BRANT HALDIMAND NORFOLK
Catholic District School Board

Administrative Procedure

Electronic Security
OPS #400.18

Adopted:	October 31, 2022
Last Reviewed/Revised:	April 28, 2026
Responsibility:	Superintendent of Education, Information/Technology
Next Scheduled Review:	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 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