, images, or content without appropriate consent.

This policy also addresses the emerging threat of AI-generated image exploitation, including Deepfakes — an AI-generated or AI-manipulated media (such as video, audio, or images) that makes it appear someone said or did something they did not actually say or do. Any incident involving AI-generated imagery of students or staff shall be treated as a safeguarding, cyber security, and criminal matter and responded to accordingly.

See Section 6 (Deepfakes and AI-Generated Content) below for definitions, prohibited conduct, and reporting expectation.

This policy should also be read alongside the KGS Mobile Phone/Smart Device Policy, which governs the possession and use of mobile phones and smart devices on School premises and during educational activities. Where a breach of that policy also involves online conduct — for example, an unauthorised device being used to film, photograph, or post content — both policies apply and the matter may be addressed under either or both frameworks.

2. Scope

This policy applies to:

All students enrolled at the School.

All social media platforms including, but not limited to Instagram, TikTok, Snapchat, X, YouTube, WhatsApp, Discord, gaming platforms, and emerging digital platforms.

All online activity on or off campus, during or outside school hours, where the School is identifiable

AI-generated or AI-manipulated images and videos involving members of the school community, regardless of whether such content was created on or off school premises.

The possession and use of mobile phones and smart devices on School premises and during educational activities, which is addressed separately by the KGS Mobile Phone/Smart Device Policy and should be read alongside this policy.

Students and parents/guardians are required to support this policy as part of their shared commitment to the values and community of Karachi Grammar School.

As a school we will help students learn to use social media effectively to:

- evaluate misinformation
- identify manipulated media
- understand algorithms
- respect intellectual property
- understand digital footprints
- engage respectfully in online debate
- understand AI ethics

Parents/guardians are expected to monitor and support appropriate online behaviour at home and to work in partnership with the School in reinforcing this policy.

3. Guiding Principles

All online activity should demonstrate the School's Core Values:

Integrity: Communicating honestly and responsibly and avoiding behaviour that misrepresents others or the School.

Respect: Treating others with dignity, empathy, and inclusivity in all digital interactions.

Responsibility: Recognising that online actions have consequences and taking ownership of one's digital behaviour.

Excellence: Maintaining high standards of conduct that reflect the reputation of the School.

Intellectual Curiosity: Using digital platforms thoughtfully to engage with ideas, creativity, and learning.

Compassion: Demonstrating kindness and understanding and avoiding behaviour that harms or excludes others.

Senior students, including council members and prefects, are expected to be familiar with the Policy, demonstrate leadership in digital conduct and act as visible role models for younger students. Prefects/Monitors should actively promote respectful online behaviour and report concerns where appropriate.

4. Use of School Uniform on Social Media

4.1 General Rule

The School uniform represents Karachi Grammar School at all times.

Any student posting content while wearing the School uniform is considered to be acting as a representative of the School and must demonstrate behaviour consistent with the School's Core Values.

4.2 Prohibited Content While in School Uniform

Students must not post, share, or appear in content while wearing the School uniform that includes:

- Inappropriate, offensive, discriminatory, sexualised, or explicit material
- Bullying, harassment, intimidation, or exclusion of others
- Swearing, obscene gestures, or suggestive behaviour
- Promotion or depiction of alcohol, vaping, smoking, drugs, fake or real guns/ammunition, or illegal activity
- Dangerous behaviour, pranks, or activities that may cause harm
- Content that brings the School into disrepute
- Content recorded on School premises without permission
- Content that promotes a product, brand, or commercial organisation

These restrictions apply regardless of platform, privacy settings, or intended audience.

4.3 School Identification Without Uniform

Even when not wearing the School uniform, students must not post content that:

- Identifies the School by name, logo, caption, location, or tagging
- Implies endorsement by the School
- Damages the reputation of the School or its community

Students should exercise integrity, responsibility, and good judgment when referencing the School online.

