The Asian International School

CYBER SAFETY POLICY

*** Bases for policy development**

- This policy is in line the Asian School's Guiding Principles, specifically:

+ As the world moves towards multiculturalism, it is the mission of the Asian International School to give highest priority to motivating and stimulating students to learn beyond their borders, in order to instill internationalism in education and desire for lifelong acquisition of global knowledge and world peace.

+ The School will provide curricula that stimulate intellectual attributes and encourage self-discipline, critical thinking, respect for others' opinion and creative approaches to problems.

+ The School will provide modern learning and study areas that are equivalent to or better than those of the best international school facilities.

+ The School will prepare every student for a productive future in the modern developing world through diverse learning experiences.

- This policy is based on United Nations Convention, Vietnam's laws, Vietnam's Law on Cybersecurity, and the Asian International School's policies/regulations, specifically:

+ Article 54 of Children Law no. 102/2016/QH13 by Vietnam's National Assembly: "Relevant authorities and organizations shall take responsibility for educating and protecting children partaking in online environment under all circumstances; parents, teachers, and caregivers shall impart knowledge and skills for children to protect themselves upon joining online spaces.";

+ UN Convention on the Rights of the Child;

+ Asian International School's Child Protection and Safeguarding Policy;

+ Asian International School's Anti-Bullying Policy;

+ Asian International School's Bring Your Own Device Policy.

1. PURPOSES

- To ensure safety and wellbeing of staff, faculty, and students who use the Internet for work, study, research, and communication;
- To provide staff, faculty, and students with guidance on safe use of information technology (IT), understanding and compliance with procedures for prevention or timely intervention of inappropriate online behaviors;
- To guarantee alignment with the values established in the School's Guiding Statements and regulations pertaining to cybersecurity, thereby developing standards within the education environment.

2. DEFINITIONS

- Cyber Safety applies to all IT devices and equipment with access to the Internet, including but not limited to personal computer (PC), laptop, smartphone, tablet, etc.;
- Cyber Safety means all individuals shall be protected and know how to protect themselves against inappropriate behaviors violating community standards on online spaces;
- Cyber Safety refers to immediate intervention of unsafe behaviors, addressing and knowing how to handle violations of standards on online spaces within the school community.

3. CYBER SAFETY PRINCIPLES

While presenting a multitude of opportunities, the Internet also harbors considerable threats and challenges. Therefore, the following principles should be followed at all times:

- All staff, faculty, and students must change their device name (on their phone, laptop, iPad, etc.) into their full name before accessing the Internet to preempt external security threats and cyberattacks directed at the School's network;
- All staff, faculty, and students shall be protected and know how to protect themselves against potential online threats, particularly those related to their work and study;

- All students will be securely protected when using the School's IT resources and infrastructure;
- All staff, faculty, and students are thoroughly instructed on appropriate online behaviors;
- Students are given support for safe use of the Internet and electronic device, understanding how to be respectful toward others;
- Parents and guardians are guided on how they can ensure Cyber Safety for their child;
- System security shall be reviewed and updated regularly;
- Login username, information, account, and password must be used safely and effectively;
- Personal information of staff, faculty, students will be kept confidential and will only be disclosed in emergency;
- New social media and communication platforms must have their appropriateness and risks assessed before getting accepted into the School's network;
- The School's online filter may not ensure cyber safety for any staff, faculty, students using their personal 3G, 4G, 5G service(s). However, students using their own device have all signed a commitment to this policy with approval from parents. At any time, should any breach of commitment be discovered, the violating student will be punished in accordance with this policy. The same measure shall apply to staff and faculty.
- Should any staff, faculty, or student employ different instruments, applications, software to bypass the School's online filter, which the existing IT infrastructure of the School may not be able to handle, and be caught doing so, appropriate disciplinary action(s) will be taken, which may range from limitation on to total loss of access to parts or the entirety of the School's IT infrastructure, or any other measures deemed appropriate by the School Board. Individuals failing to comply with this policy may, as a consequence of their action, incur a compensation, be denied access to the IT resources and infrastructure, receive permanent technology

ban, suspension or expulsion (for students), or dismissal (for staff and faculty) according to the severity of their violation and the extent of damages caused.

4. ROLES AND RESPONSIBILITIES

School Board

- Building actionable policies for the school community to understand and implement accordingly, ensuring cyber safety, preempting violations, and mitigating risks to the School's IT infrastructure;
- Communicating this policy to all staff, faculty, students, parents;
- Ensuring transparency in reporting procedures and handling issues related to Cyber Safety;
- Ensuring all staff, faculty, students, parents understand and implement this policy effectively for their own good;
- Coordinating the process of review, evaluation, and adjustment to the policy to keep up with rapid global technological development as well as changes in Vietnam's regulations;
- Directing efforts to address issues and concerns pertaining to Cyber Safety.

