



PHILIPPINE-EMIRATES PRIVATE SCHOOL L.L.C.

Abu Dhabi, United Arab Emirates

DIGITAL SAFETY AND RESPONSIBLE USE POLICY

1. Introduction

Philippine Emirates Private School (PEPS) recognizes that digital technology plays an essential role in teaching, learning, communication, and school operations. PEPS is committed to ensuring that all digital platforms, devices, systems, and online interactions are used safely, responsibly, ethically, and in alignment with ADEK safeguarding and digital safety requirements.

This policy establishes clear standards for the safe and responsible use of digital technology by students, staff, parents, contractors, and visitors while protecting students from online harm, cyber risks, abuse, exploitation, and inappropriate digital behavior.

This policy is connected to the PEPS Safeguarding Policy, particularly the “Digital Safety” section on pages 9–10.

2. Purpose

The purpose of this policy is to:

- Promote safe and responsible digital behavior.
- Protect students from online abuse, cyberbullying, exploitation, and harmful content.
- Ensure proper use of school digital systems and devices.
- Establish clear digital safeguarding responsibilities.
- Maintain confidentiality, privacy, and data protection.
- Support digital literacy and cyber awareness.
- Align PEPS practices with ADEK safeguarding and digital safety expectations.

3. Scope

This policy applies to:

- All PEPS students
- Teaching and non-teaching staff
- School leadership
- Contractors and visitors using school systems
- Parents/guardians accessing school platforms
- All digital devices connected to PEPS systems
- All school-managed digital platforms and communication systems

This policy applies both:

- On-campus and off-campus



- During face-to-face learning
- During online or hybrid learning
- During school trips and extracurricular activities involving digital devices

4. Policy Statement

PEPS maintains a zero-tolerance approach toward:

- Cyberbullying
- Online harassment
- Digital abuse or exploitation
- Unauthorized recording or sharing of content
- Access to harmful or inappropriate content
- Misuse of school technology systems
- Breach of privacy or confidentiality
- Sharing false, offensive, discriminatory, or harmful content

All members of the PEPS community are expected to act responsibly and maintain respectful, safe, and professional digital behavior at all times.

5. Digital Safety Principles

PEPS commits to the following digital safety principles:

5.1 Student Protection

Students must be protected from:

- Cyberbullying
- Online predators
- Exposure to inappropriate materials
- Identity theft
- Digital harassment
- Online scams and phishing
- Unauthorized online contact

5.2 Responsible Use

Technology must be used only for:

- Educational purposes
- Official communication
- Authorized school activities



5.3 Confidentiality and Privacy

All personal information and school data must be handled securely and confidentially.

5.4 Digital Citizenship

Students and staff must demonstrate:

- Respectful online communication
- Ethical digital behavior
- Responsible social media usage
- Awareness of digital footprints

6 Acceptable Use of Technology

6.1 Students

Students are expected to:

- Use school internet and devices responsibly.
- Access only educational and authorized content.
- Respect others during online communication.
- Report unsafe or suspicious online behavior immediately.
- Keep passwords confidential.
- Follow teacher instructions during digital activities.

Students must NOT:

- Access inappropriate websites or content.
- Use VPNs or methods to bypass internet filtering.
- Download unauthorized software or applications.
- Record or photograph others without permission.
- Share offensive, violent, or inappropriate content.
- Use fake accounts or impersonate others.
- Engage in cyberbullying or online harassment.

6.2 Staff

Staff must:

- Maintain professional boundaries online.
- Use official school communication platforms only.
- Protect student confidentiality and records.
- Monitor students during digital learning activities.
- Immediately report digital safeguarding concerns.



Staff must NOT:

- Communicate privately with students through personal social media accounts.
- Share confidential student information.
- Post student images without authorization.
- Use school systems for inappropriate activities.

7 Internet and Network Safety

PEPS shall implement:

- Filtered and monitored internet access
- Firewall and antivirus protection
- Restricted access to harmful websites
- User authentication systems
- Secure Wi-Fi management
- Network monitoring and activity logging

Network Authentication and Access Control

Philippine Emirates Private School (PEPS) utilizes the **TP-Link Omada Controller System** for centralized network management, monitoring, and internet authentication.

All faculty and staff members are provided with a unique username and password to securely access the school internet and wireless network services. User authentication credentials are individually assigned and monitored by the IT Department to ensure accountability, secure access, and protection against unauthorized network usage.

The Omada Controller system enables PEPS to:

- Monitor connected users and devices
- Restrict unauthorized access
- Maintain secure internet connectivity
- Apply internet filtering and access control policies
- Detect suspicious or abnormal network activity
- Maintain activity logs for digital safeguarding and cybersecurity purposes

Students are only permitted to access authorized internet services using approved school devices and designated educational areas under teacher supervision.

Unauthorized sharing of login credentials, bypassing authentication systems, or attempting to gain unauthorized network access is strictly prohibited and may result in disciplinary action.

All internet usage may be monitored to ensure compliance with school safety requirements and ADEK digital safeguarding expectations.

