



**BRANT HALDIMAND NORFOLK
Catholic District School Board**

Agenda
Catholic Education Centre
322 Fairview Drive
Brantford, ON N3T 5M8

**Policy Committee Meeting
Tuesday April 21, 2026 ♦ 3:00 p.m.
Boardroom**

Trustees:

Dan Dignard (Chair), Dennis Blake, Bill Chopp, Carol Luciani, Toni Poirier
Rick Petrella (on leave)

Senior Administration:

Mike McDonald (Director of Education & Secretary), Rajini Nelson (Superintendent of Business & Treasurer)
John Della Fortuna, Kevin Greco, Michael Lawlor, Phil Wilson (Superintendents of Education)

1. Opening Business

- 1.1 Opening Prayer
- 1.2 Attendance
- 1.3 Approval of the Agenda
- 1.4 Approval of Minutes from the Policy Committee Meeting – March 10, 2026. Pages 2-3
- 1.5 Business Arising from the Minutes

2. Committee and Staff Reports

- 2.1 ITS #600.02 – Information and Communications Technology Use Pages 4-16
Presenter: John Della Fortuna, Superintendent of Education
- 2.2 OPS #400.18 – Electronic Monitoring Pages 17-20
Presenter: John Della Fortuna, Superintendent of Education

3. Adjournment

Next meeting: Tuesday May 19, 2026 – 3:00 p.m.



BRANT HALDIMAND NORFOLK Catholic District School Board

Minutes

Catholic Education Centre
322 Fairview Drive
Brantford, ON N3T 5M8

Policy Committee Meeting Tuesday March 10, 2026 ♦ 4:00 p.m. Board Room/ Microsoft Teams

Trustees:

Dan Dignard (Chair), Dennis Blake, Bill Chopp, Carol Luciani, Toni Poirier

Regrets: Rick Petrella (on leave)

Senior Administration:

Mike McDonald (Director of Education & Secretary), Rajini Nelson (Superintendent of Business & Treasurer)
John Della Fortuna, Kevin Greco, (Superintendents of Education)

Regrets: Michael Lawlor, Phil Wilson (Superintendents of Education)

1. Opening Business

1.1 Opening Prayer

The meeting was opened with prayer led by Trustee Dignard.

1.2 Attendance

Attendance was noted as above.

1.3 Approval of the Agenda

Moved by: Carol Luciani

Seconded by: Dennis Blake

THAT the Policy Committee of the Brant Haldimand Norfolk Catholic District School Board approves the agenda of the March 10, 2026, meeting.

Carried

1.4 Approval of Minutes from the Policy Committee Meeting – February 17, 2026

Moved by: Toni Poirier

Seconded by: Carol Luciani

THAT the Policy Committee of the Brant Haldimand Norfolk Catholic District School Board approves the minutes of the February 17, 2026, meeting.

Carried

1.5 Business Arising from the Minutes - Nil

2. Committee and Staff Reports

2.1 Police Records Check Policy #300.15

Superintendent Greco presented the revised Police Records Check Policy. The revised Policy includes amendments to align with new legislation including the requirement for employees to renew their Police Records Check every five (5) years. The revision provides a clear distinction between the levels of Police Records Check and specifically the Criminal Record and Judicial Matters Check (CRJMC) and the Vulnerable Sector Check (VSC). The type of Police Records Check required for each position will be determined by the Board. The new provisions also apply to students participating in educational placements, practicum or other work integrated learning opportunities within Board schools or facilities, as required under Ontario Regulation 521/01. It was noted that the annual offence declaration still needs to be completed by employees. Discussion around communication with staff was had along with the associated



costs to the employee. Further clarification was sought around what is included with the Vulnerable Sector Police Records Check.

Moved by: Toni Poirier

Seconded by: Carol Luciani

THAT the Policy Committee recommends that the Committee of the Whole refers the Police Records Check Policy #300.15 to the Brant Haldimand Norfolk Catholic District School Board for approval.

Carried

2.2 Community Use of Schools Policy #400.05

Superintendent Nelson presented the Community Use of Schools Policy. The Community Use of Schools Policy and Administrative Procedure were reviewed to ensure they remain current and aligned with Board practices, Ministry guidance, and operational requirements. Changes around hours for public use were clarified and adjusted to better align with operational requirements and the Board's cost recovery model. The approval processes within the administrative procedure were updated to reflect the current organizational structure and responsibilities within facility services and school administration. The roles and responsibilities of staff and permit holders were revised to improve clarity and ensure alignment with current operational practices. The Superintendent of Business and Treasurer will review and establish the Community Use of Schools Rates and Fees annually, with any revisions reported to the Board for information, as appropriate. Discussion was had surrounding the categories of the fees for non-profit groups and parishes.

Moved by: Bill Chopp

Seconded by: Dennis Blake

THAT the Policy Committee recommends that the Committee of the Whole refers the Community Use of Schools Policy #400.05 to the Brant Haldimand Norfolk Catholic District School Board for approval.