Child Protection Committee

- Keeping updated on risks to children using IT devices and services;
- Collaborating with School Counselling Office to organize sessions on civil, effective, safe use of online platforms;
- Raising awareness and supporting staff, faculty, students in issues related to Cyber Safety;
- Closely collaborating with IT Team and other departments as required;
- Ensuring appropriate and effective employment of cyber safety measures on campus (e.g.: the use of online web filter, firewall, antivirus software, etc.);
- Complying with step-by-step procedures as established by the School;

IT Team

The IT Team shall be responsible for ensuring the optimal functionality of the

School's IT infrastructure, cybersecurity systems, online filters, closely monitoring them, specifically:

- Ensuring operating systems and IT devices are constantly monitored and updated as appropriate;
- Ensuring antivirus software serves its intended purposes, gets updated frequently and installed on all devices on campus;
- Making sure the administrator's password is changed periodically and not to be reused within 12 months;
- Maintaining administrative and monitoring work to detect vulnerabilities in time for immediate remedy;
- Recording details of all issues and concerns pertaining to Cyber Security.

Staff and faculty

- Understanding that the use of any device or application connected to the School's network will be strictly monitored;
- Attending all relevant training sessions and fully comprehending the Cyber Safety Policy;
- Reporting issues and concerns pertaining to Cyber Security to campus management or Campus Child Protection Committee;
- Promoting and sharing cyber safety practices via appropriate means and integrate such practices into the curricula.

Students

- Understanding that abuse or misuse of IT devices/services by any means will result in disciplinary actions in accordance with regulations;
- Fully grasping the reporting process for concerns of cyberbully and abuse both in and out of school;
- Understanding the Cyber Safety Policy and keeping up to date about online risks via different channels such as School's newsletters, website, integrated lessons, training sessions with school counsellors, with the Child Protection Committee, or with homeroom teacher;

- Complying with Bring Your Own Device Policy.

Parents/Guardians

- Getting updated on the School's Cyber Safety Policy;
- Giving support to empower their child;
- Fully grasping the established Bring Your Own Device Policy and cooperating with the School to ensure diverse learning experiences for students;
- Cooperating with homeroom teacher and the School Board to monitor student's cyber safety practices at school and at home.

Visitors

- Complying with this policy when using the School's IT resources and infrastructure, like any other member of the school community;
- Getting supervised and supported by a person from the reception department/unit throughout the visit when using the visitor's personal 3G, 4G, 5G service(s); receiving appropriate warning should such department/unit detect any breach of policy on the visitor's part;
- Understanding and complying with the Code of Conduct reserved for visitors, which will be introduced by the reception department/unit.

5. DISCIPLINARY ACTIONS

Upon detecting any attempt to access unsafe link, the School's online filter and firewall will block connection. Only the administrators may see a list of connected devices and the page(s) they access, which is submitted daily to the campus management.

a. For violations committed by students

- **Step 1:** Upon discovering that a student attempts to gain access to an unsafe site, the IT Team immediately checks the device and report to campus management;
- **Step 2:** Campus management collaborates with student's homeroom teacher to look up the student's information, consult with the Child Protection Committee and homeroom teacher for appropriate resolution, and seek guidance from the School Board. After a final decision is approved by the School Board, campus management

shall collaborate with the Child Protection Committee and homeroom teacher for implementation.

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

  + First-time violation: Student will be given warning and educated about the dangers of unsafe content to physical and mental wellbeing. The School collaborates with parents to ensure against student's recidivism;

  + Second-time violation: The School will conduct a meeting with the student, require a written record from the student, and ask the parents for cooperation in giving warning, educating, and following student's progress. The students is also required to complete a written essay on the consequences for breach of this policy.

  + Third-time violation onward: Homeroom teacher will file a report to the campus management to be submitted to the School Board for further deliberation. The School Board, campus management, and the Child Protection Committee shall consider establishing a disciplinary council to agree on a resolution in accordance with current regulations.

b. For violations committed by staff or faculty

- **Step 1:** Upon discovering that a member of staff or faculty attempts to access unsafe content, the IT Team immediately checks the device and report to campus management;
- **Step 2:** Campus management assesses the severity of the violation, propose a resolution, and seek guidance from the School Board. Once a final decision is approved by the School Board, campus management shall work with the violating staff/faculty member.
- **Step 3:** Campus management works with staff or faculty member and reports the result to the School Board to record the violator's details for further monitoring:

  + **First-time violation**: Violating staff/faculty member will be given warning for breach of policy and educated about the dangers of unsafe content to physical and mental wellbeing;

  + **Second-time violation**: The School will conduct a meeting with the violator on

record, requiring them to submit a written incident report as well as written commitment against recidivism. Disciplinary actions regarding the violator's monthly performance review, pay raise, and annual bonus promotion will also be taken in accordance with the School's regulations.

+ **Third-time violation onward**: The School Board considers establishing a disciplinary council to agree on appropriate resolution in line with current regulations, with the highest punishment being termination of labor contract.

c. For violations committed by parents/visitors

- **Step 1:** Upon discovering that a parent or visitor to any campus attempts to access unsafe content, the IT Team immediately reports to and works with the department/unit welcoming such parent/visitor and issue a reminder to comply with the School's policy;
- **Step 2:** After the reminder, the reception department/unit should closely monitor such parent/visitor throughout their visit.
- **Step 3:** Should the parent/visitor make another attempt to access unsafe content, reception department/unit may ask the IT Team to disconnect their device, seek permission from campus management to withhold visitation right of such parent/visitor due to non-compliance with the School's policy.

Note: *This policy may be subject to change with every update to the School's IT resources and infrastructure, technological trend, and State's policy or regulation. In such case, the newly adjusted policy will be immediately communicated to shareholders.*

THE ASIAN INTERNATIONAL SCHOOL