POLICY P.074.IT

TITLE: COMPUTER NETWORK SECURITY

Date Issued: **February 1999**
Last Revised: **XX *October 2019***
Authorization: **Board: 27 January 1999**

1.0 OBJECTIVE

To ensure the safety, security, integrity, and business continuity of computer network systems to protect the information ~~stored,~~ ***owned,*** processed, or transmitted electronically by the Ottawa-Carleton District School Board,

2.0 DEFINITIONS

In this policy,

2.1 Access means direct or indirect use, attempt to use, instruct, communicate with, cause input to, cause output from, or otherwise make use of any resources of a computer or other electronic device, computer system, facility or network.

2.2 Authorization means having the express or implied consent or permission of the owner, or of the person authorized by the owner to give consent or permission to access a computer, computer system, or computer network in a manner consistent with the authorized consent or permission.

2.3 Board means the Board of Trustees.

2.4 Computer refers to any electronic device or communication device that stores, retrieves, processes, or transmits data.

2.5 Computer system refers to a set of related, connected or unconnected, devices, software, or other related computer equipment.

2.6 Computer network means the interconnection of computers, electronic devices, software, or other equipment.

2.7 Computer property includes electronic impulses, electronically produced data, information, financial instruments, software, or programs, in either machine or

human readable form, any other tangible or intangible item relating to a computer, computer system, computer network, and copies of any of them.

2.8 Confidential means data, text, or computer property that is protected by a security system that clearly evidences that the owner or custodian intends that it not be available to others without the owner's or custodian's permission.

2.9 District means the Ottawa-Carleton District School Board.

2.10 Encryption or encrypted data refers to the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.

2.11 Information ~~is defined as~~ ***means all information holdings that are stored, transmitted, or processed electronically in the course of District business.***

2.12 Integrity of information means safeguarding information from unauthorized alteration or destruction.

2.13 Physical Assets ~~are defined as~~ ***refers to*** the information technology infrastructure, such as computers, ***devices,*** software applications, network ~~wiring~~ ***equipment and peripherals,*** encryption devices, etc. used in the processing, storage, and transmittal of information.

2.14 Security system refers to access control technologies such as encryption, password protection, and other forced authentication or access controls designed to keep out unauthorized persons.

2.15 Security Threats refers to any possible danger that might exploit a vulnerability to breach security safeguards and therefore cause possible harm to the District's information and/or physical assets.

2.16 Sensitive information refers to data that contains personally identifiable information.

3.0 GUIDING PRINCIPLES

3.1 The Board believes that:

a) a strong, reliable, and secure computer infrastructure is essential to ensuring an effective working and learning environment;

b) a secure infrastructure includes effective long-term contingency and incident management planning to prevent, manage and quickly recover from a security threat or any incident and reduce risk to the organization; and

c) on-going training and support to all employees on information security, possible threats, and safeguards is essential to implementing this policy.

3.2 Physical assets and any form of information received, created or gathered on behalf of the OCDSB in the course of District business are corporate assets and considered property of the OCDSB. ~~All information in the Board, in whatever form, stored on any media, is an asset and the property of the Ottawa-Carleton District School Board. Similarly, physical assets owned and utilized in the processing of this information are the property of the OCDSB.~~

4.0 SPECIFIC DIRECTIVES

~~***4.1*** This policy applies to all areas within the OCDSB and is in addition to existing Ottawa-Carleton District School Board policies and procedures and to sections of the *Education Act* pertaining to access to and retention of information or records.~~

~~***4.2*** Superintendents, principals and managers/supervisors are accountable for safeguardingSuperintendents, principals and managers/supervisors are accountable for safeguarding information and physical assets under their control. All employees are responsible for the protection of these assets from unauthorized use, modification, disclosure or destruction (whether accidental or intentional) and for maintaining the integrity of these assets and their availability to others as required in the performance of their duties.~~

~~***4.3*** The requirement to identify potential security threats and safeguard information and physical assets also applies to students, parent volunteers, vendors, consultants, and other organizations that are party to agreements between themselves and the OCDSB, as may be appropriate.~~

4.4 ***Stakeholders, including*** staff, ***trustees,*** parent***s*** ~~volunteers~~, students, vendors, consultants***, and partners, with OCDSB-owned*** information and physical assets under their control ***shall:***

a) safeguard the confidentiality and integrity of such assets;

~~b) protect such assets from unauthorized use, modification, disclosure or destruction (whether intentional or accidental);~~

c) maintain their availability to others as required in the performance of their duties; and

d) ***identify and report potential security threats and/or breaches.***

4.5 The District shall make every reasonable effort to protect and secure information and assets from threat, abuse and/or misuse, including through human error,

hardware malfunction, natural disaster, security break, and/or malicious attack.