Carried

3.0 Adjournment

Moved by: Dennis Blake

Seconded by: Bill Chopp

THAT the Policy Committee of the Brant Haldimand Norfolk Catholic District School Board adjourns the March 10, 2026, Policy committee meeting.

Carried.

Next meeting: April 21, 2026, 3:00pm – Boardroom

**REPORT TO THE BRANT HALDIMAND NORFOLK CATHOLIC
DISTRICT SCHOOL BOARD POLICY COMMITTEE**

Prepared by: John Della Fortuna, Superintendent of Education
Presented to: Policy Committee
Submitted on: April 21, 2026
Submitted by: Mike McDonald, Director of Education & Secretary

**INFORMATION AND COMMUNICATIONS TECHNOLOGY USE
POLICY ITS #600.02**
Public Session

BACKGROUND INFORMATION:

The Brant Haldimand Norfolk Catholic District School Board relies on information and communications technology (ICT) to support student learning, Board operations, and effective communication. The Information and Communications Technology Use Policy, ITS #600.02 establishes and outlines expectations for the safe, responsible, and appropriate use of Board technology resources by all users, in alignment with Catholic values, legislation, and Ministry of Education directives.

DEVELOPMENTS:

The revised policy reflects updated Ministry requirements and emerging operational needs, including:

- Clarified accountability under the Superintendent of Education, Information/Technology.
- Alignment with PPM 128, including restrictions on social media access and expectations for personal mobile device use during instructional time.
- Introduction of a formal governance framework for digital tools, applications, and artificial intelligence platforms.
- Strengthened cybersecurity, privacy, and incident reporting expectations, including mandatory staff training.
- Updated user responsibilities related to acceptable use, data protection, and system security.

The next scheduled review of this policy will occur during the 2029-2030 review cycle.

RECOMMENDATION:

THAT the Policy Committee recommends that the Committee of the Whole refers the Information and Communications Technology Use Policy ITS #600.02 to the Brant Haldimand Norfolk Catholic District School Board for approval.



Information and Communications Technology Use #600.02

Adopted:	September 9, 2003
Last Reviewed/Revised:	August 28, 2024 April/May 2026
Responsibility:	Superintendent of Education, Information/Technology
Next Scheduled Review:	2025-26 2029-2030

Policy Statement

The Brant Haldimand Norfolk Catholic District School Board believes that network, computer systems, and associated resources are integral to the education environment and must be available for student learning and the Board's business. We commit to using these technologies in a manner consistent with Catholic values, emphasizing responsible and appropriate use. In alignment with PPM 128, access to social media platforms is restricted on all Board/school networks and devices, and personal mobile devices must not be used during instructional time except under specific circumstances. Further, the Board believes in the benefits that technology can bring to support its daily operating activities and student achievement. As a Catholic learning community, we commit to use these and all technologies in a manner, which is consistent with the Mission and Vision of Catholic education and the teachings of the Catholic faith.

The Brant Haldimand Norfolk Catholic District School Board will ensure that:

- Information and Communication Technology tools and resources are integral to driving improvement in staff and student learning and efficiency.
- Board owned classroom and staff computers and devices will be used solely for education or work-related purposes.
- Information and Communication Technology tools and resources enable the Board to broaden its communication networks and provide the Board with the ability to connect with all geographic areas under the Board's jurisdiction.
- Staff and students must be given and be prepared to use Information and Communication Technology tools and resources to ensure they become collaborators in learning, seekers of knowledge and acquirers of new skills.
- All Board assets and equipment are to be protected.
- The use of technology must be appropriate.
- Information and Communication Technology tools and resources must be used such that they provide a safe and nurturing environment for learning and working.

Application and Scope

The purpose of this Policy and Administrative Procedure is to protect both the Board and its users from risks associated with using these resources, including but not limited to; virus attacks, spam, loss of data, invasion of privacy, loss of service and an array of legal issues and to promote effective use and efficient business practices as well as to promote student achievement through activities initiated by the IT Governance Council (ITGC). Through this administrative procedure, the Board endeavors to educate staff and students with the intent to maximize the value that its information and communications technology (ICT) investment brings to support student achievement.



