



Queen
Elizabeth's
School

DUBAI SPORTS CITY

E-Safety Policy

Academic Year 2026-27

	Name	Title	Date
Prepared by	Dan Clark	Principal	20/04/2026
Reviewed by	Belle Wagner	Head of Prep	22/04/2026
Approved by	Governing Body		10/07/2026
Next review	August 2027		

1. Purpose & Scope

This policy sets out how Queen Elizabeth's School Dubai Sports City (QE) ensures the safety and wellbeing of students, staff and the wider community in all online activity. As digital interaction becomes increasingly interconnected with learning, communication, and wellbeing, QE is committed to fostering a secure, respectful, and responsible digital environment.

This policy applies to:

- All QE students
- All teaching, administrative, operational, and support staff
- Governors, contractors, visitors, and volunteers
- Parents/carers supporting children's online activity at home

The policy provides a coherent framework for safe digital conduct, prevention of harm, effective response to incidents, and community-wide education and acknowledges that the development of digital skills and citizenship are fundamental to the school's mission of developing confident, able and responsible young people.

2. Regulatory context

Our approach aligns with current UAE federal legislation and KHDA expectations, including:

- Federal Decree Law No. 34 of 2021 on Combatting Rumours and Cybercrimes.
- Federal Decree Law No. 45 of 2021 on Personal Data Protection.
- Wadeema's Law (Federal Law No. 3 of 2016) protecting child rights and digital safety.

We also draw upon international guidance, including UK publications such as Teaching Online Safety in Schools, Preventing and Tackling Bullying, and the UKCIS Framework to support best practice.

3. Principles

Our online safety approach follows six core principles:

- **Safety First** – online environments are structured, monitored and protective.
- **Respectful behaviour** – Digital conduct reflects on-site behavioural expectations.
- **Education & empowerment** – Students, staff and families receive guidance on safe and responsible use.
- **Inclusion** – Students of determination should receive adapted tools and support.
- **Partnership with families** – Clear communication ensures aligned expectations.
- **Safeguarding continuity** – All safeguarding policies apply equally online and on site.

4. Categories of Online Risk

We address digital risk across four key areas:

- **Content risk:** exposure to harmful, illegal or age-inappropriate content.
- **Contact risk:** interactions with others, including grooming, coercion, or pressure.
- **Conduct risk:** harmful behaviours such as cyberbullying or sharing explicit images.
- **Commerce risk:** phishing, scams, fraud, or unauthorised purchases.

5. Roles & Responsibilities

Principal & Senior Leadership Team (SLT)

- Ensure effective policy implementation and compliance.
- Oversee filtering, monitoring and online safety procedures.
- Embed online safety within curriculum, pastoral systems and staff training.

Designated Safeguarding Lead (DSL)

- Lead online safety incident management and escalation.
- Maintain digital safeguarding logs.
- Conduct annual policy review and digital risk assessment.
- Provide regular training and updates for staff.

IT Manager / Digital Systems Lead

- Maintain secure digital infrastructure.
- Manage filtering and monitoring systems.
- Conduct vulnerability checks and malware protection.
- Support investigations with technical evidence.

All Staff

- Model professional digital behaviour.
- Use school-approved platforms and accounts.
- Report concerns immediately to the DSL.
- Enforce and uphold acceptable use expectations.

Parents/carers

The school takes the view that optimal online safety can only be achieved where home and school are collaborative and consistent in their approach.

Parents are encouraged to:

- Monitor home digital activity.

- Support discussions on safe online behaviour.
- Report concerns promptly.

Students

The school's educational philosophy has at its core the mission of developing confident young people who are able to navigate the challenges of the modern world. Through their time in the school, students will be encouraged to, and given training in how they can:

- Use devices responsibly.
- Protect personal information.
- Report harmful or suspicious content.
- Treat others with respect online.

Visitors/contractors

- Follow school ICT expectations.
- Use digital systems only for authorised purposes.

6. Online Safety Education for Students

The school provided a comprehensive programme to ensure that you people are empowered to engage positively with technology, and to evaluate the challenges it poses. Online safety learning includes training on:

- Evaluating information accuracy and media manipulation.
- Understanding digital footprints.
- Privacy, consent and data protection.
- Emotional wellbeing, healthy boundaries and peer influence.
- Ethical and responsible use of AI.

