

Title: **PERSONAL** **ELECTRONIC DEVICE**

Adopted: May 2024

Reviewed:

Revised:

Authority: PPM 128: The Provincial Code of Conduct and School Board Codes of Conduct

Freedom of Information and Protection of Privacy Act (FIPPA)

 Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)

Related: KidsAbility Centre Policy: Computer Use

 KidsAbility Centre Policy: Social Media

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**POLICY**

It is the policy of the KidsAbility School Authority that authorized employees and guests be allowed to bring their own personal electronic devices (PEDs) to the school and that these devices be allowed to connect to the Authority’s public Wi-Fi infrastructure.

**Definition:**

1. For purposes of this policy “Personal Electronic Devices” (PEDs) means privately owned wireless and/or portable electronic hand-held equipment that includes, but is not limited to:
* mobile communication systems and smart technologies;
* portable internet devices;
* Personal Digital Assistants (PDAs);
* hand held entertainment systems and
* portable information technology systems that can be used for word processing, wireless Internet access, image capture/recording, sound recording and information transmitting/receiving/storing.

**Guiding Principles**

1. The Authority is committed to ensuring that the use of technology on Authority premises is for proper work-related purposes, or to support learning, in a manner that is not detrimental or harmful to the interests of others.
2. Use of technology on Authority premises must not compromise the confidentiality or proprietary nature of information belonging to the Authority.
3. The Authority reserves the right to monitor all usage, regardless of the ownership of devices and to take corrective measures as required, if inappropriate use is detected.

**General Guidelines**

1. The responsibility to keep the device secure rests with the individual owner. KidsAbility is not liable for any device stolen or damaged. If a device is lost, stolen or damaged, the issue will be handled by the Principal in a process similar to that utilized for other personal artifacts.
2. It is recommended that skins (decals) and other custom touches are used to physically identify one device from others. Additionally, protective cases for technology are encouraged.
3. The use of personal devices is strictly voluntary and a personal decision. The Authority provides either dedicated or shared equipment for the use of all staff.

1. The Authority is not responsible for any lost, stolen, or damaged personal devices. Staff and guests are responsible, at all times, for their personal devices.
2. The Authority is not responsible for any fees associated with the use of a personal device.
3. The Authority will not provide secure locations for personal devices.
4. Staff and guests may not use personal devices to record, transmit, or post photos of a person without their knowledge and consent and only within the context of school work or school event.
5. All staff and guests connecting to the Authority Wi-Fi, must adhere to Centre Policy: Computer Use.

**General Procedures**

1. Staff, guests and parents/guardians must adhere to the appropriate Code of Conduct, as well as all Authority and KidsAbility Centre policies.
2. All persons must take full responsibility for their PED and keep it on their person at all times. The Authority is not responsible for the security of the PED.
3. A PED must not be used to record, transmit or post photographic images or video of a person, or persons during school activities and/or hours.
4. The school's network filters will be applied to each person’s connection to the internet and individuals must not attempt to bypass these filters.
5. Personal devices will be connected to a segregated connection that will only allow access to the internet, no exceptions. Personal devices will not be able to connect to on premise servers, printers, or other devices.

1. Documents, in any format (Word, Docs, Excel, Sheets, PowerPoint, PDF, etc.), containing confidential information of the Authority, information about students, staff, parents, or vendors may not be stored on any personal device without expressed written consent.
2. Bringing on premises or infecting the network intentionally with a Virus, Trojan, or program designed to damage, alter, destroy, or provide access to unauthorized data or information will result in disciplinary actions.
3. Processing or accessing information on school property related to “hacking”, altering, or bypassing network security policies will result in corrective and/or disciplinary actions.
4. The Principal has the right to collect and examine any device that is

suspected of causing problems or was the source of an attack or virus infection.

**Resources**

[**PPM 128: The Provincial Code of Conduct and School Board Codes of Conduct**](https://www.ontario.ca/document/education-ontario-policy-and-program-direction/policyprogram-memorandum-128)

[**Freedom of Information and Protection of Privacy Act (FIPPA)**](https://www.ontario.ca/laws/statute/90f31)

[**Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)**](https://www.ontario.ca/laws/statute/90m56)



**Bring Your Own Personal Electronic Device - Staff**

Personal use of equipment is guided by the following regulations:

1. KidsAbility Centre Policy: Computer Use
2. Freedom of Information and Protection of Privacy Act (FIPPA)
3. Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)

All staff members requesting access to Authority email on personal devices must:

 • Ensure that their device is protected with either a pin or password.

 • Where a personal device is accessing Authority email, notify the Centre’s IT Department if the device is lost or stolen.

 • Where a personal device accessing Authority email is lost or stolen, the Authority, at its discretion, can remotely wipe all Authority data and Authority email accounts on the device in order to ensure privacy and data security.

Failure to comply with these regulations may result in revocation of privileges including the ability to access the Authority’s Wi-Fi.

 Staff Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

I understand and agree to abide by the BYOD agreement and applicable policies and

guidelines. I further understand that violations may result in the loss of my network and/or device privileges, and possibly other disciplinary or legal action.

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Staff Signature Date