Primrose Hill International School Electronic Device Policy

Purpose

This policy outlines the acceptable use of electronic devices to maintain a safe and secure education environment with the goal of preparing students for the future, improving learning, and fostering digital citizenship.

Definitions

Electronic devices shall include all computing devices that can take photographs; record audio or video data; store transmit or receive messages or images; or provide a wireless connection to the Internet. Examples of these devices include, but shall not be limited to desktops, laptops, tablets, smartphones, e-readers, as well as any technology with similar capabilities. ____ devices are restricted.

Digital Citizenship is the norms of responsible behaviour related to the appropriate use of technology. It encompasses digital literacy, ethics, etiquette, and online safety.

User is any individual granted authorisation to use electronic devices. Users may include students, parents, staff, volunteers, visitors, contractors, or individuals employed by service providers.

1. Authorised Use of Electronic Devices
Electronic devices brought to school shall be restricted to educational and administrative purposes in approved locations and times under the supervision of school personnel. Authorized users shall:

- use electronic devices in accordance with the expectations set forth in the school Code of Conduct and Internet Acceptable Use policy;
- comply with guidelines set by school personnel for the use of electronic devices while on school property or while engaged in a school-sponsored activity;

- take photographs and audio/video recordings only with a person's consent and when authourized by school personnel for educational purposes;
- access the school network using approved infrastructure only.

2. Responsibilities

- All users are responsible for:
  - registering their electronic device with the school and submitting a signed Use of Electronic Devices Agreement prior to connecting to the school network;
  - ensuring electronic devices are used in accordance with school policies and procedures;
  - caring, maintaining, securing, and storing electronic devices;
  - preserving privacy of accounts, login names, passwords, and/or lock codes to maintain security of electronic devices and data;
  - maintaining safe and productive learning environments when using electronic devices;
  - practicing digital citizenship.
- All administrators are responsible for:
  - informing users of school policy;
  - establishing and monitoring digital citizenship through the school Code of Conduct and Internet Acceptable Use policy;
  - responding effectively to disciplinary issues resulting from inappropriate electronic device usage;
  - communicating appropriately with school personnel, parents, and students if school policy is violated from electronic device usage;
  - providing information to users explaining how to connect electronic devices to the school network.
- Teachers are responsible for:
  - creating equitable learning opportunities that include electronic devices for education purposes when relevant to curriculum and instruction;
  - determining when students are able to use school or personal electronic devices for education purposes;
  - supervising student use of electronic devices;
  - responding effectively to disciplinary issues from inappropriate electronic device usage;
  - communicating appropriately with administrators, parents, and students if school policy is violated from electronic device usage.

- Students are responsible for:
    - using electronic devices for educational purposes in approved locations under the supervision of school personnel only;
    - implementing virus and malware scanning on their electronic devices;
    - reporting any inappropriate electronic device usage to a teacher or administrator immediately;
    - ensuring their electronic devices are charged prior to bringing them to school;
    - continuing to learn using an alternative method if an electronic device malfunctions.
- Parents are responsible for:
    - helping their children take all reasonable steps to care, maintain, secure, store, and transport their electronic device;
    - helping their children preserve the privacy of accounts, login names, passwords, and/or lock codes;
    - identifying the electronic device by labelling it, recording details such as make, model, and serial number, and/or installing tracking software;
    - procuring hazard or theft insurance for an electronic device;
    - encouraging their children to follow school policy and practice digital citizenship;
    - contacting the school office to communicate with their child during the school day, instead of using text messages, emails, phone calls, 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.

3. Unauthorized Use of Electronic Devices

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;
- circumventing school's approved network infrastructure to access Internet connections using an external wireless provider;
- downloading files that are unrelated to educational activities;
- engaging in non-educational activities such as playing games, watching videos, using social media, listening to music, texting, or taking personal calls;
- cheating on assignments or tests;

- accessing information that is confidential;
- 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 harass, threaten, embarrass, or target another person;
- infecting a device with a virus or other program designed to alter, damage, or destroy;
- committing a crime under federal, provincial, and/or municipal statues;
- infringing upon copyright laws or plagiarizing protected information;
- using network resources for commercial or political party purposes.

4. Consequences: Remedial and Disciplinary Action

- Individuals who do not comply with this Policy will be subject to appropriate consequences consistent with the school Code of Conduct and Internet Acceptable Use Policy.
- Consequences may include, but are not limited to, the following, either singularly or in combination depending on the individual circumstances:
    - temporary confiscation of device;
    - search of device contents to locate evidence of misuse;
    - limitations, suspension, and/or revocation of access privileges to personal and school technology resources;
    - disciplinary measures, up to and including dismissal;
    - legal action and prosecution by relevant authorities.

