EV-S.2224
SMCS

Policy

December 2024

EVEREST SCHOOL

EVEREST SCHOOL

Table of contents

Everest Schools (EV-S) has implemented the SMCS policy (Minor Safety and Secure Communication) to ensure the protection of children when using information and communication technologies (ICT). This policy establishes clear protocols and specific responsibilities to safeguard minors when accessing digital tools. It focuses particularly on securing online interactions in the educational context, ensuring that students are protected from risks associated with internet and digital platform use, while promoting a safe and responsible learning environment.

1. Objectives of the SMCS policy

- **Ensuring the Protection of Minors in the Use of Digital Technologies**

This involves implementing measures to safeguard children when using digital tools such as computers, smartphones, and the Internet. These measures include:

✓ Parental Controls: Utilizing software and applications to restrict children's access to certain content.

✓ Content Filtering: Applying filters to block access to inappropriate or harmful websites.

✓ Monitoring: Supervising children’s use of technology to detect and prevent risky behavior or exposure to harmful content.

- **Guaranteeing a Secure Online and Offline Environment**

Creating safe spaces where students can interact and learn without fear is essential:

✓ Safety Policies: Developing clear policies for online and offline safety, including protocols for reporting and addressing abuse.

✓ Staff Training: Ensuring that teachers and school staff are trained to recognize and manage risk situations.

✓ Physical and Digital Security: Protecting students’ personal information and ensuring the security of school infrastructure.

- **Educating Children and Youth About the Risks Associated with Digital Tool Use**

Students must understand the potential dangers of using technology:

✓ Educational Programs: Developing training programs to raise awareness about cyberbullying, sharing personal information, and accessing inappropriate content.

✓ Interactive Workshops: Organizing interactive sessions where students learn how to navigate the Internet safely.

✓ Educational Resources: Providing materials such as guides and educational videos to help children understand and avoid online risks.

- **Providing a Legal and Ethical Framework for Students’ Online Activities**

It is vital to ensure that students' online activities are governed by clear and ethical rules:

✓ Clear Regulations: Establishing rules that define acceptable and unacceptable online behavior.

✓ Privacy Protection: Ensuring that students' data is safeguarded and their privacy is respected.

- ✓ Digital Responsibility: Promoting responsible and ethical use of technology, raising students' awareness of the consequences of their online actions.

These measures and initiatives help create a secure and educational environment for students while preparing them to use digital technologies responsibly and safely.

2. Security Measures Implemented

- Internet Filtering: Implementation of filtering systems to block access to inappropriate or harmful websites for children.
- Online Supervision: Monitoring students' online activities to detect suspicious or inappropriate behavior.
- Protection of Personal Data: Ensuring that students' personal information is safeguarded in compliance with data protection regulations (e.g., GDPR).
- Account and Credential Management: Requiring students to use secure accounts and credentials to access the school's online platforms.

3. Training and Awareness for Students

- ✓ **Online Safety Education:** An initiative aimed at equipping students with the skills and knowledge needed to navigate the internet safely and responsibly.
  - ✓ Interactive Workshops: Led by trained experts or teachers, these workshops cover topics such as creating secure passwords, recognizing malicious links, and managing privacy settings.
  - ✓ Educational Resources: Distribution of illustrated guides or educational videos tailored to students' age to explain essential concepts.
  - ✓ Practical Simulations: Exercises where students learn to recognize risky situations, such as phishing emails or suspicious requests.
  - ✓ Promotion of Responsible Behavior: An initiative to encourage respectful and responsible use of digital tools, covering the following themes:
    - ▪ Cyberethics: Discussions about respecting others online, such as the importance of avoiding insults or rumors.
    - ▪ Digital Identity Management: Raising awareness about the impact of social media posts, especially regarding privacy and future reputation.
    - ▪ Cyberbullying Prevention: Learning strategies for responding to or reporting harmful behavior, with clear roles for teachers and students in addressing these issues.
  - ✓ Recognizing Risks: An introduction to help students recognize and proactively manage online dangers, particularly the following risks:
    - ▪ Cyberbullying: Identifying signs of abusive behavior, whether directed at oneself or a peer, and knowing where to seek help.
    - ▪ Phishing: Explaining techniques used by fraudsters to obtain personal information and how to spot them (suspicious URLs, urgent requests, etc.).

