



Niagara Catholic District School Board

ELECTRONIC COMMUNICATIONS SYSTEMS POLICY (EMPLOYEES)

ADMINISTRATIVE OPERATIONAL PROCEDURES

200 – Human Resources

Policy No 201.12

Adopted Date: January 31, 2006

Latest Reviewed/Revised Date: May 28, 2024

The Electronic Communications Systems Policy (Employees) (201.12) and Administrative Operational Procedures establish the standards that govern the use of the electronic communications systems for all employees of the Niagara Catholic District School Board.

PREAMBLE

The Niagara Catholic District School Board supports teaching and learning through the provision of technology for staff and students. It is the expectation of the Board that the use of such technology will be conducted in a manner consistent with the Board Mission, Vision, and Values, supporting a respectful and equitable culture of caring, inclusion, dialogue, and the dignity of all.

Acknowledgement and informed consent of the Electronic Communications Systems Policy (Employees) and Administrative Operational Procedures are implied when employees use their Niagara Catholic login credentials to access the electronic communications systems of the Board.

New employees will be expected to sign the Electronic Communications Systems Agreement as a condition of employment.

DEFINITIONS

Electronic Communications - Any electronic engagement with others, including, but not limited to, telephone, email, texting, video chat software, blogs, websites, and social media platforms.

Electronic Communications Systems - Systems used to access or store digital files or information, including, but not limited to, a computer's internal hard drive, external hard drive, internet (hard-wired and Wi-Fi), and the cloud.

Social Media - Platforms that enable users to create and share content or participate in online communications with others (social networking). These include, but are not limited to, *Facebook, Twitter, Instagram, Snapchat, LinkedIn, and YouTube.*

Personal Device - Equipment owned and maintained by the employee at their own expense.

Board-Issued Device - Equipment owned and maintained by the Niagara Catholic District School Board provided to employees.

Personal Use - Use of electronic communications unrelated to an individual's employment.

Professional Use - Use of electronic communications related to and necessary for the individual's employment.

ACCEPTABLE CONDUCT

1. The use of the Board's electronic communications systems must reflect the highest standard of courtesy and professional conduct. Employees are to be mindful of the tone of their messaging when engaging online with others. Profanity, vulgar language, sarcasm, the use of full capitalization (to indicate yelling) or the use of disrespectful language is unacceptable in any correspondence.
2. Employees must not send or post messages of a bullying, fraudulent, defamatory, intimidating, unlawful or sexually explicit nature.
3. The creation or distribution of disparaging statements about the Board, other employees, unions, departments, students, parents/guardians, or community partners or trolling others online via any form of electronic communications system is strictly prohibited.
4. Employees are not authorized to provide personnel or employment information on behalf of the Board.
5. Employees must not engage in any activity intended to conceal their own identity or to misrepresent themselves as someone else. Such action may result in discipline, up to and including termination.
6. Employees must not provide students with their personal mobile number or ask students for their mobile phone number or engage with them on social media outside of classroom accounts.
7. Employees must not engage in direct messaging (DM) one on one with students. This form of communication is strictly prohibited.
8. When approved by a principal, employees may use social media to communicate with a group of students, such as for the purpose of communication on an educational field trip or tournament.
9. Employees are to use Board email accounts for Board-related correspondence, including engagement with parents.

BOARD-ISSUED DEVICES

Employees must not use their Board-issued device, whether at home or on a system network, to intentionally access websites which would generally be considered inappropriate for viewing under good community standards. Examples may include, but are not limited to pornographic sites, sites containing xenophobic, homophobic, or transphobic materials, sites espousing misogyny or misandry, debunked claims, or other misinformation. Participation in such inappropriate conduct may result in discipline, up to and including termination of employment.

Employees have the right to be free from harassment from others, as Board email is seen to be an extension of the workplace. Employees encountering such messages or materials should report the incident to their immediate supervisor. The supervisor shall respond in a manner they deem appropriate in accordance with Board policy and procedures. Employees should not engage with individuals in such cases.

RESPONSIBLE USAGE

The Board expects that all employees/users will treat Board-issued devices responsibly, notwithstanding the normal use of wear, and will make every effort to return the equipment in such a condition expected after use. Niagara Catholic reserves the right to apply reasonable repair or replacement costs for lost or damaged technology.

RECORDS

All messages sent on the Niagara Catholic District School Board communication systems are Board records and the Board reserves the right to access and disclose the content of such messages.

USE OF ELECTRONIC COMMUNICATIONS DURING WORK HOURS

The use of electronic communications (including, but not limited to, desk or mobile phones, tablets, email, or social media) by employees must not impede an employee's ability to fulfill their work responsibilities, adversely affect performance or productivity, and not be for personal gain.

Policy/Program Memorandum 128 sets clear standards on the use of mobile devices during instructional time.

- Educators are not to use personal mobile devices during instructional time, unless explicitly for work-related purposes.