4.4 Filming and Photography on Campus

To protect the privacy, dignity, and safety of the School community:

- Filming or photographing on School premises for social media requires written approval from the Head of Section or a staff member specifically designated by the Head of Section.
- Students must not record staff or other students without consent
- Recording during classes is strictly prohibited
- Secret recordings are strictly prohibited
- Students must not have a mobile phone or smart device on School premises in order to film or photograph, except where an exception has been granted under the KGS Mobile Phone/Smart Device Policy (e.g. a documented medical exception or a specific, time-limited permission); any approved filming or photography must still comply with the requirements of this section

These expectations reflect the School's commitment to Respect, Responsibility and Compassion.

5. Privacy, Safety, and Digital Wellbeing

The School will provide education on digital safety, responsible online behaviour, and media literacy through appropriate programmes such as IT lessons, PSHCE, assemblies, and workshops. Karachi Grammar School recognises that students are developing their understanding of digital responsibility and aims to support this through education as well as guidance.

Students are encouraged to practise responsible digital behaviour by:

- Using the highest available privacy settings
- Avoiding sharing personal details such as location, routines, or school schedules
- Reporting online harassment, impersonation, threats, or harmful behaviour immediately

The School reserves the right to investigate online activity that may affect student welfare or the reputation of the School community. **Sharing unauthorised material related to any assessments/examinations, whether confidential or fake, on any communication or social media platform may be considered malpractice. Examples of such malpractice are:**

- **Receiving such material and not reporting it**
- **Forwarding such material after receiving it**

6. Deepfakes and AI-Generated Content

Deepfake: Synthetic or digitally manipulated media — including video, images, audio, or voice recordings — created or altered using artificial intelligence to depict a real, identifiable person saying, doing, or appearing to endorse something they did not actually say, do, or endorse.

This includes, but is not limited to:

- **Face-swap or manipulated video** depicting a member of the KGS community
- **Voice cloning**, including synthetic phone calls, voice notes, or audio messages impersonating staff, students, or School leadership
- **Fabricated images**, whether wholly AI-generated or edited, placing a real person in a false or misleading context
- **Impersonated official communication** — fake letters, emails, or messages (e.g. WhatsApp, SMS) falsely attributed to School leadership, staff, or the School itself, whether or not AI tools were used to generate them
- **AI-generated text impersonation** — content mimicking a real person's writing style or voice to fabricate statements attributed to them

Policy Statement

Prohibited

- Creating, editing, or generating deepfake content depicting any member of the KGS community (student, staff, or leadership) without their explicit consent
- Creating or sharing any sexualised, intimate, or degrading AI-generated imagery of a minor or any member of the School community — this constitutes a serious safeguarding violation and will be escalated immediately as such, regardless of intent claimed
- Using AI tools to impersonate School leadership, staff, or official School communications (e.g. fake circulars, fake WhatsApp accounts purporting to be from the School)
- Sharing, forwarding, or amplifying known or suspected deepfake content targeting a member of the School community

Caution — Reportable

- Receiving unsolicited communication (message, call, voice note) that seems to originate from a School authority but feels inconsistent or suspicious — do not act on it or forward it; report immediately to the designated contact (IT, Officer Communications, or Academic Committee)

- Encountering AI-generated content of uncertain origin depicting a member of the School community — report rather than investigate or share independently
- Use of AI tools for legitimate creative, academic, or presentation purposes that incidentally involves a real person's likeness (e.g. a class project) — requires prior staff sign-off

Guidance for the Community

- Verify official communications through known, published channels (e.g. direct call-back to the School office) before acting on unusual requests, especially those involving urgency, money, or personal information
- Staff and students are encouraged to familiarise themselves with common signs of AI-manipulated audio/video (unnatural pacing, mismatched lip movement, inconsistent lighting/audio quality)
- Parents are encouraged to discuss deepfake awareness with their children as part of broader digital literacy at home

7. Breaches of Policy

7.1 Investigation

The School may investigate social media activity where:

- The School or its uniform is identifiable
- Student wellbeing or safety may be affected
- School values or codes of conduct may have been breached

Staff are responsible for monitoring, reporting, and responding to concerns related to student social media use. The School's Officer Communications is responsible for advising on appropriate use of the School's name, image, and brand, and may be involved in reviewing or addressing content that impacts the School's reputation.