References

- Copyright Act (R.S.C., 1985, c. C-42)
- Education Act, R.S.O., 1990, c. E.2
- Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), R.S.O. 1990, c. M.56
- Human Rights Code, R.S.O. 1990, c. H.19
- Criminal Code (R.S.C., 1985, c. C-46)
- Highway Traffic Act, R.S.O. 1990, c. H.8
- Occupational Health and Safety Amendment Act (Violence and Harassment in the Workplace), 2009, S.O. 2009, c. 23 – Bill 168
- 300.01P – Workplace Harassment Policy
- 300.20P – Workplace Violence Prevention Policy
- 600.03P – Electronic Web Sites Policy
- 600.31 Laptop/Netbook/Portable Device Usage for Staff Procedures Board Policy
- 600.32 Laptop/Netbook/Portable Device Support for Staff Procedures Board Policy
- 600.33 Laptop/Netbook/Portable Device Security for Staff Procedures Board Policy
- **BHNCDSB Artificial Intelligence Guideline for Educators**
- **BHNCDSB Artificial Intelligence Guideline for Responsible Corporate use of GenAI**

Forms

- 600.02.01F – Information and Communications Technology Use Acknowledgement Form.
- 600.02.02F – Technology Use Agreement – Primary Students.
- 600.02.03F – Technology Use Agreement – Junior Students.
- 600.02.04F – Technology Use Agreement – Intermediate and Senior Students.

Appendices

- N/A

Definitions

Administrators: Principals and Vice-Principals in a school.

Appropriate Use: Relevant federal and provincial laws and regulations govern the use of the computer and information technology systems of the Board. In addition, use must be always consistent with Board policies and procedures. Users are expected to use the Board's information technology systems and resources, as well as internet and email services in a lawful, responsible, and ethical manner consistent with the educational, informational, and recreational purposes for which they are provided. Users will be subject to disciplinary action for misuse. Misuse of these systems may also, in some instances, subject the Board to lawsuits.



Computer Operations Personnel: Personnel employed to provide software and hardware support for computer systems such as the **Manager Chief Information Officer** of Information Technology, Network and Systems Administrator, Computer Technicians, and staff within the Data Services Department.

Electronic Communication: E-mail, electronic conferencing, personal and group electronic chat sessions, video conferencing, text messaging and any other means of electronic communication.

Information and Communications Technology: Usually called ICT, is often used as an extended synonym for information technology (IT) but is usually a more general term that stresses the role of unified communications and the integration of telecommunications (telephone lines and wireless signals), intelligent building management systems and audio-visual systems in modern information technology. ICT consists of all technical means used to handle information and aid communication, including computer and network hardware, communication middleware as well as necessary software. In other words, ICT consists of IT as well as telephony, broadcast media, all types of audio and video processing and transmission and network-based control and monitoring functions.

System Administrator: Personnel responsible for maintenance of server software, global conferences, and other related duties.

User: All employees, students, trustees, members of Board committees, school council chairs, parents/guardians, and all other persons given authorized access to the Board's computing and information technology facilities and resources are considered users. Users may access these tools from locations other than their work locations. Using Board-provided technology from the office, home or other location is using a corporate asset. Therefore, the Board, its employees and students are responsible for any misuse of its technology. If an employee sends personal views, they must provide appropriate disclaimers so that the remarks are not taken as representative of the Board.

Administrative Procedures

Superintendents, Administrators and Managers

- Ensure that staff, upon hiring and annually thereafter, are made aware of Board Information and Communications Technology Policies and Procedures.
- Ensure that staff and students are aware of the expectations regarding the use of any Board-supplied technology or personal device that is connecting to the Board's network and/or Board-provisioned technology services.
- Determine appropriate action, corrective, and disciplinary measures to address staff and student violations of this procedure in consultation with senior management as necessary on a case-by-case basis for situations where staff and students are not in compliance with Board Information Technology Policies and Procedures.
- Ensure staff and students are aware of restrictions on personal mobile device usage and social media access as per PPM 128.
- Enforce policies requiring that personal mobile devices for students in grades 9 to 12 be stored out of view and powered off or set to silent mode during instructional time, except when explicitly permitted by an educator.
- For grades K-8, enforce policies requiring that personal mobile devices be stored out of view and powered off or set to silent mode throughout the instructional day.



Administrators

- Coordinate and manage technologies within their school in accordance with the directives from the IT Governance Council (ITGC) to promote student achievement.
- Develop an understanding for, as well as monitor and supervise the acceptable use of electronic communication and social media technologies when used in any Board facility.

Teachers

- Manage the collection of Student Information and Communications Technology Use Agreement forms pertaining to the Board's Information Technology Policies, Procedures and Acceptable Use.
- Manage student use of computing and information technology facilities and resources within their assigned teaching areas in accordance with the directives from the IT Governance Council (ITGC) to promote student achievement.
- Instruct and model for students, the appropriate use of technology.
- Instruct all students to comprehend and as well as supervise students in their adherence to all Board Information Technology Policies and Procedures.
- Consult with the school administrators, as necessary, and use the Board Information Technology Policies and Procedures and/or the School's Code of Conduct when applying sanctions for misuse and/or illegal use of the Board's computing and information technology facilities and resources.
- Teach proper techniques and standards for learning, collaboration, and creating evidence of learning using digital tools and resources with an emphasis on privacy, copyright infringement, online etiquette, and cyber bullying.
- Monitor and enforce the appropriate use of personal mobile devices and social media within their teaching areas.
- Explicitly permit the use of personal mobile devices for educational purposes, health and medical purposes, or to support special education needs as outlined in PPM 128.
- Confiscate personal mobile devices that are not stored out of view during instructional time and require students to place them in a designated storage area.