This is delivered through lessons, assemblies, Personal Development Time (PDT) and targeted interventions.

7. Education for parents/carers

The school plays an important part in the development of a community, and in that role seeks to provide parents with the support and education they need to support their children. We provide:

- Annual online safety briefings.
- Regular guidance on screen time and wellbeing.
- Termly information updates.
- Access to reputable online safety resources.
- Clear information on filtering and monitoring systems.

8. Cyberbullying prevention & response

QE does not tolerate cyberbullying, or any type of bully. In countering this, we will:

- Teach students how to identify and report harmful behaviour.
- Record, investigate and escalate incidents.
- Provide support for victims and perpetrators.
- Engage external agencies where required.

Consequences will align with the QE Positive Behaviour Policy, and may include device restrictions or disciplinary action.

9. Use of devices & mobile phones

The proliferation of devices and mobile phones has presented a number of exciting opportunities for you people, and when used well, can provide transformative learning experiences. They can also, however, be a significant distraction, and impact on the cognitive development of young minds. Therefore, we seek to draw a balance that ensures that all use of such devices is shown to promote student progress.

By students

- Phones must remain switched off and unseen during the school day.

- Only school-approved devices may be used during lessons.
- Recording others requires explicit staff permission.
- Unapproved applications or personal browsing are not permitted.

By Staff

- Staff must use strong passwords and multi-factor authentication.
- Ensure devices auto-lock and remain encrypted.
- Use school-approved communication channels only.
- Avoid storing sensitive data locally.
- Breaches may lead to disciplinary action.

10. Monitoring, filtering & security

QE uses a 1:1 device programme to ensure that it is able to comply with the highest international standards of monitoring and filtering, to ensure the safety of young people using the internet. It achieves this through a layered monitoring system that:

- Filters harmful content.
- Forbids this use of VPNs or other similar programmes aimed to subvert controls.
- Alerts DSL/IT to high-risk activity.
- Logs usage in accordance with UAE laws.
- Is reviewed annually for effectiveness.

The school may review activity on any QE-owned device or platform.

11. Incident management & response

The safety and wellbeing of young people are the paramount concerns of our whole community, and all staff have a responsibility to report any concerns immediately to the DSL. Where there is an incident, responses may include:

- Investigation and evidence gathering.

- Parent meetings.
- Behaviour-related sanctions.
- Device usage restrictions.
- Referral to external agencies (police, social services, cybercrime units).

Incidents involving indecent images of minors or threats will be escalated without delay.

12. Artificial Intelligence (AI)

QE recognises both the opportunity and risk AI presents. Through our STEAM programme and our conceptual curriculum and our Futures Programme, we seek to provide students with the opportunities to engage with generative AI in a way which supports development. Through those channels, we ensure:

- AI literacy is embedded in the curriculum.
- Ethical and responsible use.
- Prohibition of harmful or misleading AI-generated content.

Staff approval is required for AI tools involving student data.

13. Training & professional development

The digital world is fast moving and dynamics, and therefore the school seeks to ensure that staff and students have regularly updated training to ensure that they are as up to date as is possible. This training includes, but is not limited to:

- An online safety induction for all new staff.
- Annual refresher training for all staff.
- DSL and deputies undertake enhanced training every two years.
- Governors receive safeguarding and online safety updates.

14. Quality assurance & review

Whilst all staff have a responsibility to act in ways which support the aims and intention of this policy, the following staff have specific responsibility to quality assure the school's work in this area, namely;

- SLT leads an annual review of online safety provision based on feedback from staff, students, and parents informs improvement and a review of incidents in the prior year.
- The DSL completes annual digital risk assessments.
- Governors monitor and approve updates.

15. Links With Other QE Policies

- Safeguarding & Child Protection Policy
- Positive Behaviour Policy
- Data Protection & Privacy Notices
- Inclusion Policy
- ICT & Acceptable Use Agreements
- Complaints Policy
- Anti-Bullying Policy