7.2 Consequences

Violations will be handled under the School's existing disciplinary framework, with severity assessed according to intent, harm caused, and whether safeguarding concerns are engaged. Cases involving impersonation of School leadership or fabricated official communication and cases involving minors and any sexualised or degrading content will be escalated immediately as safeguarding matters, in line with PECA 2016 and referred where appropriate to NCCIA or the Digital Rights Foundation.

Consequences may include

- Immediate removal of content
- Parent or guardian notification
- Loss of privileges
- Detention, suspension, or further disciplinary action

Repeated or continual breaches of this policy may result in escalated consequences. Breaches may be referred to external authorities where appropriate.

8. Reporting Concerns

Concerns regarding social media activity should be reported to:

- Head of Year/House
- Senior Staff Member
- School's Media Officer

Reports will be handled sensitively.

Related Policies: This policy should be read in conjunction with the KGS Mobile Phone/Smart Device Policy.

Appendix I

The following resources are recommended with regards to AI-generated image exploitation and online safety. Pakistani authorities are listed first, followed by global resources.

Reporting Harmful or Exploitative Content

Pakistan — Primary Channels

- **National Cyber Crime Investigation Agency (NCCIA)** — Pakistan's lead cybercrime authority (replaced FIA Cyber Crime Wing in April 2025). The NCCIA operates under the Ministry of Interior and is headquartered at National Police Foundation Building, Sector G-10/4, Islamabad. Helpline: **1799** | Office: 051-9106691 | Website: nccia.gov.pk [Wikipedia](#)
- **Digital Rights Foundation (DRF) — Cyber Harassment Helpline:** Pakistan's first dedicated, free, confidential helpline for victims of online harassment, including non-consensual image abuse. Helpline: **0800-39393** | Monday–Sunday, 9:00 AM–5:00 PM | Email: helpdesk@digitalrightsfoundation.pk Provides legal advice, digital security support, and psychological counselling. [Digitalrightsfoundation](#)
- **Pakistan Telecommunication Authority (PTA)** — To report and request removal of unlawful online content (nudity, pornography, exploitative material) under PECA 2016. Content complaints: content-complaint@pta.gov.pk | Consumer helpline: **0800-55055** | Website: pta.gov.pk [Pakistan Telecommunication Authority](#)
- **Child Protection Helpline — 1121:** A nationwide toll-free helpline set up to report child abuse cases. [ProPakistani](#)
- **Madadgaar National Helpline — 1098:** A victim support service operated by ROZAN, covering child and women's protection cases including online abuse.

Legal Framework

- **Prevention of Electronic Crimes Act (PECA) 2016:** The primary legislation governing cybercrime in Pakistan, including child sexual abuse material, non-consensual image sharing, blackmail, and harassment. Recent amendments have increased penalties for child exploitation offences to 14–20 years' imprisonment, and these offences are now non-bailable and non-compoundable. [Pakistan Today](#)
- **PTA Content Removal Powers (Section 37, PECA 2016):** The PTA has authority to block and remove unlawful online content upon complaint.

Global Resources — Retained for International Reach

- **Take It Down — NCMEC (ncmec.org):** A global service helping minors request removal of exploitative images online — accessible to Pakistani users.
- **Internet Watch Foundation (IWF) (iwf.org.uk):** Report child sexual abuse material hosted anywhere online; IWF works with platforms globally to remove content.
- **Report Remove Tool — NSPCC / Childline:** For young people wishing to request removal of intimate images online — usable internationally.

