Title: **APPROPRIATE USE OF INFORMATION TECHNOLOGIES**

Adopted: February 2024
Revised:
Reviewed:
Authority: Municipal Freedom of Information and Protection of Privacy Act
Ontario Health Information Protection Act
Ontario Student Record Guidelines
Ontario Personal Health Information Protection Act
Ontario Libel and Slander Act
Related: Policy SHSM 015: Student Personal Electronic Device (BYOD)
Policy GOV 009: Confidentiality for Staff and Volunteers
Policy HR 011: Electronic Monitoring
Policy OPR 003: Social Media
Policy OPR 004: Social Media guidelines and On-Line Content
Policy SHSM 002: Student Discipline
Policy SHSM 003: Code of Conduct
Policy OPR 005: Privacy Protection and Access to Information

POLICY

It is the policy of the Bloorview School Authority that all students, parents, volunteers, staff, service providers and practicum participants use the Authority's information technology and on-line computer systems safely and appropriately.

BACKGROUND

1. The Authority maintains various electronic systems, including E-mail. Internet access, WIFI, educational applications, computers, etc. as part of its technology platform.
2. The Bloorview School Authority provides a safe and secure technology environment that allows network and internet access to staff, students, and guests for the purposes of learning and to facilitate Authority business.
3. Bloorview School Authority provides on-line systems and resources for use by employees and students. On-line resources include all material that is accessed through a computer, laptop/tablet or other electronic devices. Safety and security of those systems must be adhered to by all staff and students.
4. The Authority reserves the right, without prior notice to the employee, student, members of the Authority, or service provider, to monitor the use of technology on Authority premises. Further the Authority reserves the right without prior notice to monitor any activity on any

device at any time at any location when using Authority provided credentials. Authority owned technology provided to an employee, student, or service provider, may be accessed or recalled without any prior notice.

5. The Authority recognizes the changing nature of technology and continues to work to remain current while providing the school community with increased opportunities for the use of new technologies and applications

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. It is the responsibility of all staff, parents, volunteers, students and students at Bloorview on practicum placements to follow the guidelines as outlined herein.
3. School staff may also wish to consult with their union regarding guidelines for the use of technology
4. It is the responsibility of all staff to instruct and model for students' appropriate digital citizenship and to monitor student adherence to these guidelines.
5. It the responsibility of the school leadership (Principal, Vice-Principal, Supervisory Officer) to instruct and model for staff appropriate use of technology and to monitor adherence to this policy
6. Use of technology on Authority premises must not compromise the confidentiality or proprietary nature of information belonging to the Authority.
7. The use of any technology on Authority premises must be to assist in the conduct of Authority business and should only be utilized as directed or outlined by the Authority.
8. When using Authority provided technology including e-mail and internet services, all email and internet communications sent and received by users are the property of the Authority. E-mail, internet, or voice-mail communications are not private or personal despite any such designation by the sender or the recipient. Personal or private communications transmitted on the Authority's electronic information system may be accessed, reviewed, copied, deleted, retained, or disclosed by the Authority at any time and without notice
9. From time to time, employees or service providers will have access, or have in their possession electronic versions of student data. It is the employee's and service provider's responsibility to safeguard that data under the Ontario Student Record Guidelines and if applicable, the Municipal Freedom of Information and Protection of Privacy Act and/or the Ontario Health Information Protection Act. Employees or service providers who suspect that this data has been compromised shall notify the Principal immediately.

PROCEDURES

Personal Safety Rules

1. Staff, parents and students will:
    - Never reveal personal information, photos or videos on-line about someone else without their prior permission and knowing the information will not be used for harmful purposes;

- Never send photographs of themselves, another person or a group over an electronic network without prior informed permission of all the individuals involved and, in the case of minors, their parents or guardians;
- Only use school owned devices when taking pictures or videos of students, parents, staff or of school related activities (with the exception of parents taking pictures of their own children, and no others):
- Immediately report to a teacher or the Principal any message or request that is received that is upsetting or suggests personal contact;
- Never publish the specific dates, times and locations of field trips to people who are not directly entitled to such information or to public forums where unknown persons might access the information;
- Never share their passwords or accounts with others and must make all efforts to safeguard this information from unauthorized users;
- Refrain from giving out personal information, such as their family name, email address, home address, school name, city, country or other information that could help someone locate or contact them in person.