- Inappropriate Content: Learning how to report disturbing images, videos, or messages on various digital platforms.

The school plans to implement this concretely through:

Inclusion in the Curriculum and Parental Involvement: Integrating online safety and responsible behavior sessions into regular courses such as technology, citizenship, or social studies, and organizing similar sessions for families to help them support their children at home.

4. Roles and Responsibilities

- School Responsibilities: Ensure the implementation of the SMCS policy and provide ongoing training for teachers and staff on digital safety.
- Parental Responsibilities: Parents are encouraged to remain vigilant about their children's use of technology at home and to ensure they use the internet safely and appropriately.
- Student Responsibilities: Students are expected to follow the rules set by the school regarding the use of digital technologies and report any suspicious activity.

5. Managing Security Incidents

- **Response to Incidents Involving Minors' Safety**

The incident response policy ensures a swift, effective, and legally compliant intervention. It includes:

- ✓ Reporting: Identifying the incident, notifying the responsible parties, and alerting the authorities if necessary.
- ✓ Protection: Removing the child from danger, providing psychological support, and ensuring confidentiality.
- ✓ Investigation: Conducting a thorough investigation, documenting the facts, and informing parents according to legal protocols.
- ✓ Corrective Measures: Applying appropriate sanctions and updating policies to prevent future incidents.
- ✓ Communication: Informing staff and preparing an official statement if required.
- ✓ Prevention: Training staff, organizing simulations, and auditing existing systems.

- **Incident Reporting**

Everest Schools has implemented a clear system enabling students, parents, or staff to report any digital security violations:

- ✓ Digital Reporting Box on Kinderpedia: This application provides direct and confidential access to alert the responsible authorities automatically.
- ✓ Secure Email Address: A dedicated secure email (e.g., ...) where users can send their reports.
- ✓ Emergency Phone Line: The school’s telephone line can be used to report any digital security issues immediately.

- ✓ Paper and Digital Forms: Everest Schools provides a secure dropbox at the reception for submitting anonymous paper reports.
- ✓ Digital Security Committee: The school has appointed a digital security committee, comprising two teachers, two students, and the academic assistant, to review incidents, discuss issues, and propose solutions.
- ✓ Training and Awareness: Everest Schools organizes training and awareness sessions for students and staff to help them identify and report digital security incidents.

6. Data Protection and Confidentiality

a. **Confidentiality of Information**:

The policy ensures strict management of students' data in compliance with national and international data protection laws, such as Law 09-08 in Morocco and the GDPR for institutions following European standards.

b. **Collection of Student Data**:

Everest Schools collects only the data necessary for educational and administrative purposes.

c. **Informed Consent**:

- ✓ Parents or legal guardians must provide explicit consent through a form detailing the data collected and its intended use.
- ✓ Transparency is ensured through a privacy policy available online and upon request.

d. **Secure Storage of Data**:

To protect student data from unauthorized access, loss, or theft, Everest Schools has:

- ✓ Set up a secure room equipped with cameras to store student records.
- ✓ Utilized the Kinderpedia application, designed to ensure that only authorized individuals have access to student information.

e. **Use of Data**:

Everest Schools guarantees that student data is used only within a legitimate and predefined framework.

- ✓ **Authorized Purposes**: Include administrative and academic management, such as registrations, evaluations, and report cards, as well as communication with parents and pedagogical follow-up, particularly for the implementation of personalized educational plans.
- ✓ **Strict Prohibitions**: Student data cannot be sold, shared, or used for commercial purposes. Additionally, the use of student photos or information in publications requires explicit consent from parents.

f. **Rights of Parents and Students**:

Everest Schools ensures data transparency and control, offering the following rights to the concerned parties:

- ✓ **Access**: Parents can request a copy of the data collected about their child.

- ✓ **Rectification**: Parents can request corrections in case of errors.
- ✓ **Deletion**: Parents can request the deletion of data when it is no longer necessary.

g. **Secure Sharing of Information**:

Student information can only be shared with authorized parties and in a secure manner, ensuring the confidentiality and safety of the data.

The SMCS policy aims to create a safe, ethical, and responsible environment for children and youth, preparing them to navigate the digital world in an informed and respectful manner.