Students

- Abide by the Board's Information Technology Policies, Procedures and Acceptable Use Agreement.
- Student users of the Board's technology resources must complete, with applicable signatures, a Brant Haldimand Norfolk Catholic District School Board Student Information and Communications Technology Use Agreement. Access to Board technology resources will be denied to students that do not have this form signed and on file. Without a signed form, an active student network account will not be generated.
- Students that violate the Student Information and Communications Technology Use Agreement will be reported to the administrator of their respective school and their computing privileges will be suspended or revoked depending on the severity of the violation. All illegal activities will be reported to the Superintendent or designate and fully prosecuted of the law.
- Computer use by students is a privilege, not a right.
- Store personal mobile devices out of view and ensure they are powered off or set to silent mode during instructional time, except when use is explicitly permitted by an educator.
- For grades K-6, store personal mobile devices out of view and powered off or set to silent mode throughout the instructional day.
- Hand in personal mobile devices if seen by an educator and store them in a designated area.



All Users

- Ensure that technology resources are used in an effective, efficient, moral, and ethical, equitable and lawful manner.
- All users (e.g., staff, students, parents/guardians, outside agencies, volunteers, etc.) of Board software/systems (e.g., Brightspace, Office 365, Teams, Outlook email, the BHNHub, etc.) are required to sign in using their personal board-provided username and password and participate with transparency in a manner consistent with this policy.
- Users must not impersonate other users (e.g., another staff member, another student, another parent/guardian's, etc.) to gain access to information (e.g., Brightspace class page, Student Portfolios, Teams resources, emails, files, etc.) or activities (e.g., Brightspace discussions, Teams meetings, Teams chat conversations, etc.).
- All users are responsible for creating and maintaining a strong password for each board software/system they have been provided access to.
- All users are responsible for safeguarding board software/systems and the information contained in them by following appropriate behaviours (e.g., ensuring that they lock or sign out before leaving their device unattended, keeping passwords private, not forwarding links, messages, emails, or files, etc.).
- Users who use personal devices (e.g., cell phones, tablets, laptops, desktop computers) when accessing board software/systems must take every reasonable effort to ensure their device is free of malware and protected by appropriate means (e.g., anti-virus software, password, lock screen, etc.).
- Users who use shared personal devices (e.g., the home computer, shared iPad, etc.) must sign out of all board software/systems (e.g., Brightspace, Office 365, Teams, Outlook email, the BHNHub, etc.) before leaving the device for others to use.
- ~~While discouraged with board-provided devices, staff may choose to install and run VPN software (e.g., Nord, Express, CyberGhost, Private, Surfshark, IPvanish, etc.). Staff and students who use VPN software on their device may experience disruptions or be unable to use board-provided online resources (e.g., Teams, Office 365, Brightspace, the BHNHub, etc.). Only BHNCD SB-approved VPN software may be used on Board devices and to access Board resources. Use of consumer VPNs is prohibited~~
- Ensure that all users authenticate to networks, devices, and applications as themselves and not assume another person's identification during the authentication process.
- Use the Board's network, technology, and technology services in a lawful, responsible, and moral and ethical manner consistent with the educational, informational, and recreational purposes for which they are provided.
- Agree never to use a system to perform an illegal or malicious act. Any attempt to increase the level of access to which (s)he is authorized, or any attempt to deprive other authorized users of resources or access to any Board computer system shall be regarded as malicious and may be treated as an illegal act.
- Upon finding a possible security lapse of any kind on any system, all users are obliged to report the security lapse to the system administrator who will investigate the problem.



Information

The Board's network and computer systems are provided to support education, research, academic development, and Board-related business. Access to social media platforms is restricted, and personal mobile devices must not be used during instructional time except for educational purposes, health and medical purposes, or to support special education needs as directed by an educator. The Board is not responsible for any consequences arising from unauthorized use.

Procedures

1. Rights

Computer systems, networks, facilities, and accounts are owned and operated by the Board. The Board reserves all rights, including termination of service without notice, to the computing resources which it owns and operates. These procedures shall not be construed as a waiver of any rights of the Board, nor shall they conflict with applicable acts of law. Users have rights that may be protected by Federal, Provincial, and local laws.

2. Privileges

Access and privileges on the Board's network and computing systems are assigned and managed by the administrators of specific individual systems. Eligible individuals may become authorized users of a system and be granted appropriate access and privileges by following the approval steps prescribed for that system.

Users may not, under any circumstances, transfer or confer these privileges to other individuals. Any account assigned to an individual shall not be used by others without written permission from the system administrator. The authorized user is responsible for the proper use of the system, including password protection.