5. Liability

- Users are solely responsible for the care and use of electronic devices they choose to bring to school. Users bringing these devices to school do so at their own risk.
- The school and school personnel shall not be liable for the loss, damage, misuse, or theft of any student-owned electronic device: possessed/used during the school day; in/on school buildings, property, vehicles, or contracted vehicles; during transport to/from school; while attending school-sponsored activities.
- The school and school personnel shall not be responsible for any negative consequences to electronic devices caused by running specific software or by accessing the school network.

6. Technical Support

- School personnel shall not provide technical support, troubleshooting, or repair for user-owned electronic devices.

Parents Concerns about BYOD

Do I have to supply a device for my child to bring to school?
No, you don't. Participation is voluntary. The school will provide access to devices when technology is required through scheduled computer lab time, booked mobile carts, or via a lending library.

What device should I purchase?
The device you purchase for your child is based on your discretion. It can be a laptop, tablet, e-reader, or smartphone. The device must be able to connect to the school network and a MAC address must be provided.

What software is required?
No specific software will be required. Educators will attempt to leverage whatever software is available on the device. If specific software is required, the school will provide access through scheduled computer lab time, booked mobile carts, or via a lending library. Parents are encouraged to provide protection software on the device to prevent malware and viruses.

When can my child use his or her device at school?
A device must be used for educational purposes under the direction and supervision of school personnel. Usage is not guaranteed and is based on the discretion of the teacher.

What happens if my child runs up cellular network charges while using the device at school?
Students must use the school WIFI network. Use of a 3G/4G network is prohibited. Any cellular network charges due to unauthorized use will be the responsibility of the parent.

Will my child be able to access inappropriate content?
BYOD will allow students access to the school WIFI network. The network is filtered to block access to inappropriate content. However, no filtering system is perfect. If students inadvertently access content that is unsuitable, they should inform their classroom teacher.

Is it possible for my child to perform all their schoolwork using their device?
No. Use of the device will vary depending on the learning outcome. Some assignments will still require students to complete the work by hand or using traditional instructional materials such as printed books. In some cases, the teacher may have a system for handing out and accepting work electronically, however this will vary depending on the situation.
Will my child be able to text friends during class?
Use of the device will be limited to educational purposes. Students may exchange messages under the direction and supervision of school personnel as it relates to the assignment. Any unauthorized exchange of messages is a violation of the BYOD policy.

Can I contact my child using their device during school hours?
Contacting your child during school hours via text messages, emails, phones calls, or other digital means can disrupt the learning environment. If you need to contact your child, please phone the school office.

Is the school responsible for loss, theft, or damage?
No. Your child is responsible for the care and security of their device.

What recourse do I have if my child's laptop is stolen?
Theft is the responsibility of the owner. Contact school administration if your child's device is stolen. To aid authorities, it is advised that you label the device, record device details such as make, model, and serial number, and install tracking software. It is also recommended that parents contact their insurance company to obtain hazard and/or theft coverage.

What happens when my child's battery dies?
Your child is responsible for bringing their device fully charged to school each day. It is advised that if one battery does not provide the required length of use then a second battery should be purchased. Charging a device is limited to stations throughout the school. Permission for their use is required by school personnel. If a charging station is not available and a battery fails, your child is responsible for finding an alternative way to complete the assignment.

What happens if my child forgets their device at home?
Your child is expected to come to school prepared to learn. Students will be encouraged to store their files using a web app, making their work accessible through any device with the Internet. If deemed essential, your child will be able to access their work using a school owned device. However, if this is not available, your child must find an alternative way to complete their work.

Does my child have to share his or her device?
No. Your child should not lend his or her device to another student. It is for their exclusive use. From time to time, an assignment may have a collaborative component in which students work together in partners or small groups. In this learning situation, your child will maintain sole use over their device.

Can a teacher confiscate or search my child's device?
Yes. School personnel can confiscate a device if they suspect a breach of the BYOD policy. If there is suspicion of inappropriate content or misuse, the school can search the device with the expressed consent of the parent.
Will cyberbullying increase now that students have devices while in school?

Digital citizenship is an important element of the BYOD initiative. Students must learn how to behave responsibly when using technology. Bullying of any kind will not be tolerated and is a direct violation of the existing Code of Conduct.

Will my child have access to technical support while at school?
Your child must be familiar with how to use their device. Teachers are not IT support staff. Instructions will be available to explain how to access the school WIFI network. However, school personnel will not troubleshoot hardware, software, or network issues.