Digital Safety & Social Media Policy

1. Purpose

The purpose of this policy is to ensure that all members of the school community — students, staff, and parents — use **digital devices, the internet, and social media responsibly and safely**. It aims to:

- Protect students from **online risks**, including cyberbullying, exploitation, and exposure to harmful content.
- Promote **responsible and ethical use** of digital platforms.
- Support compliance with **UAE cyber laws**, **ADEK student protection standards**, and **school IT guidelines**.

2. Scope

This policy applies to:

- All **students, staff, parents, and visitors** using school-owned or personal digital devices within school premises.
- All **online communications, emails, educational apps, and social media activities** conducted using the school's name, logo, or resources.
- All digital interactions related to **school operations, teaching, and learning**.

3. Policy Statement

The school is committed to maintaining a **safe digital environment** where technology supports learning and communication without compromising the **privacy, dignity, or safety** of any individual. The school will:

- Educate all users on **safe and ethical online behavior**.
- Monitor and manage the use of **school networks and devices**.
- Act promptly against **cyberbullying, harassment, or misuse of digital platforms**.
- Protect the **digital wellbeing and privacy** of students and staff.

4. Legal and Regulatory Framework

This policy aligns with the following regulations and frameworks:

- **ADEK Student Protection Policy (Version 1.1, 2024)**
- **UAE Cybercrime Law – Federal Decree-Law No. 34 of 2021**
- **ADOSH 4.0 – IT and Digital Communication Safety**
- **UAE Penal Code – Federal Law No. 3 of 1987**
- **UAE Data Protection Law – Federal Decree-Law No. 45 of 2021**
- **ISO/IEC 27001 – Information Security Management Systems**

5. Objectives

- Promote **safe and respectful digital behavior** among students and staff.
- Protect school data, networks, and systems from **unauthorized access and misuse**.
- Prevent **cyberbullying, harassment, and exploitation**.
- Ensure that all digital communications uphold **professional and ethical standards**.
- Support a culture of **digital citizenship and accountability**.

6. Roles and Responsibilities

6.1 School Principal / Director

- Ensure full compliance with ADEK and UAE cyber safety laws.
- Approve digital safety programs and online communication guidelines.
- Authorize the use of school social media accounts and official digital communications.

6.2 OSH Department / IT Officer

- Monitor online safety practices and investigate digital incidents.
- Maintain records of reported digital misconduct.

- Provide annual digital safety training to staff and students.
- Implement technical controls (firewalls, filters, and access permissions).

6.3 Teachers and Staff

- Model **ethical digital behavior** at all times.
- Use only approved platforms for teaching and communication.
- Protect student data and privacy in online materials.
- Report any incident of cyberbullying or inappropriate digital behavior.

6.4 Students

- Use the internet and devices **responsibly and respectfully**.
- Never share personal information, passwords, or images online.
- Report suspicious messages or online behavior to a teacher or counselor.
- Refrain from taking photos or videos of others without permission.

6.5 Parents and Guardians

- Support safe technology use at home.
- Monitor their child's online behavior and screen time.
- Report any online safety concerns to the school.

7. Acceptable Use Guidelines

- School devices and networks must be used **for educational purposes only**.
- Students must not access, share, or download inappropriate material.
- Use of social media must **respect the reputation of the school and its members**.
- Confidential information must never be disclosed or discussed online.
- Personal communication during lessons or work hours is not permitted.

8. Cyberbullying Prevention

- Cyberbullying includes sending harmful messages, posting offensive content, spreading rumors, or impersonating others online.
- The school maintains **zero tolerance** toward any form of cyberbullying.
- Victims will receive **counseling and support**, while offenders may face disciplinary action, including suspension or referral to authorities.
- All cyberbullying cases must be documented using the **Digital Incident Report**

- **9. Social Media Conduct**

For Staff:

- Only authorized staff may post on **official school accounts**.
- Posts must reflect professionalism, accuracy, and cultural sensitivity.
- Personal opinions should not be represented as school views.
- Staff should not share student photos without written parental consent.

For Students:

- Students may not create or post content representing the school without permission.
- Inappropriate or harmful online content related to school life is prohibited.
- Respectful communication must be maintained on all digital platforms.

10. Data Protection and Privacy

- Personal information (e.g., student names, grades, photos) must be stored securely.
- Data sharing outside the school requires **parental and management approval**.
- Access to school systems must be password-protected and regularly reviewed.
- Users must log off computers and devices when unattended.

11. Online Learning and Remote Access

- Online lessons must be conducted through **school-approved platforms** (e.g., MS Teams, Google Classroom).
- Cameras may be used during virtual learning only under supervision.
- Teachers must maintain professional backgrounds and communication standards.
- Students must attend virtual classes dressed appropriately and behave respectfully.

12. Incident Reporting and Investigation

- All digital or cyber incidents must be reported immediately to the **OSH or IT Officer**.
- The **Digital Safety Incident** will be used to document the event.
- Investigations will determine cause, impact, and preventive measures.
- Repeated or serious violations may be reported to **ADEK or UAE authorities**.

13. Training and Awareness

- Annual **Digital Safety Awareness Programs** shall be conducted for students, parents, and staff.
- Specialized sessions on **cyber ethics, privacy, and online behavior** will be provided.
- Students will participate in **Safer Internet Day** and digital wellbeing campaigns.

14. Disciplinary Actions

Violations of this policy may result in:

- Verbal or written warning.
- Restriction of digital access or device confiscation.
- Suspension or termination of employment (for staff).
- Reporting to law enforcement if UAE Cybercrime Law is breached.

15. Monitoring and Review

- The OSH Department will conduct **quarterly audits** of network safety and social media use.
- This policy will be reviewed annually or after any serious cyber incident.
- Updates will reflect any **ADEK or UAE legal amendments**.

16. References

- **ADEK Student Protection Policy (Version 1.1, 2024)**
- **UAE Cybercrime Law – Federal Decree-Law No. 34 of 2021**
- **ADOSH 4.0 – Digital and Communication Safety Standards**
- **UAE Data Protection Law – Federal Decree-Law No. 45 of 2021**
- **ISO/IEC 27001 – Information Security Management Systems**
- **UNICEF Digital Safety Framework for Schools (2023)**

Principal		OSH officer
Sister Claudette Dababneh		Marwah Aljammali