DURHAM CATHOLIC DISTRICT SCHOOL BOARD
Learning and Living in Faith

ADMINISTRATIVE PROCEDURE – 431-1

Acceptable Use of Information and Communication Technology

Area:	Operations
Policy Reference:	Acceptable Use of Information and Communication Technology (PO431)
Approved:	February 11, 2008
Revised:	November 10, 2014; October 11, 2022

1. Purpose

The purpose of this administrative procedure is to provide a framework for implementing the Acceptable Use of Information and Communication Technology Policy (PO431).

2. Definitions

Nil

3. Procedures

3.1 User responsibility

3.1.1 Users will not knowingly transmit, relay or receive information or materials that are threatening, racist, pornographic, homophobic or that are malicious, inappropriate and/or unlawful. Users are advised that email constitutes a legal document. Existing laws for libel and or defamation of character apply. Email is also subject to legal subpoena.

3.1.2 All users will acknowledge their rights and responsibilities by becoming familiar with the Acceptable Use of Information and Communication Technology Policy (PO431) and its attendant administrative procedures.

3.1.3 All users agree to immediately (within 24 hours) report any incident or suspected incidents of unauthorized data access, data loss and/or disclosure of company resources, databases, networks, etc. to their Superintendent or designate and the Board's ICT department. Any questions relating to this policy should be directed to the CIO.

3.1.4 All users who are not employees of the Board who apply for access to this service will sign and submit to the appropriate principal, supervisor or manager the Acceptable Use of Information and Communication Technology Agreement Form (Form AF431-1) (see Appendix 1) and read and understand the Acceptable Use of Information and Communication Technology Policy (PO431) and Administrative Procedure (AP431-1) prior to signing.

3.1.5 If a user inadvertently accesses unacceptable materials or an unacceptable internet site, the user will immediately exit, and disclose the inadvertent access to a principal, appropriate supervisor, manager or designate immediately (within 24 hours). This disclosure may serve as a defence against an allegation that the user has intentionally violated Board policy and its attendant administrative procedure.

3.1.6 Users will exercise extreme caution about revealing personal information to others. For example, passwords should not be shared with family or friends, nor should personal information be disclosed.

3.1.7 Users will not gain unauthorized access to information resources, another person's materials, information or files without permission of that person, nor will they attempt to log on as another user.

3.1.8 Users will familiarize themselves with and respect copyright laws and licensing agreements as well as the Board's Copyright Policy (PO439) and its attendant administrative procedure (AP439-1). Users will not knowingly plagiarize works, for example text or images they find on the internet, nor will they use another person's property without that person's approval. Where approval is received the appropriate acknowledgements shall be cited.

3.1.9 Users will make no modifications of any kind to Board-owned and installed hardware or software without the express approval of the Board's ICT department. This includes, but is not limited to, any reconfiguration of devices.

3.1.10 Exclusions

a) Users will not use Board technology:

- to conduct or assist political campaigns for municipal, provincial or federal elections, including advocating for or against specific candidates or causes;
- to communicate or divulge inappropriate information about individuals;
- to conduct a business;
- to pursue unauthorized commercial purposes or financial gain unrelated to the business of the Board;
- to offer to provide goods or services or to advertise products;
- to search for or purchase goods or services for personal use.

3.1.11 Users must report any hardware, software or security problem immediately to their principal, supervisor or manager. Installation of any hardware or software

is prohibited as is 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 for other users.

3.1.12 Vandalism is prohibited. Vandalism is defined as any malicious 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. Use of non-Board hardware or software, for example personal laptops, handheld devices or peripheral devices, on the network environment is prohibited without the authorization of the principal, supervisor or manager.

3.1.13 Inappropriate use of digital material is prohibited. For example, the posting of images or data containing personal information on the internet without the consent of the individual, principal/supervisor/manager.

