



Title: PERSONAL ELECTRONIC DEVICE (BYOD)

Adopted: February 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:

Policy SHSM 002	Student Discipline
Policy SHSM 003	Code of Conduct
Policy SHSM 007	Digital Citizenship
Procedure St #1	Student Discipline
Policy: SHSM 007	Appropriate Use of Information Technologies

POLICY

It is the policy of the Bloorview School Authority that authorized employees, students 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. For students, consent must be obtained prior to connecting to the Authority's technology 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.
 - 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. BSA 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 or Vice-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 and students.
4. The Authority is not responsible for any lost, stolen, or damaged personal devices. Staff, students and guests are responsible, at all times, for their personal devices.
5. The Authority is not responsible for any fees associated with the use of a personal device.
6. The Authority will not provide secure locations for personal devices.
7. Staff, students 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.
8. All staff, students and guests connecting to the Authority Wi-Fi, must adhere to Policy SHSM 007: Appropriate Use of Information Technologies.

Guidelines Specific to Student Use of Personal Electronic Devices

1. The use of personal device to provide educational material is not a necessity but a privilege. When abused, privileges may be taken away. When respected, they will benefit the learning environment as a whole.
2. Students are never required to bring in outside technology to school. All students will continue to be able to utilize school equipment.

3. The PED technology in use must be deemed by the principal or teachers to have a potential benefit to student learning in a safe academic or a respectful environment, aligned with school values and Ontario school curriculum expectations.

GENERAL PROCEDURES

1. Students, staff and parents/guardians participating in the PEDs program, must adhere to the appropriate Code of Conduct, as well as all Authority policies, Acceptable Use of Information Technologies policy and policies related to student discipline
2. All persons must take full responsibility for their PED and keep it on their person at all times. The school 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 student's connection to the internet and students 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
6. 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 the expressed consent
7. 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.
8. Processing or accessing information on school property related to "hacking", altering, or bypassing network security policies will result in corrective and/or disciplinary actions.
9. 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.

Guidelines Specific to Student Use of Personal Electronic Devices

10. Printing from a PED is not possible at school.
11. A PED must be charged prior to bringing it to school and run off its own battery while at school.
12. A PED must not be used to cheat on assignments or tests, or for non-instructional purposes (such as making personal phone calls and text/instant messaging)
13. During instruction students may access only files on the computer or internet sites which are relevant to the classroom curriculum.

14. Students must comply with any teacher request to shut down the device or close the screen.

Consequences

15. Upon a first offence, the student will be reminded of these Personal Electronic Devices requirements, asked to turn off the device, and put it out of sight;
16. Upon a second offence, the device will be confiscated by staff. The student or his/her parent or guardian will pick up the device at the end of the school day.
17. Upon further offences, the student will lose the privilege of bringing a personally owned electronic device to school for a period of time.
18. Students may also be subject to other disciplinary consequences as deemed necessary by the Principal based on the circumstances surrounding the offence. The Parent/Guardian and student will be notified of this loss of privilege in writing.



Bring Your Own Personal Electronic Device (BYOD) - Staff

Personal use of equipment is guided by the following regulations:

1. Appropriate Use of Information Technologies (Policy SHSM 007)
2. Personal Electronic Device (Policy SHSM 015).
3. Freedom of Information and Protection of Privacy Act (FIPPA)
4. 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 Authority'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 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



Bring Your Own Personal Electronic Device (BYOD) - Student

Bring Your Own Device (BYOD) Student Personal use of equipment is guided by the following regulations:

- Students are required to adhere to Policy SHSM 007: Appropriate Use of Technologies Policy
- Student and parent/guardian are required to adhere to the Policy SHSM 015: Personal Electronic Device
- Students who are under the age of 18 must have written permission from a parent or legal guardian, prior to using the devices in school. This permission is required to be granted annually.
- Permission to use your own device in the classroom is at the discretion of the supervising teacher/staff.
- At no time, are student personal devices allowed in exams, tests or other events listed by the Authority, the school or the teacher, as technology free.
- Any recording including but not limited to video, image or sound without authorization of the supervising teacher/staff is prohibited.

Failure to comply with these regulations may result in revocation of privileges including the ability to access the Authority 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

Student's Signature

Date

As a parent I understand that my child will be responsible for abiding by the above policy and guidelines. I have read and discussed this with them and they understand the responsibility they have while using their personal devices. In the event that they violate this agreement, the district may confiscate and inspect the device, and taken appropriate action.

Parent's Signature

Date