Dream . Learn . Grow
Bloorview
SCHOOL AUTHORITY

Title: **PERSONAL ELECTRONIC DEVICES**

Adopted: December 2020
Reviewed: November 2021
Revised: February 2024, June 2024
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
	Procedure St #1	Student Discipline
	Policy: SHSM 007	Appropriate Use of Information Technologies

POLICY

It is the policy of the Bloorview School Authority (herein referred to as the "Authority") that authorized employees, volunteers, 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, prior 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. The Authority 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, volunteers and students.

4. The Authority is not responsible for any lost, stolen, or damaged personal devices. Staff, volunteers, 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, volunteers , 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, volunteers , 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, volunteers and parents/guardians participating in the PEDs program, must adhere to the appropriate Code of Conduct, Appropriate Use of Information Technologies policy, policies related to student discipline and all other Authority policies

2. All members of the school community must not use personal mobile devices[1] during instructional time except under the following circumstances.

    a. for educational purposes, as directed by an educator,
    b. for health and medical purposes
    c. to support special education needs.

3. All persons must take full responsibility for their PED. The school is not responsible for the security of the PED.

4. 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.

5. 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.

6. 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

7. 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

8. 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.

9. Processing or accessing information on school property related to "hacking", altering, or bypassing network security policies will result in corrective and/or disciplinary actions.

10. 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

1. For grades 7 to 12 students' personal mobile devices are stored out of view and powered off or set to silent mode during instructional time, except when their use is explicitly permitted by the educator under the circumstances outlined in number 2 above.

2. Except when the use of a Personal Electronic Device is explicitly permitted by the educator under the circumstances outlined in number 2 above, If the educator sees a personal mobile device in a grade 7 -12 class that is not stored out of view, they will require the device ***be handed in*** for the instructional period. The device must be placed, ***by the student,*** in a storage area in a location in the classroom designated by the educator.

3. For students in grade 6 and below, the students' personal mobile devices are stored out of view and powered off or set to silent mode through out the full instructional day, except when their use is explicitly permitted by the educator under the circumstances outlined in number 2 above.

4. Except when the use of a Personal Electronic Device is explicitly permitted by the educator under the circumstances outlined in number 2 above, if an educator sees a personal mobile device that is not stored out of view by a student in grade 6 or below, they must require the device be ***handed in*** for the instructional day. The device must be placed, ***by the student,*** in a storage area in a location designated by the Principal.

5. If the student does not hand in their personal mobile device when required, they must be sent to the Principal's office

6. Even if a PED is being used under the circumstances outlined in number 2 above, printing from a PED is not possible at school.

7. A PED must be charged prior to bringing it to school and run off its own battery while at school.

8. 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)

9. During instruction students may access only files on the computer or internet sites which are relevant to the classroom curriculum.

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

11. Clear expectations of students, educators and the Principal are outlined in Policy SHSM 003: Code of Conduct.

12. Best use of technologies practices for educators in the classroom and students are outlined in Policy SHSM 007: Appropriate Use of Information Technologies.

13. Parents will be reminded annually of this policy, its requirements and consequences for non-compliance via the parent handbook.

14. Students will be reminded, via signage in the classroom and via the classroom teacher, of this policy, its requirements and consequences for non-compliance .

15. This policy, its requirements and consequences for non-compliance, will be posted on the public website of the Authority.

Consequences

1. Upon a first offence, the student will be reminded of these Personal Electronic Devices requirements, reminded to power off the device, and put it out of sight;

2. Upon a second offence, the device will be confiscated by staff. The student or the student's parent or guardian will pick up the device at the end of the school day.

3. Upon further offences, the student will lose the privilege of bringing a personally owned electronic device to school for a period of time. The Parent/Guardian and student will be notified of this loss of privilege in writing

4. Students may also be subject to other disciplinary consequences as deemed necessary by the Principal based on the circumstances surrounding the offence.

Personal Electronic Device - 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

Personal Electronic Device - Student

Student use of a personal electronic device is guided by the following regulations:

- Students are required to adhere to Policy SHSM 007: Appropriate Use of Technologies Policy
- 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 and is restricted to those circumstances outlined in Policy SHSM 015: Personal Electronic Device
- 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