



AP I8 Acceptable Use of Technology

Legislative References: *Freedom of Information and Protection of Privacy Act (FIPPA)*; School Act Section 85; *Canadian Charter of Rights and Freedoms*; *Canadian Criminal Code*; *Copyright Act*

Policy Reference: None

Collective Agreement References:

Date: May 30, 2024

The District acknowledges that informed and responsible use of electronic information and communication systems, and social media, promotes technological literacy and offers many other educational benefits. Accordingly, the District is committed to promoting responsible digital citizenship and to minimizing the risks associated with the use of electronic communications systems and access to social media, and therefore governs the use of technology by students, staff, parents, volunteers, and the community.

The District encourages acceptable, ethical, responsible and legal use of all District and personal technology by users. Such use will be consistent with this Administrative Practice and any other Board policies or other administrative practices.

The District acknowledges the need to protect the integrity of school and working environments and that the safety, security and privacy of students, staff and other users are of paramount importance.

The District has designed this Administrative Practice to reflect the dynamic and evolving nature of technology. However, due to the continual change that occurs in technology, this Administrative Practice is to be reviewed on a regular basis.

Definitions

District Technology means any electronic device, service or system designed or used to assist in learning, communications or business operations (including but not limited to computers, cell phones, cameras, social networking sites, e-mail and voice services, school networks, etc.) owned and/or operated by the District, including but not limited to the District's network, servers, and e-mail.

Personal Technology means any electronic device, service or system designed or used to assist in learning, communications or business operations (including but not limited to computers, cell phones, cameras, social networking sites, e-mail and voice services, etc.) owned and/or operated by a District User and excludes District owned technology.



District Network/Intranet means a privately maintained computer network that can be accessed only by authorized persons, especially members or employees of the organization that owns it.

System means interrelated and interdependent hardware and software and data communication devices.

User means all students, staff, parents, school volunteers and the community using District technology or personal technology that is connected with any District or District-related activities, including off-campus activities if such activities have a connection to the District or its schools.

Processes

1. Technology and Instruction
 - 1.1. New technologies shift the ways that information may be accessed, communicated and transferred. As student and staff access to rich information resources is desirable, best instructional practice requires the integration of information and communication technology tools into all aspects of student and professional learning. This environment will be characterized by openness, accessibility, transparency, ethical use, and personal accountability and responsibility of all users.
2. Security and District Rights
 - 2.1. Access
 - 2.1.1. Access to District technology is a privilege, not a right.
 - 2.1.2. The District expects that the use of District technology will occur in an appropriate, ethical, responsible, and legal manner for the purposes of supporting educational programs and the District's administrative services.
 - 2.1.3. All users are responsible for ensuring they have reviewed this Administrative Practice prior to making use of District technology services.
 - 2.1.4. The District's Information Technology Manager may block messages or remove files that are unacceptable and/or in violation of District standards.
 - 2.1.5. If District equipment is provided to a District technology user, a District form must be completed where applicable.
 - 2.2. Use of Technology
 - 2.2.1. Technology must be utilized in a manner that will not negatively impact or threaten the security or integrity of the District's technology system.
 - 2.2.2. All property (intellectual and physical) created with District technology is the sole property of the District.



2.2.3. The District is aware that users, during personal time, may use District technology for non-District related purposes (e.g., personal banking, communications, etc.). The personal use of District technology must be appropriate and comply with this Administrative Practice and all District policies, practices, standards, and expectations. The District is not responsible for the loss of any personal data or information created or stored on District technology.

2.3. Etiquette and Privacy

2.3.1. Users are responsible for all activities carried out through their user accounts. All activities must be professional, respectful and factual.

2.3.2. All users are expected to conduct communications using the District's technology services in a courteous, respectful, and otherwise appropriate manner consistent with the Board's mission statement, Board policies, administrative practices, and the guidelines and expectations outlined in the student codes of conduct.

2.3.3. Users bear the sole responsibility for the material they choose to access, send, or display. Users should be aware the District has the right to monitor any network activity to maintain both the operation and appropriate function of the information network and records of use are automatically created.

2.3.4. Use of District technology, except as otherwise provided by law, Board policy or Administrative Practice (e.g. in relation to the District's use of student and employee information and records) is neither private nor confidential and may be monitored without notice.

2.3.5. Users will respect the privacy of others and not tamper with, open, or read other users' files, passwords and/or accounts.

2.4. The District is not responsible for:

2.4.1. Repair of privately-owned computers (hardware or software).

2.4.2. Compatibility problems with its networks, computers, and software.

2.4.3. Network connectivity problems.

2.4.4. Theft or damage to privately owned computers, software, or data.

2.4.5. Providing licenses for software used on privately owned computers.

2.5. Safety

2.5.1. The use of District technology or personal technology in relation to a school District activity or related activity must not result in a threat, real or potential, to the safety and welfare of students and/or staff or any other member of the school community.

2.5.2. All staff shall read and accept the conditions for appropriate and safe use of technology as outlined in this Administrative Practice.



- 2.5.3. Upon registering in a school, parent/guardian signs consent for student access to district technology (included on student registration form).
 - 2.5.4. All staff shall agree to Terms of Acceptable Use to access M365 suite as part of their account log in process.
 - 2.5.5. Information regarding the safe and appropriate use of District and personal technology shall be provided to students and staff by the Principal at the beginning of each school year.
3. Integrity and Plagiarism
 - 3.1 Technology must be utilized in a manner that upholds the integrity of the District, educational programs, and the school environment.
 - 3.2 Users must not copy or plagiarize any information obtained through District technology, personal technology, or any other means, and claim it as their own. Plagiarism is a serious offence. Students who engage in plagiarism will be subject to this Administrative Practice, the Student Code of Conduct and school rules.
 - 3.3 Users must comply with all District licensing agreements, provincial copyright laws and all Canadian law.
 4. Violations of Administrative Practice
 - 4.1 Violations of this Administrative Practice may result in privileges relating to District and personal technology being suspended or revoked.
 - 4.2 Inappropriate use of technology by students and staff may result in disciplinary action up to and including exclusion from school and termination of employment.
 - 4.3 Violations of this Administrative Practice may be reported to the appropriate law enforcement authorities and may also be subject to criminal investigations and/or criminal charges.
 - 4.4 The Superintendent or designate may from time to time exempt a user or department from compliance with this Administrative Practice where a valid business reason exists.