3. Accounts

Users do not own accounts on Board devices and technology but are granted the privilege of exclusive use.

4. Confidentiality

No Expectation of Privacy

Users should not expect privacy regarding any activities conducted using the Board's computer and/or telecommunication property, systems, or services. The use of passwords, usernames, or account numbers does not create a reasonable expectation of privacy or confidentiality for information maintained or transmitted. The Board reserves the right to review, retrieve, read, and disclose any files, messages, or communications created, sent, received, or stored on Board systems and/or equipment.

The Board's right to review—also referred to as monitoring—is exercised to ensure the security and protection of business records, prevent unlawful and/or inappropriate conduct, and maintain a productive and safe work environment.

Reporting Concerns and Access Authority

If policy violations are suspected or discovered, concerns must be reported to the Chief Information Officer of Information Technology, who is responsible for coordinating the technical response and escalating matters as required.

No IT staff member may intentionally view, read, or access private or confidential user information without explicit approval from the Superintendent responsible for Information Technology or the Director of Education. Such approval may only be granted when access is necessary for the purposes outlined above.



Exceptions for IT Operational Duties

Exceptions exist for IT staff who may require access to system data as part of their roles and responsibilities. This includes circumstances where systems personnel must inspect corrupted, damaged, or malfunctioning data in order to restore functionality or troubleshoot technical issues. Any such access must be strictly limited to the least invasive level required to perform assigned duties.

This exception does not remove IT staff from the obligation to maintain confidentiality. Personal or confidential information encountered during the performance of technical duties must not be disclosed or used in any manner, except where disclosure is necessary in good faith to restore an otherwise unusable document or system.

No Expectation of Privacy

~~Users should not expect privacy with respect to any of their activities when using the Board's computer and/or telecommunication property, systems, or services. Use of passwords or account numbers by users does not create a reasonable expectation of privacy and confidentiality of information being maintained or transmitted. The Board reserves the right to review, retrieve, read, and disclose any files, messages or communications which have been created, sent, received, or stored on the Board's computer systems and/or equipment.~~

~~The Board's right to review, also called monitoring, is for the purpose of ensuring the security and protection of business records, preventing unlawful and/or inappropriate conduct and creating and maintaining a productive work environment.~~

~~If policy violations are suspected or discovered, they will be reported immediately to the appropriate system administrator. The administrator is not permitted to see or read the contents intentionally, unless authorized a Senior Administrator of the Board, to read document information where not germane to the foregoing purpose; or disclose or otherwise use what they have seen. One exception, however, is that of systems personnel who may need to inspect a damaged document to restore its contents. This exception is limited to the least invasive level of inspection required to perform such duties. Furthermore, this exception does not exempt technicians/system administrators from the prohibition against disclosure of personal and confidential information, except insofar as such disclosure equates with good faith attempts to restore the otherwise unusable document.~~

~~If policy violations are discovered or suspected, access to trustee accounts must be approved by the Director of Education and the Chair of the Board in writing.~~

5. Copyright

Software is protected by copyright laws. Therefore, the Board network and computing facilities are not to be used to copy software except as permitted by law or by contract with the owner of the copyright software. This means that software may only be copied to make back-up copies, if permitted by the copyright owner. The number of copies and distribution of copies may not be done in such a way that the number of simultaneous users in a division, department or in the district exceeds the number of original copies purchased by that division, department, or the district.

Content is also protected by copyright laws. Therefore, the Board network and computing facilities are not to be used to copy or distribute copyrighted content except as permitted by law or by contract with the owner of the copyrighted material. Users are to become familiar with the laws related to copyright to educate themselves and to avoid possible infringement. See <https://www.accesscopyright.ca/> for more information.



6. Violations

An individual's computer use privileges may be suspended immediately upon the discovery of a possible violation of Board Policies or Administrative Procedures. Such suspected violations will be confidentially reported to the appropriate Manager in the case of staff and to the School Administrator in the case of students. The Manager or School Administrator will consult with the appropriate Superintendent to determine appropriate action. The violations of these policies or procedures will be dealt with in the same manner as violations of other Board policies or procedures and may result in disciplinary review. In such a review, the full range of disciplinary sanctions is available, including the loss of computer use privileges, suspension, dismissal from the Board and legal action. Violations of some of the above policies may constitute a criminal offense.

Minor infractions of this Policy and Administrative Procedure, when accidental, such as consuming excessive resources or overloading computer systems, are generally resolved informally by the person administering the accounts or network. This may be done through electronic mail or in-person discussion and education.

Repeated minor infractions or misconduct, which are of a more serious nature, may result in the temporary or permanent loss of computer access privileges or the modification of those privileges. More serious violations include, but are not limited to, unauthorized use of computer resources, attempts to steal passwords or data, unauthorized use or copying of licensed software or content, repeated harassment, or threatening behavior. In addition, offenders may be referred to their department supervisor or supervisory officer for further action.

