DURHAM CATHOLIC DISTRICT SCHOOL BOARD
Learning and Living in Faith

No Changes

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; January 10, 2022

1. Introduction

It is the policy of the Durham Catholic District School Board (the "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

Nil

3. Purpose

The purpose of this policy is to define standards, procedures, accountability, and restrictions for end users who have legitimate business requirements to access Board data from a device connected to an unmanaged network outside of the Board's direct control. The policy applies to any hardware and related software that could be used to access Board resources, even if this equipment is not Board sanctioned, owned or supplied.

The overriding goals of this policy are to protect the integrity of the private and confidential business data that resides within the Board's technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently stored unsecurely on a device or carried over an unsecure network where it can potentially be accessed by unsanctioned sources. A breach of this type could result in loss of information, damage to critical applications, and damage to the Board's public image.

All users employing a device connected to an unmanaged network outside of the Board's direct control to back-up, store, and otherwise access Board data of any type must adhere to Board-defined processes for doing so. This policy provides staff accountability for loss, stolen or damaged Board issued devices.

4. Application / Scope

This policy and its attendant administrative procedure apply to the Board of Trustees, employees (full and part-time), students, parents/guardians, and external contractors/consultants or any other agents who utilize either Board-owned or personally owned devices to access, store, back-up, relocate or access any organization or client-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust the Board has built with its device users. Consequently, employment at the Board does not automatically guarantee the initial and ongoing ability to use these devices to gain access to the Board's networks and information. It addresses a range of threats to, or related to the use of, enterprise data.

5. Principles

5.1 The Board of Trustees 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 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 integrity of the system and compliance with procedures. This includes personal devices connected to the Board's ICT. 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 Personal and private information of students and staff members stored in various applications (e.g., student information system, human resources/payroll) is protected under the Municipal Freedom of Information and Protection of Privacy Act ("MFIPPA"). 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 When using Board provided technology including Board email, Board provided credentials or Internet services, all email and Internet communications sent and received by users are the property of the Board. Email, Internet, or voicemail communications are not private or personal despite any such designation by the sender or the recipient. Personal or private communications transmitted on the Board's electronic information system may be accessed, reviewed, copied, deleted, retained, or disclosed by the Board at any time and without notice.

6.3 The Board reserves the right to use any monitoring activity, and may access any files, documentation, electronic communications and use of Internet at its discretion at any time as is reasonable in the circumstances in the event of an investigation of a safety, legal, administrative or disciplinary nature.

6.4 The Board is committed to 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.

6.5 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.

6.6 All users should be aware that the Board must comply with Freedom of Information requests for the production of records in its custody and control not subject to an exemption, including information recorded and stored electronically (e.g, emails, browsing history, documents, etc.).

6.7 All users of ICT must comply with the Board's obligation under MFIPPA not to disclose personal information, including information stored electronically, unless authorized under MFIPPA.

6.8 The Board supports efficient, ethical and legal utilization of ICT. Where there are reasonable and probable grounds to believe that there has been a contravention of this or other policy or procedure, professional code, code of conduct or other statute, regulation or Ministry of Education requirement, the Board may initiate an investigation that may include the seizure, search and/or monitoring of Board ICT.

6.9 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.

6.10 Use of Board ICT by all Trustees, staff, consultants and volunteers constitutes agreement to comply with the terms and expectations outlined in this policy and its attendant procedures.

6.11 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.

6.12 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 to the extent that is reasonable under the circumstances.

6.13 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.

6.14 All employees must ensure their use of information technology resources such as computers, software, Internet and Intranet and other technology hardware within the Board is in accordance with federal and provincial laws and regulations such as MFIPPA, Canada's Anti-Spam Legislation ("CASL") and Personal Health Information Protection Act ("PHIPA").

6.15 All users of Board ICT must respect intellectual property rights, and that the Board retains ownership of all intellectual property created for work-related purposes using Board ICT.

6.16 All users of Board ICT are prohibited from downloading Board data to personal devices. If personal devices are being used for work-related purposes, they must be password protected.

6.17 The Director or designate 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.

6.18 Where it is determined that users have breached this policy, the Director or designate 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.

6.19 The Board will not be held responsible for the loss or damage of any personally owned device.

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)
7.5 Bill 88, Working for Workers Act, 2022

8. Related Policies and Administrative Procedures

8.1 Acceptable Use of Information and Communications Technology Administrative Procedure (AP431-1)
8.2 Acceptable Use of Mobile Devices (AP431-2)
8.3 Data Access and Management Policy (PO427)
8.4 Data Access and Management Administrative Procedure (AP427-1)