POLICY
NETWORK SAFETY POLICY

*** Basis for policy development:**

- Based on the mission and educational objectives of the school, as follows:

+ In a world that is developing towards multilateral cooperation, the primary mission of the Asia International School is to encourage and motivate students to transcend boundaries in order to embrace the international spirit in education, aspire to global knowledge and world peace.

+ Create appropriate teaching programs that encourage students to be disciplined, creative, critical thinkers, respecting opinions and new approaches of individuals.

+ Provide international standard learning and research facilities.

+ Provide diverse learning experiences to prepare each student for a bright future in the modern developing world.

- Based on the United Nations Convention, Vietnamese laws, Vietnamese cybersecurity laws, and specific policies/regulations of the Asia International School, including:

+ Article 54 of the Law on Children No. 102/2016/QH13 of the Vietnamese National Assembly: "Relevant agencies and organizations have the responsibility to disseminate, educate, and protect children when participating in the online environment in all forms. Parents, teachers, and caregivers are responsible for educating knowledge and guiding skills for children to protect themselves when participating in the online environment."

+ United Nations Convention on the Rights of the Child.

+ Child protection policy of the Asia International School.

+ Anti-violence/bullying regulations of the Asia International School.

+ Regulations on the use of personal electronic devices of the Asia International School.

1. OBJECTIVES OF THE POLICY

- Ensure the safety, physical and mental health of staff, teachers, employees and students using the Internet for work, teaching, learning, research, and communication purposes.

- Guide staff, teachers, employees and students in the safe use of information technology (IT), understanding and complying with the processing procedures to prevent and promptly address inappropriate behaviors in the online environment.
- Ensure consistent operation of the school with the values stated in the public directives and compliance with the regulations on cybersecurity, establishing standards in the educational environment.

2. TERMINOLOGY EXPLANATION

- Network safety refers to all information technology (IT) devices connected to the Internet, including desktops, laptops, smartphones, and tablets.
- Network safety means that each individual is protected and knows how to protect themselves from improper behaviors and violations of community standards in the online environment.
- Network safety is timely prevention of unsafe behaviors, handling and knowing how to address misconduct when violations of standards occur in the online environment within the university.

3. PRINCIPLES OF NETWORK SAFETY

The internet provides many opportunities for individuals, but it also carries various risks and challenges. Therefore, it is necessary to ensure that:

- All staff, teachers, employees and students of the school must change their names on their devices (phones, laptops, iPads, etc.) to ensure the safety of the school's network system, prevent external intrusion, and harm to the school's network system.
- All staff, teachers, employees, and students of the school are protected and know how to protect themselves from potential hazards in the online environment, especially when working and studying at the school.
- All students must be guaranteed absolute safety when using IT infrastructure within the school.
- All staff, teachers, employees, and students must be instructed and fully understand the specific procedures for behavior in the online environment.
- Students are supported to use the internet and electronic devices safely and demonstrate mutual respect.
- Parents and guardians of students are provided with guidance on ensuring network safety for their children.
- Information system security is regularly reviewed and updated.
- All usernames, login information, accounts, and passwords must be used safely and effectively.

- All personal information of staff, teachers, employees, and students must be kept confidential and only used when necessary.
- All social media platforms and new technologies must be appropriately reviewed and assessed for risks before being used in the system.
- If staff, teachers, employees and students use their 3G, 4G, or 5G networks, online filters cannot guarantee network safety in the school environment. The school cannot control and support network safety in such cases. However, students, together with their parents, have signed a commitment to this policy. If the school or teachers discover any violations by students, they will be dealt with according to the provisions of this policy. Staff, teachers, and employees are not exempt from these rules.
- If staff, teachers, employees and students use various tools, means, or software to bypass the school's online safety filters, which cannot be controlled or prevented by the current IT infrastructure of the school, they will face disciplinary action according to the procedures outlined in this policy. Non-compliance with this policy can lead to restrictions or even complete loss of access to some or all forms of technology or other disciplinary measures deemed appropriate by the school administration. There will be consequences for any individuals who do not comply with these policies. Consequences may include financial compensation for damages, denial of technology access, permanent prohibition, suspension, or expulsion (for students), or termination of employment (for staff, teachers, and employees) based on the severity of the violation and the resulting harm.

4. ROLES AND RESPONSIBILITIES OF RELATED PARTIES

The school administration

- Develop policies to ensure the school community understands and implements safety measures when operating online, prevent violations, and minimize risks that may negatively impact the school's IT infrastructure.
- Disseminate this policy to all staff, teachers, employees, and students in the school.
- Ensure transparency in reporting and handling cases related to network safety.
- Ensure that all staff, teachers, employees, and students in the school understand and effectively enforce this policy for the benefit of all of them.
- Coordinate the review, evaluate the effectiveness, and adjust the policy to keep up with the ongoing development of internet technology worldwide and the regulations of Vietnam.
- Direct the resolution of incidents related to network safety.

Child Protection Board

- Update information about risks for children in the use of IT
- Collaborate with the School Counseling Office to develop topics on responsible and effective internet usage.

- Raise awareness and support staff, teachers, employees, and students regarding issues related to network safety.
- Collaborate closely with the IT department and other departments/agencies as required.
- Ensure the appropriate and effective implementation of technical safety measures in the school's online environment (e.g., web filtering software, firewalls, antivirus software).
- Adhere to the procedures for handling incidents as specified by the school.

