Policy Title:
Online Safety Policy

Approval Authority: *AIS Board of Trustees*
Compliance: *In accordance with ADEK guidelines*

Effective Date: *August 2024*
Revision Date: *May 2025*
Compliance Date: *AY 2025/26 (Fall term)*

INTRODUCTION

With the increasing time students spend on digital media for both learning and leisure, it is essential to ensure their safety in online environments. This policy aims to safeguard students by educating them about potential risks and promoting responsible, informed use of the internet and electronic communications. It provides clear guidelines for students, staff, and parents to help ensure that students engage in safe and constructive online activities. The policy is aligned with the AIS Student Behavioral Policy, Student Protection Policy, Anti-Bullying Policy, and Health and Safety Policy.

PURPOSE

- Ensure that students, parents, and staff understand the potential risks associated with internet use and are equipped with the knowledge and tools to use it safely and responsibly.
- Raise awareness among students, parents, and staff about cyberbullying and its potential emotional, psychological, and social impact on victims.
- Ensure that all members of the school community are familiar with the procedures for reporting incidents of cyberbullying and understand the school's approach to supporting those affected.

DEFINITIONS

- **Abuse (Online Context):** Any harmful behavior carried out through digital means, such as cyberbullying, harassment, threats, or exploitation that causes emotional, psychological, or reputational harm.
- **Digital Citizenship:** The responsible, respectful, and ethical use of technology and the internet, including understanding digital rights and responsibilities, online etiquette, and the impact of one's digital behavior.
- **Filtering and Monitoring:** Technical safeguards used by the school to restrict access to harmful or inappropriate online content and to track usage of school networks to ensure a safe digital environment.

- **Inappropriate Content:** Any online material that is not suitable for students, including content that is violent, sexually explicit, discriminatory, offensive, or otherwise harmful or upsetting.
- **Offensive Material:** Content that includes insults, threats, hate speech, or inappropriate language or imagery that may harm, offend, or disrespect others.
- **Online Etiquette / Netiquette:** The set of expected behaviors for respectful and appropriate communication in online environments, including using polite language, respecting others' privacy, and avoiding offensive content.
- **Online Platforms:** Digital tools or websites used for communication, learning, collaboration, or sharing content, including those officially approved by the school (e.g., learning management systems, class portals).
- **Online Safety:** The practice of protecting users, especially children and young people, from risks and harm when using the internet and digital technologies, including exposure to inappropriate content, cyberbullying, and privacy breaches.
- **Parental Controls:** Software or device settings that allow parents to monitor and manage their child's internet usage, including controlling screen time, restricting access to certain content, and tracking activity.
- **Personal Information:** Any data that can be used to identify an individual, such as full name, address, phone number, email, login credentials, or personal photos and videos.
- **School-Approved Platforms:** Digital applications, websites, or tools officially authorized by the school for instructional or communication purposes and considered safe for student use.

POLICY

1. **School Responsibilities:** The school is committed to maintaining a safe and responsible digital environment. The following statements outline the school's role in promoting online safety, educating the community, and responding to online risks.

    - The school will ensure that the Online Safety Policy and all related policies are accessible to all members of the school community through the school website.
    - The school will promote a positive and responsible digital culture by integrating digital citizenship education into the curriculum to help students develop safe, ethical, and informed online behaviors.
    - The school will provide students with clear and age-appropriate guidance on the safe use of technology, including how to protect their personal data, make responsible choices online, and report cyberbullying or other forms of abuse.
    - The school will offer workshops and resources to parents to support their understanding of online safety and their role in monitoring and guiding their children’s digital activity.
    - The school will ensure that all staff members understand their responsibilities in promoting online safety and are confident in recognizing, addressing, and reporting cyberbullying and online risks.

- The school will ensure that staff model safe, responsible, and professional use of technology in accordance with the school's Code of Conduct and online safety expectations.
- The school will foster a culture of openness and safety in which students and staff feel confident to report concerns related to online behavior without fear of retaliation.
- The school will respond promptly and appropriately to all incidents of cyberbullying, regardless of where they occur, and will take action in accordance with the Anti-Bullying Policy, Behavior Policy, and Child Protection Policy.
- Staff members who become aware of a cyberbullying incident must take immediate action by advising the student to save any relevant evidence and reporting the matter to school leadership without delay.
- The school will provide opportunities for students to contribute to online safety awareness through student-led initiatives, peer advocacy, or digital leadership roles.
- The IT Support team will implement and maintain appropriate filtering and monitoring systems to block access to harmful or inappropriate content and support a safe and secure digital learning environment.

2. **Student Responsibilities:** To ensure their safety and well-being in digital environments, students are expected to act responsibly and follow all school guidelines related to online behavior. The responsibilities outlined below aim to help students navigate the internet safely, protect their personal information, and respond appropriately to online risks such as cyberbullying and harmful content.

   - Students are expected to respect others online and demonstrate good digital etiquette. They must communicate in a polite, responsible, and appropriate manner. Offensive, threatening, or disrespectful communication is considered a serious offense.
   - Students must be cautious about who they interact with online and what personal information they share. They should only connect with trusted individuals and avoid unfamiliar contacts.
   - Students must not share personal information—including login credentials, passwords, phone numbers, or home addresses—without the permission of a parent or guardian.
   - Students must not visit unauthorized or inappropriate websites that are not approved by the school or their teacher.
   - Students must not respond to messages from unknown individuals or to abusive or suspicious emails.
   - Students must report any situation where they feel unsafe or uncomfortable online to a trusted adult (e.g., parent, teacher, or counselor) immediately.
   - Students must not engage in any form of cyberbullying. Cyberbullying—including teasing, exclusion, threats, or sharing hurtful content—is a serious offense and will result in disciplinary action.
   - Students who are victims of cyberbullying must save the evidence and report it immediately. They should not respond to the bully and must keep all messages or screenshots until they have shared them with a parent or staff member.
   - Students must follow all online safety rules, protocols, and digital conduct expectations provided by their teachers and the school.

3. **Parent Responsibilities:** Parents play a vital role in safeguarding their children's digital experiences. The responsibilities below are intended to support parents in guiding their children's safe use of technology, monitoring their online activity, and working in partnership with the school to prevent and respond to cyber-related risks, including cyberbullying and exposure to inappropriate content.

    - Parents are expected to attend school-provided information sessions on online safety. These sessions equip parents with the knowledge and tools needed to support their children's safe and responsible use of technology.
    - Parents must ensure their children understand the school's policy on cyberbullying, including its consequences and related legal implications.
    - Parents must educate their children about the risks of digital technology and encourage the development of safe, healthy, and balanced online habits.
    - Parents are responsible for actively monitoring their child's online activity. This includes regularly reviewing their digital behavior, the platforms they use, and the people they interact with.
    - Parents are encouraged to install parental control software on their child's devices to monitor online activity, set usage limits, and restrict access to inappropriate content.
    - Parents should have regular discussions with their children about network etiquette, clearly defining what types of online behavior are acceptable and promoting the responsible use of time spent online.
    - Parents must ensure their children do not share personal information—such as passwords, addresses, or contact details—through any online platform.
    - Parents must stay alert to signs of cyberbullying or exposure to inappropriate content. Ongoing conversations with their children are essential to identifying and addressing concerns early.
    - If a child reports any form of cyberbullying or inappropriate communication involving AIS students or school-approved platforms, parents must immediately inform the Head of Grade. All relevant evidence (e.g., screenshots or messages) must be preserved before any content is deleted. Refer to the AIS Anti-Bullying Policy for additional guidance.