OTTAWA-CARLETON
DISTRICT SCHOOL BOARD

PROCEDURE PR.702.IT

TITLE: APPROPRIATE USE OF INFORMATION TECHNOLOGY (STAFF)

Date Authorized: **21 November 2001**
Last Revised: **25 June 2024**
Last Reviewed: **25 June 2024**

COMMITMENT TO INDIGENOUS RIGHTS, HUMAN RIGHTS, AND EQUITY

The District recognizes its responsibility to ensure that this procedure and the associated work promotes and protects Indigenous, equity, and human rights. The District will strive to address and eliminate discrimination and structural and systemic barriers for students, staff, and community.

1.0 OBJECTIVE

To support the implementation of Board Policy P.100.IT - Appropriate Use of IT.

2.0 DEFINITIONS

Please refer to Appendix A for a full list of definitions used in this Procedure.

3.0 RESPONSIBILITY

3.1 Supervisors are responsible for ensuring that

a) their staff are aware of OCDSB Policy P.100.IT Appropriate Use of IT and associated procedures; and

b) their staff adhere to appropriate use standards and report inappropriate use to Business and Learning Technologies (B&LT).

3.2 Business and Learning Technologies is responsible for overseeing staff usage of the District's Information Technology (IT) to ensure its integrity and safety.

3.3 Employees are responsible for complying with this procedure and with any relevant standards of their professional college or association where applicable.

4.0 PROCEDURES

Scope and Application

4.1 The implementation of this procedure will always be consistent with the *Human Rights Code* and Board Policy P.147.GOV Human Rights.

4.2 This procedure applies to staff use of District IT, as defined in Appendix A, as well as the use of personal IT in the OCDSB Environment.

Appropriate Use of Information Technology (IT)

4.3 All staff will use Information Technology (IT) appropriately including:

- c) complying with the following IT-focused requirements:
  - i) using IT for educational, business, and professional development, and health accommodation purposes only;
  - ii) taking reasonable measures to secure information and District-owned IT, including, but not limited to when left unattended;
  - iii) diligently backing up data;
  - iv) restricting uploading, downloading, transferring, and/or printing information or data to the information necessary to complete their task in the most resource-efficient manner. For example, when a staff member requires access to large amounts of data, information, or printing, they will discuss such requirements with their supervisor to assess the need and to obtain approval;
  - v) reporting any hardware, software, or security problem immediately to their supervisor;
  - vi) minimizing expectations for the use of IT outside of work hours;
  - vii) notifying Business and Learning Technologies immediately of suspicious cyber activity or potential breaches; and
  - viii) ensuring their assigned IT hardware and software are returned to B&LT, upon extended leaves of absence.

- d) complying with the following behavioural requirements:
  - i) passwords must not be shared;
  - ii) accepting new changing technologies and being willing to learn and use them in the workplace environment;
  - iii) adhering to copyright laws and licensing agreements;
  - iv) ensuring that online purchases of goods and services are made on appropriate and secure sites and that all transactions involve the legal exchange of goods, services, or information;
  - v) considering the most appropriate time, place, method and software tools when collaborating and communicating with others;
  - vi) recognizing the long-term physical and psychological effects of technology, for example, eye strain, repetitive stress syndrome, or the impact of reduced physical activity;

4.4 The following uses of District technology are prohibited:

- a) violating civil or criminal law using the District technology;

- b) recording, taking, or sharing non-consensual recordings or photos of other members of the OCDSB community;

- c) vandalism;

d) advertising the sale of weapons using District technology;

e) gaining unauthorized access to information resources, another person's materials, information, or files without permission of that person or attempting to log on as another user. This includes editing messages and issuing them under someone else's name;

f) using the District technology to communicate, transmit, relay, receive, or divulge inappropriate, threatening, racist, pornographic, offensive, hateful, slanderous, malicious, unlawful, or violent information about individuals;

g) using the District technology in political campaigns for municipal, provincial or federal elections, including advocating for or against specific candidates;

h) using the District technology to conduct business, pursue unauthorized commercial purposes or financial gain unrelated to the business of the District, offer or provide goods or services, or to advertise products;

i) unnecessarily demonstrating any hardware, software, or security problem to other Users;

j) intentionally finding or exploiting security gaps, experimenting on the school's network, or using the Board system in such a way as to disrupt the use of the system by other Users. This includes the distribution of system-wide chain letters or mass-mailings and spreading computer viruses; or sending Internet e-mail which might bring the Board into disrepute;

k) modifying the District's technology, without the express permission of Business & Learning Technologies;

l) using software, applications, hardware or other technology peripherals which have not been approved for use by Business and Learning Technologies; and

m) bypassing security systems and/or processes (e.g. using a VPN to avoid the school/district firewall).