~~***4.6*** Information and physical assets shall be classified as to their value, sensitivity, integrity, availability, and accountability requirements. In addition, information and physical assets shall be safeguarded according to procedures which include their classification and assessment of related risks.~~

Security Safeguards

4.7 ***The District shall ensure the security of all computers, computer networks and*** *computer property through:*

a) ***classifying them*** as to their ***risk,*** value, sensitivity, integrity, availability, and accountability requirements;

b) ~~Access to sensitive information and assets is restricted to those whose duties require such access.~~ ***controls on system access including an authorization process for granting and or revoking system access based on specific requirements which are necessary to perform a job;***

c) ***a documented change management process for handling system upgrades, installations, or changes to software and hardware;***

d) ***ensuring all equipment that contains sensitive information are secured to deter theft;***

e) ***requiring safe and secure use and storage of any computer or network device;***

f) ***ensuring their use is in accordance with Board Policy P.100.IT Appropriate Use of Technology; and***

g) ***establishing practices for automatic log off, and requirements for locks and password screen locks.***

4.8 ***The District shall ensure that server rooms and data closets are protected by appropriate access control which segregates and restricts access from general school or District office areas.***

4.9 ***No other person, including contractors, shall be allowed unescorted access to server rooms and data closets, unless expressly authorized.***

4.10 ***The District shall ensure network controls are in place to regulate traffic moving between internal (District) resources and external (Internet) entities.***

4.11 ***The District shall ensure that appropriate network segmentation is in place to protect the integrity of systems and data, using industry standards and current***

best practices to segment internal computer networks based on the data type, user access, and level of risk.

Incident Management

4.12 The District shall ensure that malicious software protection is installed on District-owned equipment, and shall ensure practices are in place to:

a) monitor for risk;

b) respond to malicious acts;

c) report incidents; and

d) manage incidents.

4.13 Monitoring and responding to technology related incidents shall be designed to provide early notification of events and rapid response and recovery from internal or external network or system attacks.

Business Continuity

4.14 The District shall develop and deploy a District-wide business continuity plan which shall, at a minimum, include:

a) data Backup Data procedures which establish a regular schedule for the collection of backup data and practices which ensure secure location of backup data; and

b) established practices for managing data in response to threats, attacks, and/or disasters.

Monitoring and Compliance

4.15 The District shall perform routine security and privacy audits in congruence with the District's Information Security Framework.

4.16 ~~All~~ Staff members ~~are responsible for~~ shall monitor~~ing~~ and enforce~~ing~~ compliance with this policy within the scope of their duties and responsibilities.

4.17 Violations or suspected violations of ~~these~~ ***staff*** responsibilities must be reported immediately to the appropriate ~~superintendent, principal or manager/~~ ***direct*** supervisor.

4.18 ***Staff*** ~~Persons~~ found to be in violation of this policy may be subject to ~~immediate~~ disciplinary action up to and including termination of employment ***with the District****.*

4.19 Legal action and/or referral of the matter to law enforcement agencies shall be considered depending on the severity of the violation, the real or potential loss to the Board, or breach of confidentiality.

4.20 ***Violations or suspected violations by OCDSB vendors, consultants, or partners shall be dealt with in accordance with the applicable Data Sharing Agreements.***

Implementation

4.21 The Director of Education ***is authorized to*** ~~shall~~ issue ***such*** procedures ~~to implement this policy~~ ***to ensure information and physical assets security is integrated within all aspects of the operations of the District.***

5.0 REFERENCE DOCUMENTS

The Education Act, 1998, ss. 170, 171
Board Policy P.027.GOV: Corporate Records Management
Board Policy P.049.IT: Electronic Communications Systems
Board Policy P.100.IT Appropriate Use of Technology
Board Policy P.128.GOV Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
~~Board Policy P.098.CUR Anti-racism and Ethnocultural Equity Board Policy P.053.HR Alleged Harassment/Abuse~~
Board Procedure PR.516.GOV Corporate Records Management Board Procedure PR.564.IT Computer Network Security
Board Procedure PR.622.IT Appropriate Use of Technology
Board Procedure PR.669.GOV Privacy Breach
Board Procedure PR.672.IT Electronic Communications Systems
Board Procedure PR.685.IT Mobile Devices