3.1.14 While the Board recognizes that there are occasions when staff will send or receive appropriate personal communication through the Internet, provided that this is not a deterrent to their responsibilities, other use of any form of electronic communication such as emails, chats, social media or newsgroups without an educational purpose, network etiquette and conventions shall apply, and compliance with all terms and conditions of use outlined in Board policy is expected of all users.

3.1.15 Employees who are not actively reporting to work for an extended period will not retain possession of Board-issued devices (e.g., retired, short/long term disability, maternity leave, termination, resignation).

3.2 Author Responsibility

3.2.1 It is the choice of the individual departments whether or not they wish to post additional webpages to the Board main website. Such postings require the approval of the Superintendent or designate.

3.2.2 The Superintendent or designate holds the responsibility for content, copyright and protection of privacy on all webpages created for the school/department.

3.2.3 Only Board employees and those designated by the Information and Communication Technology (ICT) department may manage and maintain content on Board websites, under the direction of the Superintendent or designate.

3.2.4 The content of Board web pages must be consistent with the educational aims of the Board and consistent with the letter and the spirit of the Board policy.

3.2.5 Hyperlinks from school and/or department web pages to non-Board sites are permitted for educational purposes but these links must be checked regularly to ensure the links are functioning and the content remains appropriate.

3.2.6 Web pages created on non-Board servers for curriculum or communication purposes must be linked directly from a web page residing on a Board server. The content of each web page must be consistent with the educational aims of the Board and with the letter and the spirit of Board policies. These web pages must be checked regularly to ensure the links are functioning and content remains appropriate.

3.2.7 Personal web pages for students, without an educational purpose and outside of the context of classroom instruction will not be supported. Similarly, staff members may create pages, which have educational value and relevant to their teaching. In the interest of protecting Board web content, linking to a student's or staff member's personal web page on an external site is not supported.

3.2.8 School web pages must not contain commercial or promotional advertising. School events and fundraising activities are acceptable, as are acknowledgements of school partnerships or sponsorships consistent with Board policies. Schools may provide links to partners' or sponsors' web pages, but these links must be checked regularly to ensure the links are functioning and the content remains appropriate.

3.3 Responsibility for Technology: Availability, Reliability and Quality of Service

3.3.1 The Board through its ICT department will endeavour to provide reliable and quality service to all users during business hours. The Board:

a) makes no warranty of any kind, whether expressed or implied, for the service provided;

b) will not be responsible for any damages suffered, including loss of data resulting from hard drive failure, reimaging, delays or service interruptions;

c) is not responsible for the accuracy or quality of information obtained through internet services;

d) will attempt or assist to track down the source of any inappropriate information, email message, etc.

3.3.2 Educating our users, with regard to appropriate use and encouraging compliance with the Acceptable Use of Information and Communication Technology Policy and its attendant administrative procedure remains the best protection. An annual review of Internet Safety will be provided by Principals to staff and students at the beginning of each school year.

3.3.3 The right of the Board to access an employee's internet history, documents and/or voicemail on Board provided technology or personal devices when using Board credentials may arise in a number of situations, including but not limited to:

- compliance with disclosure requests or orders made pursuant to the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA);
- regular or special maintenance of the electronic information systems for Board owned technology;
- business-related need to access the employee's system, including, for example, when the employee is absent from work or otherwise unavailable;
- compliance with obligations to disclose relevant information in the course of a legal proceeding; and
- when the Board has reason to believe that there has been a violation of policy, or is undertaking an administrative, legal or disciplinary investigation.

Appendix 2 details routine electronic monitoring activities, mechanisms and purposes. The Board reserves the right to use any other monitoring activity 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.

3.4 Use of Board and School Equipment and Materials

3.4.1 All members of the Durham Catholic District School Board, including but not limited to trustees, staff, parents/guardians and students shall use Board equipment and materials for the purpose of the improvement of student achievement or Board sanctioned events or activities.