Appendix II

Safeguarding Guidance Resources

Note: Most safeguarding guidance resources below are UK-origin but contain frameworks, language, and tools that are applicable. They should be read alongside PECA requirements

-
- **SWGfL — Support and Advice for Schools on Synthetic Media & Deepfakes:** swgfl.org.uk
 - **Safer Schools NI — Safeguarding Pupils: Preventing and Responding to AI-Generated Image Exploitation**
 - **Safer Schools NI — Is Your Child's Photo Safe? Understanding Image Consent at Schools**
 - **ICO — Data Protection Advice on School Photography:** Rules on photographing students — relevant to KGS's own data governance obligations
 - **POSH & UKCIS — Best Practices for School Websites:** Safely managing photos and videos online
 - **Paternoster Communications — Suggested Policy for Safeguarding Against AI Deepfake Misuse of School Website Images**
 - **UNICEF Pakistan & PTA — "Safeguarding Your Child in the Digital Age":** A guidebook produced in collaboration with UNICEF Pakistan, Telenor Pakistan, and the National Commission on the Rights of Child — directly relevant for parent communications in a Pakistani school context. [ProPakistani](#)
-

Image Anonymisation Tools

(these are platform/software tools with no geographic limitation)

- **AnonFace** — realistic AI face swaps
 - **DeepPrivacy2** — replace faces with synthetic alternatives (open source)
 - **ClearFace AI** — face blurring/replacement, used in education and journalism sectors
 - **Photoshop Neural Filters** — morphs or obscures faces realistically
 - **Facepixelizer** — automatic face pixelation (free, web-based)
 - **PhotoGuard (MIT)** — protects photos from AI manipulation by scrambling pixels invisibly
-

Staff Training Resources

- **Digital Rights Foundation (DRF)** (digitalrightsfoundation.pk): Conducts awareness and training sessions in Pakistan on AI-facilitated harassment, technology-facilitated gender-based violence (TFGBV), and digital safety — a local resource for staff CPD.
 - **NCCIA Awareness Programme**: The NCCIA has launched a nationwide public awareness campaign and trained over 300 law enforcement officers in cyber investigation; their public advisories on emerging threats are accessible on nccia.gov.pk. [Pakistan Observer](#)
 - **NCSC (UK) — Professional Skills and Training** (ncsc.gov.uk): Retained — globally accessible and high quality for IT staff and DSLs.
 - **INEQE — School Guide to AI-Generated Image Exploitation**: Practical guide for school leaders and DSLs.
 - **Wellbeing Hub (Teen Tips)** (teentips.co.uk): Supporting victims of AI-generated explicit image extortion in schools.
 - **EndTAB — Cyber Abuse Safety Training**: Retained for staff training content.
-



Social Media Guidelines for Students

Area	Do's	Don'ts
General Online Behaviour	Use social media responsibly and respectfully. Ensure posts reflect the School's values: Integrity, Respect, Responsibility, Excellence, Intellectual Curiosity, and Compassion.	Do not post content that harms others, spreads misinformation, or reflects poorly on the School community.
Respect for Others	Treat classmates, staff, and others with kindness and dignity online. Think before posting or commenting.	Do not bully, harass, intimidate, or exclude others online. Do not share embarrassing or harmful content about others.
Responsibility Online	Understand that your online actions have consequences. Take responsibility for what you post and share.	Do not assume private accounts make posts acceptable. Do not share inappropriate content even if the audience is "friends only."
Posting in School Uniform	Remember that wearing the uniform means you represent Karachi Grammar School. Post content that reflects positive behaviour and school values.	Do not post content in uniform that includes: • Offensive or explicit material • Swearing or obscene gestures • Bullying or harassment • Alcohol, vaping, smoking, drugs • Fake or real guns/ammunition • Dangerous pranks or risky behaviour • Content that damages the School's reputation
Sharing exam-related material on communication or social media platforms	Immediately report any exam-related material you receive that appears confidential, suspicious, or unauthorised.	Do not share, upload, or circulate any exam-related material—whether real or fake—on any communication or social media platform.
Referencing the School	Use good judgment when mentioning the School online.	Do not tag, name, or identify the School in posts that could damage its reputation or suggest endorsement of inappropriate content.
Filming and Photography on Campus	Get written approval before filming or taking photos for social media. Ask permission before recording others.	Do not film on school premises without permission. Do not record staff or students without consent. Do not record during classes or make secret recordings.
Promotions and Commercial Content	Keep school-related posts appropriate and personal.	Do not promote products, brands, or businesses while wearing the school uniform.
Privacy and Safety	Use strong privacy settings. Protect personal information such as location or schedules. Report online harassment or threats.	Do not share sensitive personal details publicly. Ignore or hide serious online harassment or threats.