8 Digital Safeguarding Measures



PEPS shall maintain the following safeguarding controls:

8.1 Cyberbullying Prevention

- Awareness campaigns
- Reporting procedures
- Student guidance sessions
- Investigation protocols
- Support for affected students

8.2 Device Security

All school devices shall:

- Have updated antivirus protection
- Use secure passwords
- Receive regular updates and audits
- Be monitored by the IT Department

8.3 Monitoring and Reporting

Suspicious online activities may be:

- Investigated
- Documented
- Reported to school leadership and safeguarding officers

8.4 Digital Supervision

Teachers must actively supervise students during:

- Computer laboratory use
- Online learning
- Digital research activities
- Use of school devices

9 Social Media Guidelines

Students and staff must:

- Maintain respectful communication online.
- Avoid posting harmful or offensive content.
- Protect personal and school reputation.
- Respect privacy and confidentiality.

The following are prohibited:

- Posting student conflicts online
- Sharing inappropriate videos or images
- Online threats or harassment



- Spreading rumors or false information
- Unauthorized use of PEPS logos or branding

10 Data Protection and Privacy

PEPS shall:

- Protect personal data of students and staff.
- Restrict access to confidential information.
- Store records securely.
- Obtain parental consent for student images and educational publications.

All staff must comply with confidentiality and safeguarding requirements regarding digital records and communications.

This aligns with the safeguarding policy's data protection requirements.

11 Mobile Phone and Personal Device Use

Students

- Students must follow PEPS mobile phone procedures.
- Mobile phones may be collected during school hours when required.
- Students must not use devices to record incidents, emergencies, or other students without permission.
- Devices must not disrupt learning or safety procedures.

Staff

- Staff must model responsible digital behavior.
- Personal devices must not interfere with supervision responsibilities.

12 Digital Safety Education

PEPS shall provide regular digital safety education through:

- Classroom discussions
- Assemblies
- Awareness campaigns
- Parent orientations
- Cybersecurity workshops
- Safeguarding training

Topics may include:

- Cyberbullying
- Online predators
- Password security
- Digital footprints
- Social media safety
- Responsible online communication





- Data privacy

This aligns with PEPS safeguarding digital literacy education requirements.

13 Reporting Digital Safety Concerns

Any student, staff member, or parent who becomes aware of:

- Cyberbullying
- Online threats
- Inappropriate digital behavior
- Unauthorized recording
- Suspicious online activity
- Data breaches

must immediately report the concern to:

- Class Adviser
- IT Department
- Designated Safeguarding Lead (DSL)
- School Leadership

All reports shall be handled confidentially and investigated appropriately.

14 Disciplinary Actions

Violations of this policy may result in:

- Warning notices
- Parent meetings
- Temporary suspension of digital access
- Confiscation of devices
- Behavioral sanctions
- Safeguarding intervention
- Further disciplinary action in accordance with PEPS policies and ADEK regulations

Serious violations may be referred to appropriate authorities when necessary.

15 Roles and Responsibilities

School Leadership

- Ensure policy implementation and ADEK compliance.
- Support safeguarding and digital safety initiatives.

IT Department

- Maintain network security and monitoring systems.
- Conduct device audits and cybersecurity measures.

Safeguarding Committee

- Investigate digital safeguarding concerns.



- Coordinate student protection measures.

Teachers

- Supervise students during digital activities.
- Promote responsible digital behavior.

Parents

- Support safe technology use at home.
- Monitor student online activities responsibly.

Students

- Follow digital safety expectations.
- Report unsafe online behavior immediately.

16 Policy Review

This policy shall be reviewed:

- Annually
- After safeguarding incidents
- Following ADEK updates
- Following major technological changes
- Feedback from students, parents, and staff may be considered during policy review.

17 References

- ADEK Student Protection and Safeguarding Requirements
- ADEK Digital Safety Expectations
- PEPS Safeguarding Policy – Digital Safety Section (Pages 9–10)
- UAE Cybercrime Laws
- UAE Data Protection and Privacy Regulations



18 Document Review and Approval

Function	Name	Designation	Date	Signature
Final Approval	Jeselle E. Fidelino	School Principal	September 30, 2025	
Document Review	Bernardo T. Cinco	Admin Director	September 30, 2025	
Contributor Reviewer	Dennis S. Canicon	Academic Coordinator	September 30, 2025	
Contributor Reviewer	Ma. Teresa A. Postadan	School Nurse	September 30, 2025	
Contributor Reviewer	Jenalyn T. Senatin	Guidance Counselor	September 30, 2025	
Contributor Reviewer	Rosavic A. Muniyandi	Academic Coordinator	September 30, 2025	
Contributor Reviewer	Anthony A. Fidelino	HSE Officer	September 30, 2025	
Contributor Reviewer	Sheryl R. Mendoza	Wellbeing Coordinator	September 30, 2025	
Document Producer	Anthony A. Fidelino	IT Coordinator	September 30, 2025	