3.4.2 Permission from the principal or appropriate supervisor is required in situations where Board equipment or materials is taken off Board premises for Board sanctioned activities and events.

3.4.3 In situations where Board equipment or materials are used off Board premises, the principal, or appropriate supervisor shall be responsible for the care and safe keeping of any equipment and materials.

3.5 Misuse and Consequences of Misuse

3.5.1 Where a computer user violates any of the above terms and conditions, one or more of the following consequences may occur:

a) suspension or cancellation of user privileges;

b) liability for payment for damages and repairs (replacement or refresh cost, whichever is less);

c) discipline under other appropriate Board policies, including suspension, expulsion, exclusion or termination of employment; or

d) civil or criminal liability under other applicable laws.

Should an infraction occur, Board and/or school administration may immediately revoke user privileges. Any user identified as a security risk or as having a history of problems with other computer systems may be denied access to the Board's WAN and all related services.

3.6 Personally Owned Electronic Devices for Bring Your Own Device (BYOD)

3.6.1 Use of a personally owned electronic device is considered a privilege and breach of any terms and conditions associated with its use may result in cancellation of those privileges and/or disciplinary actions.

3.6.2 Disciplinary action, including, but not limited to suspension or involvement of police services, may be imposed in response to any violation of this policy when deemed necessary by the Administration based on the circumstances surrounding the offence.

3.6.3 Personally owned electronic devices may be used during instructional periods and at times and in locations as determined and permitted by the school principal and/or teachers.

3.6.4 When a student is using a personally owned electronic device without the permission of a teacher or principal, they will be subject to progressive discipline (e.g., may include, but not limited to, turning in his/her device to a teacher for a period or a day, turning in his/her device to administration for a period of time, losing the privilege of using a personally owned electronic device for a period of time).

3.6.5 When the use of personally owned electronic devices has not been authorized, they must be securely stored in a silent mode out of the sight of students and staff.

3.6.6 Personally owned electronic devices should be password protected and students are strongly encouraged to never share passwords with another party.

3.6.7 DCDSB, its schools, or its agents, will not assume responsibility for the loss, recovery, damage, repair or replacement of any personally owned electronic device brought onto Board premises, on school excursions or while the personally owned electronic device has been confiscated.

3.6.8 Personally owned electronic devices may only be connected to the Board's Wi-Fi network and never into the Board's LAN via Ethernet or other hardwire connection.

3.6.9 Unless legally licensed, users will not install software licensed by the Board or Ministry on personally owned electronic devices.

3.6.10 Prohibited use of personally owned electronic devices that may result in a student receiving disciplinary action include, but are not limited to:

a) academic integrity being compromised (e.g., use during tests or exams);

b) disruption to the instructional day or teaching-learning environment (e.g., unsanctioned use in class);

c) recording of activities that may negatively impact school climate including, but not limited to, recording any person without their consent;

d) violation of a person's reasonable expectation of privacy including, but not limited to:

- use in washrooms;
- posting of a person's image(s) on the internet or in hard copy;
- taking pictures of individuals without consent. The consent of the parent/guardian is required for all students under the age of 18;
- emailing pictures and/or recordings of individuals without consent;
- sending inappropriate text messages or images;
- compromising personal and/or school safety (e.g., bullying);
- any other situation deemed by school Administration where school security, safety, individual privacy or academic integrity is compromised.

3.6.11 Technical problems with personally owned electronic devices will not be assessed or supported by Board Information Technology staff.

3.6.12 In the event of an emergency lockdown there is to be no use of personal devices unless necessary to communicate regarding the incident and directed by the supervisor(s) (e.g., teacher, administrator). Personal devices should be shut off or in silent mode.

3.6.13 All users should be aware that in some instances, transmissions, recordings or images may be reviewed and relied on, in disciplinary matters subject to search and seizure and privacy legislation.

3.6.14 Teachers and support staff are not to store pedagogical data (e.g., student images, videos) on personally owned electronic devices.

