IT POLICY

Kothari International School (KIS), Noida

MISSION STATEMENT:

The International Baccalaureate's Mission Statement

The International Baccalaureate aims to develop inquiring, knowledgeable and caring young people who help to create a better and more peaceful world through intercultural understanding and respect. To this end the organization works with schools, governments, and international organizations to develop challenging programs of international education and rigorous assessment. These programs encourage students across the world to become active, compassionate, and lifelong learners who understand that other people, with their differences, can also be right.

Kothari International School, Noida's Mission Statement

Kothari International School epitomizes the vision of making learning meaningful, collaborative and immensely enjoyable. Our endeavour is to empower our students with knowledge and skills through engaged learning; ensure pursuit of tertiary education of their choice and make them custodians of their own physical, emotional and spiritual well-being. Our students shall endeavour to maintain and improve the quality of life-without damaging the planet for future generations. Each member of Kothari International School fraternity is in pursuit of a Perfect Score in all spheres of Life. We realize today, more than ever, that we are an interdependent world. We expect our students to appreciate the diversity and understand the value of unity. Our students shall understand their rights and responsibilities. Thus, being empowered with knowledge and skills, they shall learn to contribute towards a Zero Conflict World. Our students shall seek seamless transition into adult life; become useful members of the communities in which they live and promote tolerance, world peace and tranquillity.

The Kothari International School endeavors to cultivate an educational atmosphere that empowers children to incorporate contemporary technology into their learning experience. With a commitment to fostering 21st-century skills such as critical thinking, creativity, collaboration, communication, self-direction, and global and cultural awareness, the school aims to offer students ample opportunities for expanding and enhancing their learning journey.

Terminology Used in this Policy Document:

(a) The abbreviation 'ICT' in this document refers to 'Information and Communication Technologies.
(b) 'Cybersafety' refers to the safe, responsible, and appropriate use of the Internet and ICT equipment/devices, including mobile phones to keep themselves and people around them safe.
(c) 'Cyberbullying' refers to direct or indirect bullying behaviours using digital technology. E.g., Inappropriate comments on social media spaces.
(d) 'School ICT' refers to the school's computer network, Internet access facilities, computers, and other school ICT equipment/devices as outlined in (e) below
(e) The term 'ICT equipment/devices' used in this document, includes but is not limited to, computers (such as desktops, laptops, PDAs), storage devices (such as USB and flash memory devices), cameras (such as video, digital, webcams).

Rationale

The KIS is mandated to uphold a secure physical and emotional setting for every child, a responsibility now intricately tied to addressing cyber-safety concerns related to the use of Information and Communication Technology (ICT). While the Internet and ICT devices is very important and offer significant advantages to educational programs and school operations, they also present challenges in terms of safety. The leadership and management prioritize equipping the school with Internet facilities and ICT devices/equipment that enhance student learning outcomes and the overall efficiency of the school.

However, the Leadership and Management acknowledges that the inclusion of these technologies within the learning environment—some provided partially or entirely by the school, and others privately owned by staff, students, and other members of the school community—can facilitate the dissemination of antisocial, inappropriate, and potentially illegal content and activities. Consequently, the school bears the dual responsibility of maximizing the benefits of these technologies while also minimizing and effectively managing associated risks.

To address this, the KIS has developed and upholds stringent and efficient cyber safety protocols aimed at optimizing the advantages of the Internet and ICT devices/equipment for student learning and school operations, while mitigating and controlling any associated risks. These cyber safety protocols will not only strive to maintain a secure online environment but also fulfil the educational needs of students and other members of the school community by providing guidance on the safe and responsible utilization of current and evolving information and communication technologies.

This policy outlines the acceptable use of devices to maintain a secure learning environment with the focus of preparing students for the future. For purposes of bringing the devices to school, KIS has it's say clearly drafted i.e., "device" means a privately owned wireless and/or portable electronic hand-held equipment that is limited to, laptops, iPads, or tablets (without sim – call/text features), that can be used for word processing, wireless Internet access, image capture/recording, sound recording and information transmitting/receiving/storing, etc.

Policy Guidelines:

Internet

- Ensuring Personal Safety – Users must refrain from disclosing personal information such as home address or telephone number while utilizing the network and Internet
- User is accountable for their network usage and must exert utmost effort to avoid accessing inappropriate content. Any security or network issues must be promptly reported to a teacher or system administrator.
- Access to the internet gateway provided by the school is exclusively permitted. Personal internet-connected devices, including but not limited to cell phones and cell network adapters, should not be used while on-site.
- Firewall Restrictions: The KIS has employed filtering software and other technological tools to prevent users from accessing content deemed obscene or harmful to minors. Any attempts to bypass the content filter are strictly prohibited and will be considered a violation of this policy. The school will also monitor users' online activities through direct observation and/or other technological means.

Usage of Freeware

- Students may be asked to download free apps that teachers use for classroom activities. If parents do not wish their child to download these apps without their presence/guidance, they should send a letter to notify the facilitator regarding the same.
- If the device brought to school has any inappropriate data or information then the device would be confiscated and will only be handed to the parent after a written letter.
- During the School hours the use of social media apps and others irrelevant to the curriculum content, are discouraged and prohibited.
- Students should ensure that their device does not contain any software or apps that will independently access illegal or inappropriate file sharing sites.

