

Digital Technology, Consent and Privacy**AP No. 401.1****ADMINISTRATIVE PROCEDURES**

The use of technology in the District is primarily for educational purposes and for conducting District business. Other uses of digital technology that interfere with the operations, security, and integrity of the District or educational process are prohibited.

1. Student and Staff Use of Digital Technology

- a) Recording devices or technologies should not be used in District facilities or offices without the knowledge and consent of those whose words or activities are being recorded.
- b) Use of mobile devices and other recording methods are prohibited in change rooms, medical rooms and washrooms.
- c) Use of mobile devices shall not interfere with learning, or the operation of schools and students will follow all school and District guidelines for use while under the supervision of the District staff.
- d) Each digital technology user shall take all reasonable precautions to prevent a breach of privacy by ensuring that personal information is secure and safe.
- e) Users shall not utilize District digital technology to knowingly engage in the unauthorized collection, use or disclosure of personal information, and will immediately report any privacy breaches to the Superintendent or designate.
- f) Any personal or District devices that access District resources must not be used to facilitate access by unauthorized users or engage in the unauthorized use of District systems and networks or to sabotage or damage District digital resources or systems.
- g) Password sharing and the use of another person's login are not permitted.
- h) The use of District digital technologies to send unsolicited or irrelevant messages broadly (spam) is prohibited on District technologies.
- i) These guidelines must be shared and reviewed annually with staff, students, and parents/guardians.

2. Student Personal Digital Devices

The Board restricts the use of personal digital devices at school for the purpose of promoting online safety and focused learning environments.

Elementary School Students

For students in elementary schools, personal digital devices must be powered off and safely stored during the entire school day, from the time the student arrives on school grounds until they leave school grounds. This extends to instructional time, while off school property (e.g. field trip).

Students in elementary schools may only use personal digital devices during the school day for instructional purposes and to promote digital literacy, and only with the permission and direct supervision of a teacher or other staff member.

Secondary School Students

For students in secondary schools, personal digital devices must be powered off and safely stored away during instructional time, unless being used for instructional purposes or to promote digital literacy; this may be done with the permission and under the direct supervision of a teacher or other staff member. Secondary school students may use personal digital devices during the school day outside of instructional time, for example, before school begins, between classes, or during lunch break.

All Students K-12

Any use of personal digital device during instructional hours must be appropriate to a student's age and developmental stage.

All students are responsible for safe storage of any personal digital device(s) brought to school.

Exemptions for Individual Students

Individual students at any grade level with documented and verified needs, such as accessibility, medical, health, or learning needs may work with the School Based Team to develop an exemption plan that requires the use of a personal digital device for full inclusion.

Use of a personal digital device during the school day or instructional hours will be considered in matters of equity, such as a lack of internet access at home.

Final approval of any exemption must be given by the School Principal, and the approved plan will be shared as necessary and appropriate with staff members.

3. Expectations for Acceptable Use of District Technologies:

- a) Users are expected to read and familiarize themselves with the 'District Digital Technology User Agreement' and its terms. To facilitate this process, supervisors will inform staff and students of these guidelines before granting access to all electronic information systems.
- b) Privacy in the use of District digital resources is not guaranteed. Users should be aware that the District may monitor the use of its systems, and the Ministry of Education & Child Care or its agents may monitor their systems, including when used by District staff and students (e.g. MyEdBC).
- c) Users are expected to understand that all data traffic, user activity and material stored on District systems may be accessed, monitored, recorded and stored for system maintenance, improvement, trouble-shooting and archival purposes; to ensure compliance with this and other District policies; and to investigate complaints and incidents of misconduct that may occur.

4. District digital technologies shall not be used for illegal or inappropriate purposes.

Inappropriate use of District digital technology includes, but is not limited to:

- a) transmission of materials in violation of Canadian Law
- b) transmission, storage or duplication of pornographic material
- c) transmission or posting of threatening, offensive or obscene material
- d) transmission or duplication of material in violation of copyright law
- e) transmission of known false or defamatory information about a person or organization
- f) attempts at unauthorized access to data, servers, or external services
- g) impersonation or use of someone else's account or identity online
- h) attempts to vandalize District or external systems, including malicious attempts to destroy data of another user, systems or software, via virus or other means
- i) use of abusive, vulgar, profane, obscene, threatening, harassing or other inappropriate language

- j) posting of email, photos, and other information without permission of the author
- k) revealing of another person's personal address, phone number, picture, or other data without personal or parental/guardian consent, as appropriate

5. Consequences for unacceptable Use of District Technologies:

- a) Staff members are expected to comply with this Policy, and could face disciplinary action, including loss of privileges or progressive discipline for breaches of policy or administrative procedures.
- b) Students are expected to comply with this Policy, and could face disciplinary action, including loss of privilege and/or confiscation of devices and suspension for breaches of policy or administrative procedures.
- c) Outside users or guests could have access suspended or privileges revoked because of breaches of policy or administrative procedures.

6. Academic Integrity

Academic integrity is a foundation of learning, and all educational community members must commit to upholding the values of respect, honesty, and accountability in educational work. Students and staff must represent their thoughts and ideas using acceptable academic citation and referencing for all sources including digital sources.

7. Consent

When consent for the collection, use and disclosure of personal information is required by the District, the District follows the following procedures:

- a) Student and/or Parent/Guardian consent must be provided for photo/video recordings of individual students for use by the school/District for community print or online publications.
- b) The District maintains student consent using the District Form on school files throughout a student's time at school. If the student changes schools within the District, the form should move with the student's files.
- c) Consent forms are obtained once during a student's elementary years and once again in their high school years.
- d) Parents/guardians may change their consent options by completing a new form and submitting it to their child's school.
- e) If a consent form is not returned or the consent section is not completed, it will be registered as 'No Consent' for that student.
- f) Schools will maintain an annual 'no consent' list.

8. Surreptitious Recording

To ensure the privacy and security of the District community, students, staff and visitors are expected to refrain from the creating, sharing, posting online or publishing photos, videos and/or recordings of staff, students or visitors at District facilities, events or activities, except with consent from affected individuals.

Staff members shall refrain from posting images, photos or recordings of students on personal social media sites, except as approved by the District.

9. Outside Media/Photographers and Public Events

The District does not facilitate access by media outlets to Staff or students, except as approved by the Superintendent. When media is permitted to attend at District facilities or at District, privacy safeguards must be in place that include the following:

- a) Providing advance notice to parents/guardians and students so they may “opt-out” of events;
- b) Advising parents/guardians when media presence is scheduled at the school; and,
- c) Ensuring students with ‘no consent’ are identified to media/camera operators and are not included in any photographs, video or audio recording;
- d) Parent/Guardian consent must be received in advance for specific recording and use of a student’s photograph, video image or audio recording in a classroom or school setting.

While the District does not facilitate media access to Staff or students, it may not be possible for the District to prevent such access in every case, such as during public events or trips off of school grounds. Staff will notify their direct management supervisors if they become aware that unwelcome media access to students has taken place and the publication of student images or information may occur.

Related Policy: [401.1 – Digital Technology, Consent and Privacy](#)