Unacceptable Sites and Materials

2. On a global network such as the internet it is impossible to effectively control the content of the information. On occasion, users of on-line systems may encounter material that is controversial and which other users, parents or staff might consider inappropriate or offensive. It is the responsibility of the individual user not to intentionally access such material. If such material is accessed by accident, the incident must be reported immediately to a teacher or the Principal.
3. Bloorview School Authority is committed to meeting obligations under the Canadian Charter of Rights and Freedoms and the Ontario Human Rights Code by providing safe schools and workplaces that respect the rights of every individual. Discrimination and harassment will not be tolerated. It is not acceptable to use on-line systems to knowingly access sites, which contain material of a discriminatory or harassing nature.

Prohibited Uses and Activities

4. All users of Bloorview School Authority on-line systems will **not** knowingly do the following:
    - Copy, download, install or run viruses or other inappropriate or unauthorized materials such as games, files, scripts, fonts, or dynamic link libraries (DLL's), bulk mail, junk mail, spam, chain letters from any source.
    - store, distribute, post, download, or view any material which is defamatory, abusive, obscene, profane, pornographic, sexually explicit, threatening, racially or ethnically offensive, sexist or illegal; uses inappropriate and/or abusive language or conduct; is racially, culturally or religiously offensive or contains hate propaganda.
    - transmit or distribute the Authority's confidential or proprietary information in a manner that would constitute negligence.

- transmit and/or use of any unlicensed software, software having the purpose of damaging computer systems or files (e.g., computer viruses), software that compromises the integrity of the systems (e.g., key loggers, password sniffers) is prohibited. All software and files downloaded must be systematically checked for viruses before loading on Authority technology systems.
- make any malicious attempt to harm, destroy, or illegally access or share data of any person, computer, or network linked to the Authority's network (e.g. using software and/or hardware designed to intercept, capture and/or decrypt passwords.
- use camera phones in private areas: locker rooms, washrooms, dressing areas, at any time. Such use may be in violation of the Criminal Code and Privacy legislation and may be subject to internal and external disciplinary consequences.
- Cause damage to any computer(s) and/or equipment including, but not limited to computer hardware, furniture, projectors, connectors, keyboards, storage devices (e.g., disk drives), and pointing devices (e.g., mice).
- Use any other person's account on the system.
- Cause any user to lose access to the system – for example, by disabling accounts or changing passwords without authorization.
- Attach unauthorized devices to a computer or network. Such devices include but are not limited to portable computers, disk drives, protocol analyzers, and other electronic or mechanical devices. Move, copy, or modify any of the system files or settings on any computer, server or other device without proper authorization.
- Compromise themselves or others by unauthorized copying of information, work or software belonging to others, encouraging others to abuse the computers or network, displaying, transferring or sharing inappropriate materials. Software pirating and unauthorized copying of material belonging to others is regarded as theft.
- Copy, transfer or use files, programs or any other information belonging to the Bloorview School for any reason whatsoever unless the licensing specifically permits such actions.
- Interfere with other's lawful use of data and technology by, for example, Damaging or erasing files or information belonging to another person without authorization
- Store images, content of student work, personal information or signatures of individuals on an Authority or personal device without their prior informed consent:
- Attempt to subvert the Bloorview School networks by breaching security measures, hacking accessing records without authorization or any other type of disruption.
- Take the ideas, writings or images of others and present them as if they were yours. Under copyright laws, all information remains the property of the creator(s)/author(s) and therefore permission is required for its use. The use of copyright materials without permission can result in legal action.
- infringe on another person's copyright, trademark, trade secret of any other property without lawful excuse.
- solicits any users on behalf of any business or commercial organization without appropriate authorization;
- attempts to hide, disguise or misrepresent the identity of the sender

