ICT & ONLINE CONDUCT POLICY

Phoenix Private School, Doha – For Students and Staff

Effective Date: November 2025

Approved By: Senior Leadership Team

Next Review Date: November 2026

1. Mission, Vision, and Values

Mission:
To develop future leaders who are able to make positive changes throughout the world. We challenge today to create a better tomorrow.
Vision:
To prepare a generation of Successful Learners, Confident Individuals, Responsible Citizens and Effective Contributors.
Values:

- Perseverance
- Honesty
- Originality
- Enrichment
- Nurturing
- Inspiration
- eXcited to learn

2. Policy Statement

At **The Phoenix Private School (PPS)**, safeguarding and promoting the welfare of all students is our highest priority. Every child has the right to feel safe, valued, and protected from harm.

Our safeguarding culture is grounded in our **PHOENIX values**:

- **Perseverance** – striving to do the right thing online and offline.
- **Honesty** – being truthful and responsible in digital communication.
- **Originality** – using technology creatively and safely for learning.
- **Enrichment** – enhancing learning while respecting others' rights.
- **Nurturing** – supporting peers and contributing to a safe community.
- **Inspiration** – promoting positive digital role modelling.
- **Excitement to Learn** – embracing opportunities for safe, responsible technology use.

This policy reflects the ethical and professional standards of the **Qatari Ministry of Education and Higher Education (MOEHE)** and international best practice under **Keeping Children Safe in Education (KCSIE, 2025)**.

We operate a **whole-school approach to safeguarding**, recognising that protecting children is everyone's responsibility, both inside and outside the school environment, including online spaces.

3. Aims and Objectives

The aims of this policy are to:

- **Prevent harm** by embedding a safe digital culture throughout the school.
- **Identify children at risk** and respond swiftly to online or ICT-related concerns.

- **Ensure all staff, students, and parents** understand their responsibilities when using technology.
- **Support children's welfare and emotional wellbeing**, including protection from cyberbullying, harassment, or reputational harm.
- **Work collaboratively** with parents, MOEHE, and relevant agencies to protect students.
- **Promote positive behaviour and safe relationships** in alignment with our Behaviour Policy.
- **Safeguard students' images, reputation, and personal data**, ensuring appropriate use of media and online content.
- **Extend the scope of safe conduct beyond school premises**, addressing online activity that may harm students, staff, or the school community.

4. Scope

This policy applies to:

- All students, staff, parents, and volunteers.
- All school ICT systems and devices, including personal devices used on campus or for school-related work.
- Online behaviour outside school hours if it impacts the safety, welfare, or reputation of students, staff, or the school.
- Use of images, video, or audio recordings involving students or school premises.

5. General ICT and Internet Use

5.1 Network and Device Use

Students must:

- Only access the school network using their personal ID and password.
- Ask staff for assistance if login details are forgotten.
- Always log off after use.
- Not attempt to alter computer settings or install unauthorized software.
- Only use computers for educational purposes, homework, or school-approved tasks.
- Report any technical issues or unexpected pop-ups to staff immediately.

5.2 Internet Safety

- Internet use must be supervised and approved by a teacher.
- Students must not access inappropriate or offensive content.
- Attempts to bypass school filtering systems are strictly prohibited.
- Personal details of themselves or others must never be published online.
- Foul language, abusive messaging, or harmful posts are forbidden on school platforms.
- Reporting inappropriate content must be immediate to a teacher.

6. Digital Communication Platforms

Students must:

- Use of **MS Teams, email**, or other school-approved platforms responsibly.
- Never send messages intended to harm, bully, or upset others.
- Maintain respectful language and behaviour in all digital interactions.
- Not add staff to personal social media accounts (Facebook, Instagram, Twitter, etc.).
- Report any inappropriate messages or contacts to the school safeguarding lead.

7. Use of Images, Video, and Media

- Students must **never capture, share, or manipulate images or videos of other students without consent**.
- Images or recordings must not be used to harass, embarrass, or damage the reputation of another student or the school.
- Posting content that harms the school's reputation or links the school to inappropriate material is prohibited.
- The school reserves the right to take disciplinary action for any misuse of images or media, whether online or offline, and inside or outside school.
- Staff must adhere to **MOEHE regulations and Qatari law** regarding photography and media use.

8. Cyberbullying and Electronic Harassment

Cyberbullying includes:

- Online threats, harassment, or humiliation.
- Sharing private information without consent.
- Posting harmful content about other students or the school.

Actions:

- All incidents will be recorded, investigated, and addressed according to the school Behaviour Policy.
- Students involved will receive support, and disciplinary action may be applied.
- Severe cases will be referred to **MOEHE or relevant authorities**.

9. Off-Campus Online Conduct

- Students' online actions outside school must **not harm other students, staff, or the school community**.

- Harmful activity includes online bullying, defaming the school, or sharing inappropriate content.
- Reports of off-campus online harm will be investigated and, if necessary, referred to the safeguarding lead or authorities.

10. Students with Disabilities / SEND and Vulnerable Students

- Students with SEND or chronic health conditions may face additional risks online.
- Staff will provide extra support to identify and respond to abuse, neglect, or harassment.
- Behavioural indicators of harm must not be misattributed to disabilities.
- Safeguarding plans will consider specific barriers to reporting and communication.

11. Roles and Responsibilities

11.1 Staff

- Maintain vigilance for risks of online harm, cyberbullying, or misuse of media.
- Report any concerns immediately to the **Designated Student Protection Officer (DSPO)**.
- Model responsible digital behaviour at all times.

11.2 Students

- Follow the rules set out in this policy and the Student Contract.
- Respect peers' privacy and rights.
- Report any incidents of cyberbullying, harassment, or misuse of media.

11.3 Parents / Guardians

- Support the school's ICT and Online Conduct Policy at home.
- Encourage safe and responsible use of technology.
- Report concerns to school staff promptly.

11.4 School Leaders

- Ensure alignment with **KCSIE 2025**, **MOEHE Student Protection Policy**, and internal Behaviour & Safeguarding policies.
- Monitor implementation and review the policy annually.

12. Reporting, Monitoring, and Record Keeping

- All online incidents, misuse of media, or breaches of policy must be **reported to the DSL**.
- The school maintains secure and confidential records in accordance with **Qatar Data Protection Law (Law No. 13 of 2016)**.
- Serious incidents may involve MOEHE, police, or other authorities.
- Staff and students will receive **regular training on safeguarding and online safety**.

13. Enforcement and Sanctions

- Breaches of this policy may result in:
  - Verbal warnings or restorative approaches
  - Temporary or permanent restriction of ICT access
  - Referral to DSPO, MOEHE, or external authorities for severe cases
- Disciplinary measures are consistent with the **School Behaviour Policy** and **MOEHE guidance.**

14. Policy Review

- This policy will be **reviewed annually** and updated in line with:
  - **KCSIE 2025** guidance.
  - **MOEHE Student Protection and Care Policy 2025.**
  - School Behaviour Policy updates.
  - Emerging risks in online safety and technology.