Any offense which violates local, provincial, or federal laws will be referred to appropriate supervisory officers and/or law enforcement authorities and may result in immediate loss of all Board computer privileges.

This Policy and Administrative Procedure provides general conduct guidelines and examples of prohibited uses for illustrative purposes but does not attempt to state all required or prohibited activities by users.

Staff and students who have questions regarding whether a particular activity or use is acceptable should seek further guidance from the system administrator or site administrator. Failure to comply with Board policies or other established procedures or rules governing information technology use may result in disciplinary action, up to and including discharge. Illegal uses of the Board's Information Technology will also result in referral to law enforcement authorities.

Conduct which violates this Policy and Administrative Procedure includes, but is not limited to, the activities in the following list:

- Unauthorized use of a computer account.
- Using the Board network to gain unauthorized access to any computer systems.
- Connecting unauthorized equipment to the Board network.
- Unauthorized attempts to circumvent data protection schemes or uncover security loopholes. This includes creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data.



- Unauthorized attempts to run software not deemed to be appropriate for the purpose of student learning and the business of the Board. This includes, but is not limited to, creating and/or running applications from thumb drives such as video games, security hack tools, torrents, etc.
- Unauthorized attempts to circumvent internet content filters. This includes, but is not limited to, creating and/or running programs that are designed to use external proxies to bypass local filters.
- Knowingly or carelessly performing an act that will interfere with the normal operation of computers, terminals, peripherals, or networks.
- Knowingly or carelessly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network.
- Deliberately wasting/overloading computing resources, such as printing too many copies of a document.
- Accessing, uploading, downloading, transmitting, displaying, or distributing obscene or sexually explicit material; transmitting obscene, abusive, or sexually explicit language.
- Damaging computers, computer systems or computer networks; vandalizing, damaging, or disabling the property of another person or organization; debilitating or disabling computers, systems or networks through the intentional misuse or overuse of electronic distribution or the spreading of computer viruses through the inappropriate use of files, software, or portable media.
- Violating terms of applicable software licensing agreements or copyright laws.
- Violating copyright laws and their fair use provisions through inappropriate reproduction or dissemination of copyrighted text, images, etc.
- Using Board resources for commercial activity such as creating products or services for personal or financial gain.
- Using electronic mail to harass or threaten others. This includes sending repeated, unwanted e-mail to another user.
- Initiating or propagating electronic chain letters.
- Inappropriate mass mailing. This includes multiple mailings to newsgroups, mailing lists or individuals, i.e., spamming, flooding, or bombing.
- Forging the identity of a user or machine in an electronic communication.
- Transmitting or reproducing materials that are slanderous or defamatory in nature or that otherwise violate existing laws or Board regulations.
- Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner of the files or software.
- Participating in gambling activities, including games of chance and wagering.
- Misrepresenting oneself or the Board.
- Lobbying elected officials.
- Use of the internet for personal use during regularly scheduled working hours.
- Taking part in other activities that could cause congestion and disruption of networks and systems.



- Intentionally deleting email with informational value to the detriment of legal and statutory Board operations.
- Willfully collecting, maintaining, or disclosing personal information in contravention of the Municipal Freedom of Information and Protection of Privacy Act.
- Contravening Board policies and procedures.
- Unauthorized use of personal mobile devices during instructional time.
- Use of social media platforms on Board/school networks and devices for non-educational purposes.
- Failure to store personal mobile devices out of view and powered off or set to silent mode as required.
- Refusal to hand in personal mobile devices when requested by an educator.

Additional Guidelines

Information Technology Services staff, Student Achievement Team Members as well as other Board expert staff will establish more detailed procedures and guidelines, as needed, for specific computer systems, networks, and applications. These procedures and guidelines will cover such issues as allowable connect time and disk space, handling of irretrievable mail, responsibility for building accounts and other items related to administering the system.

- Schools must send annual notifications to parents and students reminding them of the policy on personal mobile device use and social media access, its requirements, and consequences for non-compliance.
- Educators should be provided with best practices for managing technology use in the classroom and enforcing these policies effectively.

Information Security and Privacy Training

All employees of the Brant Haldimand Norfolk Catholic District School Board (BHNCD SB) are required to complete information security and privacy training:

- **Upon Hire:** All new staff must complete the Board's approved cybersecurity and privacy training modules before being granted access to Board technology resources.
- **Quarterly Requirement:** All employees must complete a minimum of three (3) training modules on information security and privacy each year, as directed by the Board.
- **Additional Training:** Employees may be required to complete additional training modules as determined by changes in legislation, Board policy, or emerging cybersecurity threats.

Incident Reporting

All employees of the Brant Haldimand Norfolk Catholic District School Board (BHNCD SB) must promptly report any suspected cybersecurity or privacy incident, including data breaches, unauthorized access, or compromise of Board information assets.