- use technology as a means to commit, advocate or facilitate unlawful activity (examples include but are not limited to fraud, extortion, sale and/or purchase of restricted goods or the use of controlled substances);
- violates or infringes the rights of any other person according to the Bloorview School Authority policies, Ministry of Education policies, the Ontario Human Rights Code, or the Canadian Charter of Rights and Freedoms;
- Publish, without lawful justification or excuse, material that is likely to injure the reputation of any person by exposing that person to hatred, contempt or ridicule, or that is designed to insult the person or that contains inappropriate religious or political messages;
- Disclose personal information in a manner inconsistent with the Municipal Freedom of Information and Protection of Privacy Act.
- Gain unauthorized access to a computer system.
- Destroy or encrypt data without authorization and with the intent of making it inaccessible to others with a lawful need to access it.
- Use technology, to cause people to fear for their safety or the safety of anyone known to them (i.e. harassment or cyber bullying, threatening or intimidating any person or suggesting violence, hatred or discrimination toward other people);
- Unlawfully intercept someone's private communications or unlawfully intercept someone's electronic mail.
- Establish or access websites, links, postings, email messages, text messages, or any form of publishing which has an unauthorized connection to the School Authority, or which may be criminal, degrading, defamatory or inappropriate is expressly forbidden and in violation of this policy. The author will be required to remove such material as soon as it is identified as being in violation of this policy and further action may be taken against the author.
- Establish internet or external connections that could allow unauthorized access to the Authority's computer systems and information. These connections include (but are not limited to) the establishment of multi-computer file systems, ftp servers, telnet, internet relay chat or remote-control software.

Consequences

5. Violation of this policy by students or staff could result in disciplinary action up to and including dismissal and may include legal action and/or involvement of police.
6. Individuals who are in violation of any of these guidelines could be banned from further visiting and contributing to the Authority social media platforms.
7. Healthcare employees who work in the school are also bound by the policies of their professional organizations (e.g. SLP)

On-Line Publishing

8. Information published on the Internet or Intranet can reach millions of people who are mostly unknown to the original publishers. For this reason, it is important to regulate information that is published through the facilities of Bloorview School Authority.
    - The electronic publication of information using the facilities of Bloorview School is subject to all Bloorview School Authority policies and guidelines.
    - Links from a Bloorview School Authority site to outside sites must be carefully selected and are subject to the same standards of content quality as Bloorview School sites.
    - A means of contacting the publisher of any collection of information (such as a Web site) must be clearly identified on the opening screen of the collection.
    - The information published on-line must be kept current and accurate with no conscious attempt to mislead the reader.
    - Personal information such as personal addresses, phone numbers, individual or group pictures, or signatures cannot be published without express informed permission according to Bloorview School procedures.
    - For the safety of students, specific times and locations of excursions/field trips must not be published.
    - The Principal is responsible for ensuring that all work published is original or has been cleared for copyright with the originator and ownership of the copyright is clearly indicated.
    - Advertising on any Bloorview School related electronic publication is subject to the approval of the Principal.
    - All Web pages hosted on the Bloorview School Authority site or paid for by Bloorview School are considered property of Bloorview School Authority.

Liability

9. Bloorview School Authority makes no warranties of any nature or kind, expressed or implied, regarding its on-line services or resources, the continued operation of these services, the equipment and facilities used and their capacities, or the suitability, operability and safety of any program or file posted on Bloorview School Authority systems for any intended purpose.

Implementation

10. The Principal will notify parents about the existence of this policy.
11. All students and/or their parents/guardians shall read and agree to adhere to this policy prior to accessing the internet, using any Authority technology, or bringing any devices on Authority premises. If a student is under 18 years of age, a parent or guardian shall also sign the policy. This may be done as part of the student's registration process.
12. By signing this policy (and related documentation), Parents and or Guardians grant permission for their child or ward to access networked information technology, inclusive of

the internet and email. If a Parent or Guardian does not wish for their child or ward to access networked information, they shall inform the Principal in writing.

