Cyberbullying Policy
2025 – 2026

POLICY INFORMATION	
Last review date:	January 2026
Reviewed by:	IT Administrator
Next review date:	September 2026
Approved By:	Principal – Daspo Yiappos

Beirut St., Muhaisnah 4
Al Qusais Industrial Area,
Dubai United Arab Emirates
Tel: +97142543666
Website: www.oxford.sch.ae

Policy Statement

THE OXFORD SCHOOL (TOS) is committed to creating and maintaining a safe, respectful, and inclusive learning environment where technology enhances education without harming the emotional, mental, or social well-being of its students.
TOS has a zero-tolerance stance against cyberbullying and related digital misconduct. This policy outlines the school's approach to preventing, detecting, responding to, and educating about cyberbullying.

1. Definition of Cyberbullying

Cyberbullying is defined as deliberate and repeated harm inflicted through the use of electronic communication technologies, such as:

- Text messages and instant messaging
- Emails, online forums, and chat rooms
- Social media platforms (e.g., Instagram, Snapchat, TikTok, WhatsApp, Facebook)
- Gaming platforms
- Sharing or distributing embarrassing, threatening, or malicious content (texts, images, videos)

Cyberbullying includes, but is not limited to:

- Sending abusive or threatening messages
- Spreading rumours or lies online
- Publishing defamatory material about an individual
- Impersonating others online to damage their reputation
- Excluding individuals deliberately from online groups
- Sharing unauthorized or manipulated photos or videos

2. Differences from Traditional Bullying

- 24/7 access: Victims can be targeted anytime, anywhere.
- Anonymity: Bullies may hide their identity online.
- Wider audience: Content can be shared globally, instantly.
- Persistence: Content posted online can resurface indefinitely.
- Legal Impact: Cyberbullying can lead to criminal charges under UAE law.

3. Aims and Principles

- Promote a safe and positive digital environment.
- Raise awareness about the serious effects of cyberbullying.
- Establish clear procedures for reporting and addressing incidents.
- Empower students to stand against cyberbullying.
- Ensure staff are trained to identify and respond to concerns.
- Align practices with UAE Federal laws and regulations.

4. Prevention Strategies

- Integrate cyber safety and digital citizenship programs in the curriculum (PSHE, Moral Education, ICT).
- Conduct assemblies, workshops, and awareness drives.
- Display cyber safety posters around the campus.
- Engage parents through information sessions and newsletters.
- Provide regular staff CPD (Continual Professional Development) on cyberbullying detection and intervention.
- Maintain a proactive "Speak Up" culture encouraging reporting.

6 Roles and Responsibilities

6.1 Senior Leadership Team (SLT)

- Lead the creation of a safe digital culture.
- Oversee policy implementation and compliance.
- Ensure cyberbullying is addressed in the Safeguarding and Anti-Bullying Policies.

6.2 Designated Safeguarding Leads (DGCC)

- Manage all cyberbullying reports confidentially and sensitively.
- Liaise with students, parents, staff, and external agencies where necessary.
- Maintain detailed records of reported incidents and actions taken.

6.3 Teachers and Staff

- Actively monitor student behaviour online (including virtual platforms).
- Reinforce positive digital conduct during lessons and communications.
- Immediately report any suspected cyberbullying to DGCC s.

6.4 Students

- Use technology respectfully and responsibly.
- Report cyberbullying if witnessed or experienced.
- Support peers facing online harassment.

6.5 Parents and Guardians

- Supervise their child's technology usage at home.
- Encourage open discussions about digital life and challenges.

- Support school interventions and disciplinary processes when required.

7. Reporting Procedures

Students, parents, or staff can report cyberbullying through:

- Speaking directly to a trusted teacher, school counsellor, or Designated Safeguarding Lead (DGCC).
- Emailing the dedicated safeguarding address: [safeguarding@oxford.sch.ae]
- Using the School Cyberbullying Incident Report Form (available in digital and paper form).
- Anonymous reporting via the school's online reporting portal (if available).

Students are encouraged to:

- Save all abusive messages, images, or conversations.
- Take screenshots as evidence.
- Avoid responding to the bully.

Important:
Reports will be handled confidentially, and no retaliation for reporting will be tolerated.

8. Investigation and Response

Upon receiving a report:

- The DGCC will assess the nature and severity of the complaint within 24 hours.
- Evidence will be collected (messages, emails, screenshots).
- The alleged perpetrator and victim will be interviewed separately.
- Witnesses, if any, will be consulted.
- Parents of all parties will be informed appropriately.
- A decision will be made whether the behaviour constitutes cyberbullying under this policy.

Possible Outcomes:

- Verbal warning.
- Loss of internet privileges.
- Temporary or permanent confiscation of personal devices.
- Suspension (internal or external).
- Referral to police/cybercrime authorities if criminal offenses are identified.

9. Sanctions and Support For the Perpetrator:

- Behaviour intervention programs.
- Counselling support.
- Formal disciplinary actions (aligned with School Behaviour Policy).

For the Victim:

- Immediate support from the pastoral care team.
- Safe space and supervision as needed.
- Follow-up well-being checks.
- Counselling referrals if necessary.

Bystanders:

- Encouraged to support victims by reporting and not participating in harmful behaviours.
- Education about their role in breaking the cycle of bullying.

10. Working with External Authorities

TOS reserves the right to involve external agencies including:

- Dubai Police – Cybercrime Department
- Telecommunications Regulatory Authority (TRA)
- Child Protection Specialists from the UAE Ministry of Education

for serious offenses, especially where the law is broken or the safety of a student is at risk.

11. Record Keeping

- Every incident will be documented securely.
- Records will include dates, times, individuals involved, actions taken, and outcomes.
- Confidentiality will be respected according to UAE Data Protection Law.
-

12. Legal Framework (UAE Law Compliance)

Cyberbullying may involve violations of:

- Federal Decree Law No. 34 of 2021 (Combating Rumours and Cybercrimes)
- UAE Child Rights Law (Wadeema Law)
- Penal Code (Federal Law No. 3 of 1987) on Defamation and Harassment

13. Possible Legal Consequences Include:

- Fines between AED 250,000 – AED 500,000.
- Imprisonment up to 2 years.
- Deportation for non-UAE nationals in serious cases.
- Mandatory police involvement for sextortion, cyberstalking, child endangerment.

TOS will fully cooperate with authorities where required by law.

14. Breaches and Disciplinary Procedures

Breaches of this policy may result in:

- Loss of system or network access.
- Official warnings.
- Suspension or dismissal (for staff).
- Suspension, exclusion, or expulsion (for students).

Legal action in line with UAE laws

15. Policy Review

- This policy will be reviewed annually by the DGCC and updated based on evolving cyber risks, regulatory changes, and stakeholder feedback.

This Cybersecurity Policy will be:

- Reviewed annually by the IT Manager, DGCC, and Principal.
- Updated following major cyber incidents, technological changes, or amendments to UAE laws.

16. Education and Training

- Annual workshops for students on safe online behaviour.
- Annual parent seminars about online risks and digital parenting.
- Mandatory CPD for staff on recognizing, preventing, and handling cyberbullying.
- Integration of Online Safety modules in the Moral Education and PSHE curriculum.

17. Monitoring and Review

- The policy will be reviewed annually.
- Emerging risks, legal updates, or significant incidents will trigger interim reviews.
- Feedback from students, parents, and staff will be sought to improve effectiveness.
- This policy will be reviewed annually by the DGCC and updated based on evolving cyber risks, regulatory changes, and stakeholder feedback.