Social Media Guidelines for Parents

Area	School Expectation	Role of Parents
Shared Responsibility	Safe and responsible social media use is a partnership between school and home.	Reinforce school expectations and model positive digital behaviour at home.
Understanding Social Media	Social media includes all platforms where content is shared or communication takes place (e.g. Instagram, TikTok, WhatsApp, gaming platforms).	Stay informed about the platforms your child uses and how they work.
Student Behaviour	Students must reflect KGS values: Respect, Responsibility, Integrity, Compassion in all online interactions.	Encourage respectful communication and discuss appropriate online behaviour regularly.
Use of School Identity	Students must not post inappropriate content in school uniform or content that identifies the school without permission.	Remind children that representing the school online carries responsibility and consequences.
Privacy & Data Protection	Students must respect the privacy and personal data of others and avoid sharing sensitive information.	Guide children on not sharing personal details (location, routines, images of others without consent).
Online Safety	Students should avoid harmful interactions and report concerns such as bullying or fake accounts.	Talk openly about risks (cyberbullying, strangers, inappropriate content) and encourage children to seek help.
Monitoring & Guidance	Students are expected to make responsible choices online.	Monitor device use, review privacy settings, and maintain open communication without being intrusive.
Digital Wellbeing & Education	The School teaches digital citizenship, online safety, and media literacy.	Reinforce these lessons at home and encourage balanced screen time and healthy habits.
Responding to Concerns	The School will investigate issues affecting student wellbeing or school reputation.	Report concerns to the School and work collaboratively to resolve issues.
Consequences	Breaches may lead to disciplinary action; repeated issues result in escalation.	Support the School in addressing behaviour and helping children learn from mistakes.
Leadership & Role Modelling	Senior students are expected to act as role models.	Encourage children to positively influence peers and act responsibly online.
Filming and Photography on Campus	Get approval before filming or taking photos at school events. Ask permission before recording other children.	Do not film on school premises without permission. Do not record children without consent.
Parental Engagement	The School values active parent partnership in promoting safe social media use.	Your involvement is essential. Regular conversations, clear boundaries, and active guidance at home are the most effective ways to ensure your child uses social media safely and responsibly.



Social Media Guidelines for Staff

Area	School Expectation	Role of Staff
Shared Responsibility	Safe and responsible social media use is a whole-school responsibility.	All staff must model professional and responsible online behaviour, and all teaching staff must reinforce expectations consistently with students.
Professional Conduct	Staff must uphold the School's values (Integrity, Respect, Responsibility, Compassion) in all online interactions.	All staff must maintain appropriate boundaries with students online and ensure all communication is professional and appropriate.
Student Behaviour Oversight	Students are expected to adhere to the social media policy at all times where the School is identifiable.	Relevant staff must monitor student behaviour where concerns arise and address issues promptly and appropriately.
Use of School Identity	The School's name, uniform, logo, and community must not be misused online.	Relevant staff must ensure any content involving the School is accurate, appropriate, and authorised before being shared.
Filming & Photography on Campus	Filming/photography requires prior approval and must respect privacy and dignity.	Relevant staff must grant or verify approvals (where authorised), ensure consent is obtained, and intervene where misuse occurs.
Privacy & Data Protection	Student data and images must be protected and not shared.	Relevant staff must safeguard student information, avoid sharing images/data without permission, and follow school data protection protocols.
Online Safety & Safeguarding	The School has a duty to protect student wellbeing, including in online spaces.	Relevant staff must identify, report, and respond to safeguarding concerns (e.g. cyberbullying, harmful content, impersonation).
Monitoring & Reporting	The School may investigate social media activity affecting students or its reputation.	All staff must report concerns through appropriate channels (Officer Communications, Assistant Head, Head of Section). Do not ignore or handle serious issues independently.