Safety and Security of the Device

- The school is not liable for any stolen/damaged device or data loss on-site Responsibility of the device security lies with the individual owner and the.
- If a device is stolen or damaged, it will be handled through the administrative office like other personal artifacts that are impacted in similar situations.
- School staff, including technology staff can support but will not be bound to will not configure or download any software in student devices.
- Additionally, protective cases for technology are encouraged – these can have labels (simple name tags that are appropriate for school use) to identify and distinguish individual devices.
- The school officials upon reasonable suspicion may read, examine, or inspect the contents of any personal device.

Data Charges and Disclaimers

- Students are herein instructed to use the school's network and not personal data plans to access the Internet when using their devices at school. Students or their parents are responsible for all data charges that a student's device may incur due to use in school. The school will not be responsible regardless of whether the student used their device for a lesson as using personal devices is never mandatory.
- No guarantee is made that the school's wireless network will always be available. Network outages may occur without notice. In addition, no quality of wireless signal is promised. Signal strength may vary depending on the location in the school and

the number of devices simultaneously connecting to the network, along with external factors such as weather, physical disruptions of network lines, etc.
- Students should bring devices fully charged to school. Access to electrical outlets for charging should not be expected.

Basic Hardware/Software Device Requirement

- Laptop with i5 processor (or latest generation) / iOS equivalent
- Windows 10 or 11 64 bit / iOS equivalent
- Hard disk – 500gb SSD
- RAM – 8gb
- Graphics Card – 2gb
- Basic software tools like Microsoft Office, Adobe Reader, VLC player, Chrome and Microsoft edge, WINRAR-64 bit

Student Agreement

The use of technology to aid curriculum and education is not a necessity but a privilege. A student does not have the right to use their laptop or any other electronic device whenever and however they wish to, while at school. If they do not follow the prescribed guidelines then they will not be allowed to use the device.

Responsibilities and Roles

User's Responsibility
- Registering their electronic device with the school and submitting a signed 'Use of Electronic Devices Agreement' prior to connecting to the school network
- Ensuring devices are used in accordance with school policies and procedures
- Privacy of accounts, login names, passwords, and/or lock codes are maintained to secure the data and devices.
- Maintaining safe and productive learning environments when using electronic devices
- Practising digital citizenship.

Administrator's Responsibility
- Inform all the users about the school policy

- Establish and monitor digital citizenship through the school Code of Conduct and Internet Acceptable Use policy
- Effectively respond to disciplinary issues resulting from inappropriate electronic device usage
- Communicate appropriately with school personnel, parents, and students if school policy is violated from electronic device usage
- Provide the information to connect electronic devices to the school network

Teachers Responsibility

- Effectively Monitoring and Supervising student use of devices
- Learning opportunities that include electronic devices to be created so that the student become responsible digital information users.
- Plan in advance to support the use of School Devices for teaching and learning.
- Any disciplinary issues from inappropriate device usage if encountered to be addressed immediately by confiscating the device and informing the DPC.
- Communicating appropriately with administrators, parents, and students if school policy is violated from electronic device usage

Students Responsibility

- Using electronic devices for educational purposes in approved locations under the supervision of school personnel only
- Virus and malware scanning on their electronic devices to be done on regular intervals to avoid any damage to the data.
- Report any inappropriate electronic device usage to a teacher immediately.
- Charge the device prior to bringing them to school
- Be creative and think out of the box if the device malfunctions to complete the task

Parents Responsibility

- Support and guide their child take all reasonable steps to care, maintain, secure, store, and transport their electronic device
- Support and guide their child preserve the privacy of accounts, login names, passwords, or lock codes
- Ensure the personal device is labelled physically and also through software for easy identification.
- Procuring hazard or theft insurance for an electronic device
- Regularly speaking and encouraging their children to follow the school policy and practice digital citizenship

- Contacting the school office to communicate with their child during the school day, in case of any emergency, instead of using emails or other digital means that have no curriculum related/education purpose
- Assuming all responsibility for their child's unauthorized use of non-school Internet connections such as a 3G/4G cellular phone network.

Prohibited uses of electronic devices includes, but are not limited to:

- Areas where there is a reasonable expectation of privacy, such as change rooms or restrooms
- Bypassing the school's authorized network infrastructure to connect to the internet via an external wireless provider
- Downloading files that are unrelated to educational activities
- Participating or engaging in activities unrelated to education, such as gaming, video watching, social media usage, music listening, texting, or making personal calls.
- Malpractice on assignments or tests
- Accessing confidential information
- Using photographs and audio/video recordings for a purpose unrelated to the school assignment
- Obtaining unauthorized access and using it to alter, destroy, or removing data
- Engaging in cyberbullying which involves using technology to embarrass, harass, threaten, or target another person directly or indirectly.
- Infecting a device with a virus or other program designed to alter, damage, or destroy
- Infringing upon copyright laws or plagiarizing protected information

Policy Review:

The IT Policy is a working document that will be updated annually. The Policy Review Committee is made up of the Head of School, the DPC, the school's IT department and IT teachers.

Policy Designed: January 2024
Next Review in: April 2025

References:

https://www.technokids.com/blog/computers-in-schools/byod-policy-for-schools/