



**DURHAM CATHOLIC
DISTRICT SCHOOL BOARD**
Learning and Living in Faith

POLICY – 431

Acceptable Use of Information and Communications Technology

Area: Operations

Source: Chief Information Officer – Freedom of Information and Privacy

Approved: February 11, 2008

Revised: November 10, 2014

1. Introduction

It is the policy of the Durham Catholic District School Board to provide and maintain access to Information and Communications Technology (ICT) for use by students, employees and other users in a manner which is consistent with the Ontario Catholic School Graduate Expectations, the Board's strategic plan, mission and vision statements, Catholic virtues and values, Ministry of Education guidelines and with all relevant federal and provincial laws and regulations.

Inappropriate use of technology exposes the Board and users to cybercrime such as data breach, viruses and malware, and ransomware attacks. The intent of this policy is to protect the Board and users from illegal or damaging actions of individuals or organizations either knowingly or unknowingly.

2. Definitions

Canada's Anti-Spam Legislation (CASL) – a Canadian law that protects consumers and businesses from the misuse of digital technology, including spam and other electronic threats

Cloud (Cloud Computing) – the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. The term is generally used to describe data centers available to many users over the private or public Internet.

Cybercrime – criminal activity that either targets or uses a computer, a computer network or a networked device. Most, but not all, cybercrime is committed by

cybercriminals or hackers who want to make money. Cybercrime is carried out by individuals or organizations.

Data breach – a security violation in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve financial information such as credit card or bank details, first name, last name, email address, phone number, home address, etc.

Digital Citizenship – outlines the norms of appropriate and responsible behaviour as it relates to technology use, including hardware, software, Internet usage and social media.

Information and Communications Technology (ICT) – technologies that provide access to information through telecommunications. It is similar to Information Technology (IT), but focuses primarily on communication technologies. This includes the Internet, wireless networks, cell phones, and other communication mediums.

Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) – an act that establishes a general right of access to the information held by local governments and institutions. The Act also protects the privacy of individual's personal information that are part of government records.

Personal Health Information Protection Act (PHIPA) – an Ontario law that governs the collection, use and disclosure of personal health information within the health sector. The object is to keep personal health information confidential and secure, while allowing for the effective delivery of health care. Under this legislation, persons and organizations that provide health care are collectively known as health information "custodians".

Personal Technology – any device that is not Board provisioned, such as, but not limited to, personal computers, personal laptops, smart phones and tablets.

Ransomware – a type of malicious encryption software designed to block access to a computer, server, or database system until a sum of money is paid.

Viruses and Malware – destructive computer programs or malicious code designed to spread from one computer to another or attach themselves to an existing program without authorization to encrypt data or steal data.

3. Purpose

The purpose of this policy is to outline the acceptable use of information technology resources such as computers, software, social media, Internet and Intranet and other technology hardware within the Durham Catholic District School Board for the protection of all parties involved.

Since inappropriate use of the Board's technology systems exposes the organization to risk, it is important to specify exactly what is permitted and what is prohibited.

4. Application / Scope

This policy and its attendant administrative procedure apply to the Board of Trustees, Director of Education, Chief Information Officer, employees, students, parents/guardians, and external contractors/consultants when accessing the Board's ICT.

5. Principles

- 5.1 The Durham Catholic District School Board recognizes the inherent value that technology can bring to support student success and foster well-being, business excellence and employee development. The acquisition of knowledge, skills and attitudes for digital citizenship will support inclusivity, positive and meaningful relationships, innovation, engagement, responsibility and optimism.
- 5.2 Technology can contribute to effective instruction and learning if used appropriately.
- 5.3 Use of computers, software, social media, Internet and Intranet technology and other technology hardware should be used in a safe and ethical manner and appropriate to the needs and well-being of all members of the Board community.
- 5.4 For security and network maintenance purposes, authorized individuals within the Board may monitor equipment, systems and network traffic at any time. To ensure that personal documents and communications remain private, the user should use their own personal technology resources rather than connecting to or using the Board's technology, such as Internet, email, collaboration tools, digital learning and web-based conference platforms.
- 5.5 Where it is determined that users have breached this policy, the Board will take appropriate measures to address the situation. This may include, but is not limited to disciplinary action, where appropriate, and in accordance with all applicable Board policies and procedures.
- 5.6 Personal and private information of students and staff members is protected under the Municipal Freedom and Protection of Privacy Act. The Board is obligated by this Act to carefully manage all personal information within our custody and control how it is collected, used and released.