- **Immediate Reporting:** A breach occurs when there is unauthorized access to or collection, use, disclosure or disposal of personal information or data. When a breach or suspected breach occurs, an employee must contact their immediate supervisor and notify them of the breach/suspected breach. The supervisor will contact the applicable Superintendent of Education, the Chief Information Officer of Information Technology Services and the Manager of Communications and Community Relations (Privacy Officer). location. It is important that you speak to the above individuals. Please do not leave an email or phone message. If applicable and depending on each situation, a senior staff member (Superintendent or Manager) may contact the police.
- **Do Not Forward Suspicious Communications:** Employees must not forward suspicious emails, messages, or files, as this may increase risk or propagate threats. Instead, report the incident directly to IT as described above.
- **Incident Response:** The IT department will investigate reported incidents according to Board policy and applicable legislation and will communicate with affected parties as needed.

Governance of Digital Tools, Applications, and Web Services

To ensure the safe, effective, and compliant use of digital tools and resources, the Brant Haldimand Norfolk Catholic District School Board (BHNCDSB) will implement a formal governance process for the approval and management of all digital applications, platforms, and web services.

A. Taxonomy of Digital Tools

All digital tools, applications, and web services will be classified into the following categories:

- **Approved (Green):** Tools that have been assessed and determined to be safe and appropriate for use within BHNCDSB.
- **Restricted (Yellow):** Tools that are approved for limited or specific uses (e.g., Special Education, pilot programs) and subject to additional conditions or safeguards.
- **Prohibited (Red):** Tools that are not approved for use due to security, privacy, or compliance risks. These must not be used under any circumstances.

B. Intake and Review Workflow

All requests for new digital tools, applications, Artificial Intelligence platforms, or web services, or for the deployment of existing tools, must follow this intake and review process:

1. **Submission:** Staff must submit a request for review through BHN Apps, specifying the intended use, target audience, and any relevant details.
2. **Pedagogical Review:** The Program Department will evaluate the tool for instructional value and ensure it does not duplicate existing approved functionality.
3. **IT and Security Review:** The Information Technology department will assess integration, technical compatibility, and security risks, including privacy impact assessments (e.g., using ECNO VASP or similar frameworks). If these frameworks do not contain adequate assessment information a third party PIA must be obtained at the cost of requesting party.
4. **Privacy and Records Management Review:** The Privacy Officer upon request will review a PIA for compliance.
5. **Procurement and Budget Approval:** If required, the request will be reviewed for budgetary impact and procurement compliance.



6. **Final Approval:** The Superintendent or designated authority will provide final approval, as needed.
7. **Documentation:** Approved tools will be added to the BHNCDSB Approved Apps List, maintained by ITS and published internally for staff reference.

C. Data Minimization

- **Data Minimization:** Use of restricted tools must follow strict data minimization and depersonalization practices. Personal identifiers must be removed once the activity is complete.

D. Transparency and Communication

- The Approved Apps List will be accessible to all staff.

**REPORT TO THE BRANT HALDIMAND NORFOLK CATHOLIC
DISTRICT SCHOOL BOARD POLICY COMMITTEE**

Prepared by: John Della Fortuna, Superintendent of Education
Presented to: Policy Committee
Submitted on: April 21, 2026
Submitted by: Mike McDonald, Director of Education & Secretary

ELECTRONIC MONITORING POLICY - OPS #400.18
Public Session

BACKGROUND INFORMATION:

The Brant Haldimand Norfolk Catholic District School Board is committed to maintaining the safety and efficiency of its operations and ensuring a secure environment for the work of our students and staff. To support this commitment, the Board has implemented technology monitoring across physical and virtual locations. This Administrative Procedure provides employees with information on how these monitoring processes work and aligns with the requirements of Ontario’s Employment Standards Act.

DEVELOPMENTS:

The revised Administrative Procedure introduces several key updates. Responsibility for oversight has shifted from the Superintendent of Business to the Superintendent of Education. Employees will receive an electronic copy of the procedure within 30 calendar days of each implementation and review. The definition of Electronic Monitoring has been updated to clarify its role in tracking digital activities for security, health and safety, and regulatory compliance. The procedure outlines how and in what circumstances the Board electronically monitors its employees, the mechanisms used, and the purpose for doing so. It applies to all Board staff, including third-party contractors, assigned employees, and trustees, whether working on-site or remotely. The next scheduled review of this Administrative Procedure will occur during the 2029–2030 review cycle. The policy will undergo annual reviews, with revisions informed by input from the Information Technology Services team. Additionally, Transportation Services has added video surveillance under the “Tool and Circumstance” section.

RECOMMENDATION:

THAT the Policy Committee recommends that the Committee of the Whole refers the Electronic Monitoring Policy OPS #400.18 to the Brant Haldimand Norfolk Catholic District School Board for approval.