Role of Officer Communications	The School's public image and messaging must be protected.	Relevant staff must work with the Officer Communications on matters involving media, public content, or reputational risk. Seek guidance when unsure.
Education & Digital Citizenship	The School prioritises education on digital safety and responsible online behaviour.	Relevant staff must actively support and deliver digital citizenship education through lessons, discussions, and pastoral care. Reinforce positive online habits.
Responding to Incidents	Breaches of policy will be addressed in line with school procedures.	Relevant staff must apply policy consistently, document concerns, and support fair and proportionate responses.
Repeated or Serious Breaches	Ongoing or serious issues require escalation.	Relevant staff must escalate repeated concerns to senior leadership and contribute to monitoring and follow-up actions.
Student Leadership	Senior students (Prefects, Council) are expected to act as role models.	Relevant staff must support and guide student leaders in promoting positive online behaviour and addressing peer concerns responsibly.
Parent Partnership	Parents are key partners in supporting appropriate online behaviour.	Relevant staff should communicate concerns to parents when required and work collaboratively to support student wellbeing.
Staff Conduct Online	Staff conduct online should not compromise professional integrity or the School's reputation.	All staff must avoid posting content that could be perceived as unprofessional or that links students/school to inappropriate material. Use privacy settings responsibly.



Student Social Media Guidelines for House Pages | Societies | School Teams | Events

As student leaders managing official or affiliated KGS social media pages, you represent your team, your peers, and the entire KGS community. Your posts should reflect the school's core values of Integrity, Respect, Responsibility, Excellence, Intellectual Curiosity, and Compassion.

Guidelines	
✓ Represent KGS Positively	Celebrate achievements, teamwork, and school spirit. Ensure posts reflect KGS core values and standards.
✓ Be Respectful & Inclusive	Show respect and compassion for all students, staff, and community members. Avoid offensive, discriminatory, or exclusionary content.
✓ Use Clear & Thoughtful Language	Communicate professionally with correct grammar, spelling, and a respectful tone—even for fun or informal content.
✓ Get Consent for Photos	Only post images of students who have not opted out of social media. Ask permission before tagging or featuring individuals.
✓ Stay Appropriate	Share school-related, meaningful, and age-appropriate content. Avoid slang, offensive language, memes, or trends that could be misinterpreted.
✓ Collaborate with Staff	Seek guidance from the Officer Communications, Society Patron or Team Coach for major announcements, competitions, or sensitive topics or whenever you are unsure.
✗ Do Not Share Sensitive Information	Avoid posting grades, disciplinary matters, personal contact information, or internal conflicts. Respect privacy and dignity
✗ Do Not Engage in Negativity	Do not argue online, criticise others or make fun of anyone.
✗ Do Not Record or Post During Lessons	Always prioritise academic responsibilities and ensure that learning spaces are free from social media distractions.
🔒 Account Management Tips	Use strong passwords for official Instagram accounts and share them only with authorised student leaders or staff responsible for managing these accounts. This applies strictly to official account management and does not override the general principle of keeping personal passwords private. Turn off DMs unless monitored. Log out on shared devices. Hand over credentials properly when leadership changes.
💡 Final Note	Social media builds school spirit and showcases student talent. Always reflect Integrity, Respect, Responsibility, Excellence, Intellectual Curiosity, and Compassion. Contact Officer Communications at comms@kgs.edu.pk for guidance.