4. Sources

4.1 Education Act, R.S.O. 1990, c. E.2.
4.2 Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
4.3 Bill 88, Working for Workers Act, 2022
4.4 Employment Standards Act, 2000

5. Appendices

5.1 Appendix 1 – Acceptable Use of Information and Communication Technology Agreement Form (Form AF431-1)
5.2 Appendix 2 – Electronic Monitoring Activities

6. Related Policies and Administrative Procedures

6.1 Freedom of Information and Protection of Privacy Policy (PO201)
6.2 Privacy Breach Protocol Administrative Procedure (AP201-2)
6.3 Acceptable Use of Information and Communication Technology Policy (PO431)
6.4 Copyright Policy (PO439)
6.5 Copyright Administrative Procedure (AP439-1)
6.6 Communications Policy (PO440)
6.7 Media Relations Administrative Procedure (AP440-1)
6.8 Crisis Communications Administrative Procedure (AP440-2)
6.9 Media Consent Administrative Procedure (AP440-3)
6.10 Code of Conduct Policy (PO610)
6.11 Code of Conduct Administrative Procedure (AP610-1)
6.12 Student Discipline Policy (PO611)
6.13 Student Discipline Administrative Procedure (AP611-1)
6.14 Bullying Prevention and Intervention Policy (PO612)
6.15 Bullying Prevention and Intervention Administrative Procedure (AP612-1)

Appendix 1

DURHAM CATHOLIC
DISTRICT SCHOOL BOARD
Learning and Living in Faith

Acceptable Use of Information and Communication Technology Agreement Form

Please sign and return to school

To Students, Parents/Guardians and Community Members:

By signing below you are indicating that you have read the Durham Catholic District School Board Acceptable Use of Information and Communication Technology Policy (PO431) and that you understand the contents. The policy is available in any school office and is also available on the Board's website: http://www.dcdsb.ca

As a student or community member who signs this document, you agree to abide by the Board's Acceptable Use of Information and Communication Technology Policy (PO431) and acknowledge that unacceptable use of Information Technology per the Code of Conduct Policy (PO610) and Student Discipline Policy (PO611) can result in formal discipline.

As a parent/guardian who signs this document, you are aware of the behavior expected of students, and that the use of the Internet in Durham Catholic District School Board sites is strictly for educational purposes.

Student's/Community Member's Full Name (Please Print):_____

Student's/Community Member's Signature:_____

Date:_____

*If student is younger than 18 years of age:

Parent/Guardian's Full Name (Please Print):_____

Parent/Guardian's Signature:_____

Date:_____

Form Number: AF431-1
Related Administrative Procedure: AP431-1 Acceptable Use of Information and Communications Technology

Appendix 2 – Electronic Monitoring Activities

1. Web Filtering is used to monitor all internet traffic using firewalls to protect from harmful and inappropriate content.
2. Secure Access Service Edge (SASE) is used to monitor all internet traffic using firewalls to protect from harmful and inappropriate content.
3. Email Filtering is used to monitor all email traffic using data loss prevention to prevent the transmission of private/confidential data over insecure email.
4. Account authentication is used to monitor staff login to services using active directory to protect against unauthorized access.
5. Mobile Device Management software is installed on all Board-issued iPads/iPhones/Laptops to protect against loss/theft, and enforce security policies and settings.
6. Device Management (Chromebook) is installed on all Board-issued Chromebooks using Google Management Console to protect against loss/theft, and enforce security settings.
7. Video surveillance cameras and recording systems (external and public areas only) are used in some schools for safety purposes and to protect against theft and illegal activity, and for behavioural/incident monitoring and review.
8. Global Positioning System (GPS) tracking systems and associated software are installed in all board-owned vehicles to protect against loss and theft and to support staff safety in the case of a breakdown. GPS is also used in administrative investigations.
9. Door Fob systems are used in all Board owned buildings to control and monitor access.