Electronic Monitoring OPS 400.18

Adopted:	October 31, 2022
Last Reviewed/Revised:	N/A
Responsibility:	Superintendent of Business Education
Next Scheduled Review:	2026-2027 2029-2030

Purpose

The Brant Haldimand Norfolk Catholic District School Board (the “Board”) is committed to continued safety and efficiency of its operations and ensuring a safe environment for the work of our students and staff. The purpose of this Administrative Procedure is to inform employees on how the Board uses technology to monitor its technology resources in all its physical and virtual locations. This Administrative Procedure is based on recent updates to Ontario’s Employment Standards Act.

Application and Scope

This Administrative Procedure outlines how and in what circumstances the Board electronically monitors its employees, the mechanisms, and the purpose(s) for doing so. There is no expectation of privacy in using Board technology. The Board may monitor and access electronic communications, internet history/traffic, files, documents, and overall system use. The monitoring mechanisms ensure the system’s integrity and compliance with Board policies and procedures.

This Administrative Procedure applies to all Board staff, including third parties and trustees, assignment employees and trustees, in the workplace or working remotely.

References

- [Working for Workers Act, 2022](#)
- [ITS 600.02.P - Information and Communications Technology Use](#)
- [OPS 400.11.P - Video Security Surveillance](#)
- [OPS 400.13.P - Records and Information Management](#)
- [Municipal Freedom of Information and Protection of Privacy Act \(MFIPPA\)](#)
- Relevant and Applicable Collective Agreements

Forms

- N/A

Appendices

- OPS 400.18.XA – Electronic Monitoring

Definitions

Electronic Monitoring: The use of technology to ~~keep track of monitor~~ digital activities to ensure organizations comply with security, health and safety, and regulatory requirements (see Appendix A).



Administration Procedures

All electronic communication and internet communications sent and received by users while using their Board-provided credentials are the property of the Board. Communications are not private or personal despite any such designation by the sender or the recipient, unless subject to specific legal or legislative requirements. Personal or private communications transmitted on the Board's electronic information system may be accessed, reviewed, copied, deleted, retained, or disclosed at any time without notice.

The Board conducts electronic monitoring to:

1. Protect staff, students, and technology from harm.
2. Keep our facilities and property safe and secure.
3. Protect electronic resources from unauthorized access and use.
4. Protect against loss, theft, or vandalism.

From time-to-time, the Board may access data collected via our electronic systems (Board provided technology or personal devices when using Board credentials) in a number of situations, including but not limited to:

- a) To comply with legislative disclosure or access requirements under MFIPPA or to assist with the investigation and resolution of a Privacy Breach.
- b) For Board-owned technology, because of regular or special maintenance of the electronic information systems.
- c) For Board-owned technology, when the Board has a business-related need to access the employee's system, including, for example, when the employee is absent from work or otherwise unavailable.
- d) To comply with obligations to disclose relevant information in the course of legal proceedings.
- e) When the Board has reason to believe that there has been a policy violation or is undertaking an administrative, legal or disciplinary investigation.

An electronic copy of this Administrative Procedure will be provided to each employee within 30 calendar days of implementation/**review**. Should any changes be made to the administrative procedure after its implementation, each employee will be provided a copy of the revised administrative procedures within 30 days of the revisions being made. A copy of this Administrative Procedure will be retained for three years after it ceases to be in effect.



ELECTRONIC MONITORING

Tool	Circumstances	How	Purpose
Access/Security Cards	All school and Board facilities	Door readers and systems	Control and monitor access to buildings
Account Authentication	Staff login to servers and/or cloud services	Azure Active Directory Domain Controllers Active Directory tools	Protect against unauthorized access
Board Supported Applications	Overall usage	Embedded tools in Board Supported Applications	To protect against unauthorized access and monitor overall usage
Board Supported Network Infrastructure	Overall usage	Network Management and monitoring tools	Protect against unauthorized access, monitor overall integrity and availability of the network
Device Management (Android/Chromebook/Windows)	Installed on all Board Chromebooks, Desktops, Laptops, and Android devices registered to cloud management	Management Software	Protect against loss/theft, and enforce security settings
Electronic Communications	Electronic communications traffic (i.e., all incoming/outgoing email)	O365 integrated filters	Prevent the transmission of private/confidential/inappropriate data over insecure email
Global Position Systems (GPS)	All Board fleet maintenance vehicles	GPS tracking systems and associated software	Protect against loss and theft. Staff safety in case of breakdown. Administrative investigations. Dispatching decisions.
Phone Systems	School and office phone systems	Private Branch Exchange (PBX) phone system	Call quality, reliability, and availability (call volume and voicemail storage monitoring)
Video Surveillance	Most schools, Board facilities and Transportation Services	Video surveillance cameras and recording systems	Safety, theft, illegal activity, behavioral/incident monitoring and review
Web Filtering	All internet traffic	Network management and monitoring tools	Protect from harmful and inappropriate content