13. Parents and or Guardians agree to fully cooperate with the Authority and any relevant investigating authority, should a serious infraction of the policy occur due to the use of non-Authority owned technology, on Authority premises.
14. Students and/or parents will be required to read and accept the policy annually as part of the student information verification process. Failure to accept this policy will prevent the student from using any technology on Authority premises
15. Teachers shall provide students with instruction on the appropriate use of the internet and the protocols for the use of electronic mail. If other electronic communications or technology methods are to be used, they shall be accompanied by instruction on appropriate use and associated risks. Teachers shall ensure that students accessing the internet do so as part of an instructional plan
16. Failure to comply with this policy may result in the loss of access privileges, financial compensation to the Authority,–pursuance of criminal charges or civil action and/or other disciplinary action up to and including discharge.
17. The Principal will establish the steps to be taken by students and staff to respond to any violation of the policy, including if applicable the inadvertent access in the school to inappropriate/illegal material on the Internet
18. With prior permission students may also be allowed to use non-Authority technology (personal devices such as cell phones, smart phones, laptops, tablets etc.) on Authority premises (see Policy SHSM 015: Personal Electronic Devices)
19. The Authority reserves the right to monitor all usage, regardless of the ownership of devices and to take disciplinary measures as required, if inappropriate use as outlined in this policy is detected.
20. All users of Bloorview School on-line systems will:
    - Keep use of on-line services within reasonable limits in terms of time and volume of information transferred through the system. Excessive use of the system may disrupt services for all users (e.g., sending mass mailings of large documents or transferring large files at times of peak system usage).
    - Report to the Principal any harm to the system or to information on the system whether that harm has been caused accidentally or intentionally.
21. Human Resource staff will ensure all new staff acknowledge they have read and understood the policy (and related documentation) and will place a signed copy of the acknowledgement form in the employee's personnel file. Agreement with the policy is a condition of employment. Upon changes to this policy, Human Resources staff will require that existing staff acknowledge and agree to the updated policy. Agreement with the updated policy is a condition of continued employment.
22. The right of the Authority to access an employee, student, members of the Authority, guest or service provider's e-mail, internet history, documents and/or voicemail on Authority provided technology or personal devices when using Authority credentials may arise in a number of situations, including:
    - to comply with disclosure requests or orders made pursuant to the Municipal Freedom of Information and Protection of Privacy Act;

- for Authority owned technology, because of regular or special maintenance of the electronic information systems;
- for Authority owned technology, when the Authority has a business related need to access the employee's system, including, for example, when the employee is absent from work or otherwise unavailable;
- in order to comply with obligations to disclose relevant information in the course of a legal proceeding; and when the Authority has reason to believe that there has been a violation of this policy.

23. The Authority recognizes that some personal use is inevitable, provided that it is not in violation of this policy. Regardless of ownership, it is against this policy to use the Authority's technology for excessive personal use. Excessive personal use includes but is not limited to installing and using bit torrents, downloading movies and games, etc. and any other such personal use that consumes high bandwidth. Users acknowledge that personal use information is not privileged or protected by privacy legislation and users explicitly waive any privacy rights they may have or claim under the Municipal Protection of Privacy Act or any other relevant legislation, federal or provincial.

Dream . Learn . Grow
Bloorview
SCHOOL AUTHORITY

SAMPLE LETTER TO PARENTS

Parents:

Bloorview School Authority is committed to providing students with access to the Internet through the Authority's computer network. The Internet is a rich source of information and opportunities to enhance student learning. However, increased access to the Internet raises issues that must be addressed and understood.

