THE PUPIL
INTERNATIONAL SCHOOL

THE PUPIL INTERNATIONAL SCHOOL
BRING YOUR OWN DEVICE (BYOD) AND CYBERSAFETY POLICY

The Pupil works towards creating a learning environment that enables children to embrace and integrate modern technology in their learning journey. The school aims to provide students opportunities to extend and enrich learning by focusing on 21st century learning, including critical and creative thinking, collaboration, communication, self-direction, and global and cultural awareness.

I. IMPORTANT TERMS USED IN THIS 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).

II. RATIONALE

The Pupil has a statutory obligation to maintain a safe physical and emotional environment for all the children. This responsibility is increasingly being linked to the use of ICT, and several related cybersafety issues. The Internet and ICT devices/equipment bring great benefits to the teaching and learning programmes, and to the effective operation of the school. The leadership board places a high priority on providing the school with Internet facilities and ICT devices / equipment which will benefit student learning outcomes, and the effective operation of the school.

However, the Board recognises that the presence in the learning environment of these technologies (some provided partly or wholly by the school and some privately owned by staff, students, and other members of the school community), can also facilitate anti-social, inappropriate, and even illegal, material and activities. The school has the dual responsibility to maximise the benefits of these technologies, while at the same time to minimise and manage the risks.

The Pupil will thus develop and maintain rigorous and effective cybersafety practices which aim to maximise the benefits of the Internet and ICT devices/equipment to student learning and to the effective operation of the school, while minimising and managing any risks. These cybersafety practices will aim to not only maintain a cybersafe school environment, but also address the need of students and other members of the school community to receive education about the safe and responsible use of present and developing information and communication technologies.

This policy outlines the acceptable use of devices to maintain a safe and secure learning environment with the mission of preparing students for the future and fostering digital citizenship. For purposes of BYOD in The Pupil, "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.

III. POLICY GUIDELINES AND PRACTICES:

INTERNET - CYBER SAFETY & CYBER BULLYING

1. Every user must take responsibility for their use of the network and make every effort to avoid access to inappropriate content. Every user must report security or network problems to a teacher, administrator, or system administrator.
2. Only the filtered internet gateway provided by the school may be accessed; while on-site, Personal internet connective devices such as but not limited to cell phones / cell network adapters should not be used.
3. Active Restriction Measures – The Pupil will utilise filtering software or other technologies to prevent users from accessing content that is obscene or harmful to minors. Attempts to circumvent the content filter are strictly prohibited and will be considered a violation of this policy. The Pupil will also monitor the online activities of users through direct observation and/or other technological means.
4. Personal Safety – In using the network and Internet, users should not reveal personal information such as home address or telephone number.

CONTENT & APPS

1. 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.

2. Students are not allowed to store inappropriate content on the device that is brought to school, they will have to face the consequences if they do so.
3. Use of social media apps and others irrelevant to the curriculum content, are discouraged and prohibited during school hours.
4. Students should ensure that their device does not contain any software or apps that will independently access illegal or inappropriate file sharing sites.

SECURITY & DAMAGES

1. Responsibility of the device security lies with the individual owner. The Pupil is not liable for any stolen/damaged device or data loss on-site.
2. If a device is stolen or damaged, it will be handled through the administrative office like other personal artefacts that are impacted in similar situations.
3. School staff, including technology staff, will not configure, troubleshoot, or repair student devices.
3. 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.
4. School officials may read, examine, or inspect the contents of any personal device upon reasonable suspicion that the contents or recent utilisation of the device contains evidence of a violation of the established rules and policies.

DATA CHARGES & DISCLAIMERS

1. Students are herein instructed to use the school's BYOD 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.
2. 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.
3. Students should bring devices fully charged to school. Access to electrical outlets for charging should not be expected.

IV. SYSTEM SPECIFICATIONS & REQUIREMENTS

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

V. BYOD 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. When abused, privileges will be taken away. When respected, they will benefit the learning environment.

VII. ROLES & RESPONSIBILITIES OF THE SCHOOL COMMUNITY

All users are responsible for:

1. Registering their electronic device with the school and submitting a signed 'Use of Electronic Devices Agreement' prior to connecting to the school network
2. Ensuring devices are used in accordance with school policies and procedures
3. Caring, maintaining, securing, and storing electronic devices
4. Preserving privacy of accounts, login names, passwords, and/or lock codes to maintain security of electronic devices and data
5. Maintaining safe and productive learning environments when using electronic devices
6. Practising digital citizenship.

All administrators are responsible for:

1. Informing users of school policy
2. Establishing and monitoring digital citizenship through the school Code of Conduct and Internet Acceptable Use policy
3. Responding effectively to disciplinary issues resulting from inappropriate electronic device usage
4. Communicating appropriately with school personnel, parents, and students if school policy is violated from electronic device usage
5. Providing information to users explaining how to connect electronic devices to the school network

Teachers are responsible for:

1. Creating equitable learning opportunities that include electronic devices for education purposes when relevant to curriculum context and concepts
2. Determining when students are allowed to use school or personal devices for education purposes
3. Supervising student use of devices
4. Responding effectively to disciplinary issues from inappropriate device usage
5. Communicating appropriately with administrators, parents, and students if school policy is violated from electronic device usage

Students are responsible for:

1. Using electronic devices for educational purposes in approved locations under the supervision of school personnel only
2. Implementing virus and malware scanning on their electronic devices
3. Reporting any inappropriate electronic device usage to a teacher or administrator immediately
4. Ensuring their electronic devices are charged prior to bringing them to school
5. Continuing to learn using an alternative method if a device malfunctions

Parents are responsible for:

1. Helping their children take all reasonable steps to care, maintain, secure, store, and transport their electronic device
2. Helping their children preserve the privacy of accounts, login names, passwords, or lock codes
3. Identifying the personal device by labelling it, recording details such as make, model, and serial number, and/or installing tracking software
4. Procuring hazard or theft insurance for an electronic device
5. Encouraging their children to follow the school policy and practice digital citizenship
6. 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
7. Assuming all responsibility for their child's unauthorised 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:

1. Areas where there is a reasonable expectation of privacy, such as change rooms or restrooms
2. Circumventing school's approved network infrastructure to access Internet connections using an external wireless provider
3. Downloading files that are unrelated to educational activities

4. Engaging in non-educational activities such as playing games, watching videos, using social media, listening to music, texting, or taking personal calls
5. Malpractice on assignments or tests
6. Accessing confidential information
7. Using photographs and audio/video recordings for a purpose unrelated to the school assignment
8. Obtaining unauthorised access and using it to alter, destroy, or removing data
9. Engaging in cyberbullying which involves using technology to embarrass, harass, threaten, or target another person
10. Infecting a device with a virus or other program designed to alter, damage, or destroy
11. Infringing upon copyright laws or plagiarising protected information

VIII. Policy Review:

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

Last Review done in: January 2024
Next Review in: April 2025

References:

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