4.5 In limited circumstances, the transmittal of unacceptable materials by employees may be necessary to fulfill a task in alignment with the enforcement of District policies and procedures.

4.6 If a User inadvertently accesses unacceptable materials or an unacceptable Internet site, they will immediately report it to their Supervisor and B&LT for follow-up.

Appropriate Use of Personal Mobile Devices

4.7 Limited use of Personal Mobile Devices by employees during the workday is permitted in accordance with the terms and conditions of use outlined in this procedure.

4.8 Employees are not permitted to use Personal Mobile Devices during instructional time unless it is for work-related purposes or as part of an approved accommodation.

Consequences of Inappropriate Use

4.9 Supervisors suspecting inappropriate and/or unlawful use of District technology will immediately report it to their Supervisory Officer.

4.10 The District will employ web filtering software to block out identified objectionable sites, and educate staff with regard to appropriate use and compliance with OCDSB Policy P.100.IT Appropriate Use of IT.

4.11 The District reserves the right to limit access to services, as such, violations of this procedure, including being a security risk or having a history of problems with other computer systems, may result in one or more of the following:

a) restriction, suspension, or cancellation of use or access privileges;

b) restitution for damages and repairs;

c) disciplinary actions governed by Collective Agreements and employment standards and practices, including termination of employment; and/or

d) civil or criminal charges under other applicable laws.

Liability

4.12 Accidental damage or loss of school or District equipment is the responsibility of the school or District department.

4.13 The District will not accept liability for loss, theft, or damage to any Personal Mobile Device(s) while on Board property, except where it can be shown that such loss was due to negligence on the part of the District, as per Procedure PR.552.FIN: Vandalism, Theft, Damage, or Loss Affecting Board Property.

5.0 APPENDICES

Appendix A: Procedure Definitions

6.0 REFERENCE DOCUMENTS

The Education Act, as amended, Section 170
The Accessibility for Ontarians with Disabilities Act (AODA)
OCDSB Policy P.074.IT: IT Security
OCDSB Policy P.100.IT: Appropriate Use of IT
OCDSB Policy P.125.SCO: School District Code of Conduct
OCDSB Procedure PR.672.IT: Electronic Communications Systems
OCDSB Procedures PR.564.IT: IT Security
OCDSB Policy P.032.SCO: Safe Schools (Managing Student Behaviour)
OCDSB Procedure PR.552.FIN: Vandalism, theft, Damage, or Loss Affecting Board Property
OCDSB Procedure PR 703 HR - Disconnecting From Work Related Communications
OCDSB “Community of Character"
M. Ribble, “Digital Citizenship: Using Technology Appropriately”
Ontario College of Teachers, Professional Advisory: Use of Electronic Communications and Social Media,

Council of Ministers of Education “Fair Dealing Guidelines” for Copyright

Appendix A: Procedure Definitions

In this procedure,

Board Property means all school buildings, grounds and facilities under the jurisdiction of the Board. It is also applicable, for example, on school buses, during field trips, or at school-sponsored events or in other circumstances which will have an impact on school climate.

District means the Ottawa-Carleton District School Board.

District Technology (IT) means a computer, phone, tablet, printer, photocopier, hard drive or other device, software, or network owned or operated by the District which stores, transmits or provides access to information, including personal or sensitive information.

OCDSB Community means employees, students, parents, guardians, trustees, committee members, school council members, caregivers, permit holders, vendors, service providers, contractors, volunteers, visitors, and all other persons learning, working, or accessing services in the OCDSB environment.

OCDSB Environment means Board property, school buses, virtual learning and working environment, electronic media, school or work-authorized events or activities, in before- and after-school programs including co-curricular activities and field trips, and may include any other circumstances that may have an impact on the school or work climate.

Personal Mobile Device means any personal electronic device that can be used to communicate or to access the Internet, such as a cellphone, tablet, laptop or smartwatch.

School Web Sites means all school and school council web pages.

Supervisor means superintendents, principals, vice-principals, and managers.

User means any member of the OCDSB Community using personal or District IT within the OCDSB Environment.

Vandalism means any malicious or unapproved attempt to disrupt, degrade, harm, modify, disable or destroy data or property of another user or organization, computer or network hardware or software, wiring or network system itself. This includes, but is not limited to, the uploading, creation, transmission, or installation of computer viruses, viral files or malicious software.

Virus means a destructive computer program that copies or attaches itself to an existing program without your permission.

Virtual Private Network (VPN) means a service that provides security and anonymity to users when they connect to web-based services and sites. A VPN hides the user’s actual public IP address and “tunnels” traffic between the user’s device and the remote server.