6. Requirements

- 6.1 The Director of Education, or designate, shall issue administrative procedures to support this policy and amend them thereafter as the need may arise.
- 6.2 The Board is committed to effective digital citizenship and expects the same of all students and staff. This includes creating a positive school and work culture which supports the safe and responsible use of ICT.

- 6.3 All use of the Board's technology, Internet and Intranet by users shall support education, classroom activities, professional and/or career development. Board technology is not intended for personal or private use. Information stored on Board devices, Board network, and Board Cloud storage are subject to the MFIPPA, which gives members of the public the right of access to information (example: emails, voicemails, text messages, file, etc.) upon request.
- 6.4 The Board supports efficient, ethical and legal utilization of technology and internet resources. The Board has the right to monitor the individual users of its technology and information systems. The smooth operation of the network is dependent upon user adherence to the guidelines in accordance with the administrative procedures attendant to this policy.
- 6.5 Staff shall promote and encourage acceptable use of the Board's computer system and access to the Internet/Intranet to support the delivery of curriculum, and shall provide guidance, support and instruction to students with respect to use.
- 6.6 All Trustees, staff, consultants and volunteers who use Board's technology and Internet/Intranet shall become familiar with this policy and its attendant administrative procedures.
- 6.7 All students are required to review the School Code of Conduct annually which addresses the Acceptable Use of Information and Communications Technology Policy and the expectations for students respectively.
- 6.8 With access to the Internet comes the availability of material that does not have educational value in the context of the school setting. Staff shall supervise, guide and monitor student access to the Internet.
- 6.9 The principal/manager shall be responsible for content, copyright and the protection of privacy of all web pages created for the school/department.
- 6.10 The use of recording devices (e.g., cameras, video/audio recorders, webcams, integrated digital cameras and video recorders in smart phones) cannot be used in a manner that violates the privacy and dignity of others. Inappropriate use of all of these, and similar devices will result in temporary confiscation of the device and additional restrictions and further consequences may result. We must follow the CASL compliance.
- 6.11 Inappropriate technology or internet/intranet use will result in appropriate disciplinary actions in accordance with the administrative procedure attendant to this policy.
- 6.12 All employees must ensure their use of information technology resources such as computers, software, Internet and Intranet and other technology hardware within the Durham Catholic District School Board is in accordance with federal and provincial laws regulations such as MFIPPA, CASL and PHIPA.

6.13 The Board retains the right to deny access to anyone using Board provided resources, regardless of location, when used for a purpose other than the spirit and intention for which they are granted. The Board also retains the right to inspect any board provided computer or ICT device, or system and to monitor the use of any of the technology, including, without limitation, inspecting the contents of files, voicemail, email, or other digital communication. This action may include, but not be limited to, disciplinary action according to the law, and the policies and procedures of the Board.

7. Sources

- 7.1 [Education Act, R.S.O. 1990, Section 170](#)
- 7.2 [Municipal Freedom of Information and Protection of Privacy Act \(MFIPPA\)](#)
- 7.3 [Canada's Anti-Spam Legislation \(CASL\)](#)
- 7.4 [Personal Health Information Protection Act \(PHIPA\)](#)

8. Related Policies and Administrative Procedures

- 8.1 Acceptable Use of Information and Communications Technology Administrative Procedure (AP431-1)