IT Department

Responsible for ensuring the school's IT infrastructure, security systems, and online filters are functioning properly and closely monitored, specifically:

- Ensure regular monitoring and appropriate updates of the operating system and IT devices.
- Ensure that antivirus software serves its intended purpose, is updated, and installed on all devices in the school.
- Ensure that passwords are mandatory for all users and are regularly changed.
- Ensure that administrator passwords are changed periodically and not reused within 12 months.
- Administrate and monitor the system continuously, promptly detecting security vulnerabilities to address them.
- Save all the information about problems related to network safety.

Staff, teachers, employees

- Understand that the use of devices and software connected to the school's internet is closely controlled.
- Participate in relevant training sessions and fully understand the policies regarding network safety.
- Report any incidents related to network safety to the campus management board and the child protection board.
- Promote and share appropriate practices for network safety and integrate them into the educational program.

Students

- Understand that abuse or improper use of IT devices and services will be addressed according to the regulations.
- Understand the reporting process when encountering any concerns related to online harassment within and outside the school.

- Understand the network safety policy and stay updated on risks through various means such as internal newsletters, the school website, integrated lessons, and sharing workshops conducted by counseling specialists, the child protection board, and homeroom teachers.
- Understand the regulations and policies regarding the use of personal electronic devices in the school.

Parents/Guardians

- Are updated about the university's network safety policy.
- Provide support to empower children when they are granted rights.
- Understand the policy regarding the use of personal electronic devices issued by the school and support to students to engage in diverse learning activities.
- Cooperate with homeroom teachers and school administration to monitor the enforcement of network safety requirements for students at school and home.

Entering/Exiting the campus:

- If visitors use the school's IT infrastructure, they must comply with the regulations just like other members of the school community.
- If visitors use their separate 3G, 4G, or 5G networks, the respective offices responsible for receiving them should monitor and provide continuous support. If any violations are detected, appropriate reminders and warnings should be given.
- Offices need to ensure that visitors are aware of and agree to the terms of the code of conduct for entering the school.

5. VIOLATION HANDLING PROCEDURE:

The school's equipped filtering and firewall systems will automatically block connections when devices access unsafe links. The system administration department will check the list of logged-in devices and details of the pages accessed by each device, providing daily reports to the Campus Management Board.

a. FOR STUDENTS' VIOLATIONS:

- **Step 1:** When a student's device is found to access unsafe content, the IT department will check the device and report to the campus management board.
- **Step 2:** The campus management board, in collaboration with homeroom teachers, will investigate the student's information. The campus management board will consult with the Child Protection Board and homeroom teachers to seek guidance from the school administration board on how to handle the situation. After receiving instructions from the

school administration, the campus management board, along with the Child Protection Board, will take appropriate actions according to the guidelines.

- **Step 3:** Violation handling process:

  + First violation: Remind and educate the student about the dangers to their mental and physical health when accessing unsafe content. Collaborate and discuss with parents and students to commit to not repeating the violation.

  + Second violation: Conduct a meeting with the student, allow the student to explain, and commit to not repeat the violation. Additionally, communicate with parents to collaborate on reminders, education, and monitoring the student's progress. Require the student to complete an assignment on the consequences of violating the policy.

  + Third violation and subsequent violations: The homeroom teacher will prepare a report for the campus management board, which will then be submitted to the school adminstration for further actions. The school administration, campus management board, and Child Protection Board will consider establishing a disciplinary council and agree on the appropriate disciplinary measures as stipulated.

b. FOR STAFF'S VIOLATIONS:

Step 1: When a staff member's device is found to access unsafe content, the IT department will check the device and report to the campus management board.

Step 2: The campus management board will assess the severity of the violation and propose a resolution, seeking guidance from the school administration. Once the school administration approves the proposed actions, the campus management board will work with the staff member.

Step 3: The Campus Management Board works with staff, teachers, and employees, after the meeting, reports the results to the School administration and keeps records of any violations by teachers and staff for further monitoring

+ First violation: Remind the staff, teachers, and employees about the policy violations and the potential risks to their mental and physical health when accessing unsafe content.

+ Second violation: Conduct a meeting with a written record, including statements from the staff, teachers, and employees committing not to repeat the violation. At the same time,

their performance will be evaluated during the salary month, considering promotions, and annual bonuses according to the school's regulations.

+ **Third violation and subsequent violations:** The School administration will consider establishing a disciplinary board and agree on the appropriate disciplinary actions according to the current regulations. The highest penalty may include termination of the labor contract.

C. FOR PARENTS AND VISITORS:

Step 1: When a parent or visitor's device is found to access unsafe content, the IT department should immediately communicate with the reception department to remind and request cooperation in following the regulations.

Step 2: After the reminder, the reception department should monitor this matter throughout the entire visit.

Step 3: If the parent or visitor continues the behavior, the reception department may request the IT department to disconnect their access and seek guidance from the campus director to suspend their visit for non-compliance with the school's policies.

Note: This policy may change due to the current status, the university's IT infrastructure, technological trends, and government policies. When adjustments or changes occur, the school will inform all relevant parties of the updates.

DIRECTOR IN CHARGE