Bloorview School Authority has addressed issues through a policy entitled *Appropriate Use of Information Technology* which applies to students, staff and all other users of electronic resources accessed through the facilities of Bloorview School, including the Internet. This On-Line Code of Conduct includes sections covering Personal Safety Rules, Unacceptable Sites and Materials, Use Guidelines, Prohibited Uses and Activities, On-Line Publishing, and Liability. It is available on the Bloorview School Authority website http://bloorviewschool.ca under the "About the School" section, Policies and Planning or upon request from your child's teacher.

The Authority expects that students will be responsible in their use of the Internet through the facilities provided by the Authority.

Yours truly,

Principal

NB – the Parental declaration may be included as part of the overall media form.

SAMPLE - Parent/Guardian Consent

I have read and understood the Bloorview School Authority's Appropriate Use of Technology policy and:

- I recognize that the full policy and related documentation governing my child's use of technology is available on the Authority's website or from my child's school;
- I will emphasize the ethical and responsible use of technology and caution my child about unsafe communication with others on the internet;
- I grant permission for my child to access networked information technology, inclusive of the internet and e-mail for educational purposes. I am aware that my child will be given instruction in the proper use of the internet at school and further recognize that I am responsible to supervise my child's use of the computer and internet at home;
- I agree to fully cooperate with the Authority and any relevant investigating authority, should a serious infraction of the policy occur due to the use of non-Authority owned technology, on Authority premises.
- I consent to the collection, retention, use, disclosure and disposal of my child's personal information obtained:
    - While connected to or using Authority devices, Authority technology and personal devices while connected to Authority technology including but not limited to WIFI.
    - Obtained while connected to the internet using Authority provided credentials at any time, on any device and at any location

_____
Parent/Guardian Name (Printed)

_____ _____
Parent/Guardian Signature Date

Expectations for Student Use of Technology – Primary (Grades JK-3)

It is expected that I will:

- Use the internet and computers to help me learn
- Keep my password secret
- Tell my teacher right away if, by mistake, I go to a scary or bad site or if I see or read, something that makes me feel uncomfortable.
- Never tell anyone on the internet my name, age, address or phone number
- Be careful when using the computers, iPads or other technology so that it doesn't get broken
- Respect the work of others and not say it is mine
- Never meet in person with someone I have met online without my parent's approval and participation;
- Never use the computers or the internet to hurt someone or their feelings

Expectations for Student Use of Technology–Junior – Intermediate (Grades 4 – 8)

It is expected that I will:

- Use all technology equipment carefully and not damage, change or tamper with the hardware, software, settings or the network;
- Keep my password secret;
- Use the technology only to help me learn;
- Give credit to the author of work I find on the internet and obey copyright laws;
- Not provide my personal information (name, address, phone number) to anyone on the internet;
- Never meet in person with someone I have met online without my parent's approval.
- Tell my teacher about anything on the computer or other devices that is inappropriate or makes me feel uncomfortable;
- Never use any form of technology to harass, frighten, or bully anyone;
- Take care when printing and consider the environment when deciding what to print.

Expectations for Student Use of Technology– Intermediate – Senior (Grades 9 – 12)

It is expected that I will:

- Read and understood the Bloorview School Authority's Appropriate Use of Information Technologies Policy and recognize that it is governing my use of the technology on Authority premises and that these documents are available on the Authority's website.

- Agree to abide by the policy and recognize that failure to comply with the policy may result in the loss of computer and/or network access privileges, financial compensation to the Authority and other disciplinary actions consistent with the School's Code of Behaviour, Authority Policy and/or legal authorities.

Dream . Learn . Grow
Bloorview
SCHOOL AUTHORITY

Employee/ Member of the Authority/ Service Provider to the Authority

As a user / member of the Authority/ service provider of the Bloorview School Authority's technology services, I have read the Authority's Policy *Appropriate Use of Information Technologies* and I consent to the collection, retention, use, disclosure and disposal of personal information obtained:

- While connected to or using Authority devices, Authority technology and personal devices while connected to Authority technology including but not limited to WIFI.
- Obtained while connected to the internet using Authority provided credentials at any time, on any device and at any location

_____
_____
Name (Printed)

_____ _____
Signature Date

_____ _____
Witness Date