LEGISLATION

All communication is subject to policies and regulations regarding professional standards and Niagara Catholic Policies and Administrative Operational Procedures. These include, but are not limited to, [*Employee Code of Conduct and Ethics Policy \(201.17\)*](#), [*Trustee Code of Conduct Policy \(100.12\)*](#), [*Privacy Policy \(600.1\)*](#) and [*Code of Conduct \(302.6.2\)*](#), the *Copyright Act*, the *Ontario Human Rights Code*, the *Municipal Freedom of Information and Privacy Act (MFIPPA)*, and the *Personal Health Information Protection Act (PHIPA)*.

PRIVACY

1. All employees are to be aware that the Board's network does not ensure privacy to the user. Employees are to take all reasonable steps to maintain the confidentiality of employees, students, parents/guardians and other personal data.
2. All electronic communications using Board devices are the property of the Board. All electronic communications made using the Board electronic systems (e.g., Board Wi-Fi) may be accessed by the Board if requested and may be subject to *Municipal Freedom of Information and Privacy Act (MFIPPA)* disclosure.
3. Employees must not access or share contact or confidential information about any employee, student, parent/guardian beyond what is required for their employment purposes.
4. Employees are not authorized to take photos, videos, or to record any individual on Board property or at Board events/activities without the appropriate authorization, or consent of the individual and/or their parent/guardian. Permission is granted in accordance with the MFIPPA. These provisions also apply to the electronic transmission of photos, videos or other recorded information.

INFORMATION TECHNOLOGY

1. Employees are prohibited from borrowing, copying, or reusing login or passwords belonging to another employee.
2. Computer hacking, is prohibited on Board-issued technology or networks.

3. Modification (upgrading or removing) hardware components and peripherals by employees outside of Information Technology Services (IT Services) is prohibited. Any damages or labour charges resulting from unauthorized modification will be the responsibility of the individual.
4. Unauthorized movement of hardware and peripherals from an assigned location is prohibited, except by members of IT Services and with the knowledge and permission of the individual's immediate supervisor.
5. Non-Board-owned hardware and peripherals (excluding external memory) must not be physically connected (hard-wired) to the network or Internet at any Board site without the express permission of IT Services and with the knowledge and permission of the individual's immediate supervisor.
6. Users shall not install any software outside of that provided by the Board without express written permission from IT Services and with the knowledge and permission of their immediate supervisor.
7. The use of devices or technologies known to cause or could reasonably be expected to cause service disruption to the Board's electronic communications systems is prohibited.
8. Employees must not share proprietary information at any time.

PROFESSIONAL COMMUNICATION

For the purpose of professional communications, employees are expected to communicate with each other, supervisors, or parents/guardians using a Board email account.

Employees must not use Board email for any of the following reasons:

- Personal advertisements, solicitations, or donations
- Political lobbying
- Prayer chains/prayer requests (not sanctioned/requested by the Bishop, parish priest, Chaplaincy Lead or any organization sanctioned by the Board Chaplaincy Lead)
- Memes or messages intended to disparage an individual or group of individuals based on race, nationality, gender, sexual orientation or sexual identity
- Commercial or financial opportunities
- Any programs created for the sole purpose of causing damage or chaos to the Board system or other systems (such as viruses)

RIGHT TO DISCONNECT/REASONABLE EXPECTATIONS TO RESPOND

Employees are encouraged to send emails and voicemails during their regular hours of work. All employees should avoid sending work-related communications after hours (between 6:00 p.m. to 7:00 a.m., Monday to Friday and all-day Saturday and Sunday) unless the matter can be reasonably constituted as an emergency or a significant event that calls for immediate action.

SPEAKING ON BEHALF OF THE BOARD

1. In accordance with the [Employee Code of Conduct and Ethics Policy \(201.17\)](#), the Director of Education, Chair of the Board, or assigned designate are spokespersons for the Board. No other individual may speak on behalf of the Board.
2. Principals may speak to issues related directly to their school, in consultation with their Family of Schools' Superintendent of Education and the Communications Department.

MESSAGE MANAGEMENT

Messages directed to all employees are sent through the Office of the Director of Education.

Where messages are being sent to all employees or large groups, senders are asked to consider their recipient list carefully to ensure their message is sent to relevant employees. Recipients are asked to respect the time of the sender and to not reply to bulk emails unless otherwise directed to do so, including acknowledging receipt/thanking the sender.

MONITORING/CONSEQUENCES AND BOARD RIGHTS

1. As part of regular, operations, the Board does not monitor internal email and communications. The Board reserves the right to monitor electronic communications should a specific need arise. In addition, telephone logs may be checked occasionally.
2. Any request to carry out a forensic audit of Board equipment must have the approval of the Director of Education.
3. The Board has the right to limit individual or organizational use of its electronic communications systems at any time, without notice and without providing any explanation except that it is in the best interests of the integrity of the Board.
4. Any breach of the Administrative Operational Procedures may lead to discipline, up to and including termination.

The following chart is provided for transparency to employees to describe how and in what circumstances Niagara Catholic may monitor employees. The chart also identifies the purpose for which the information obtained may be used by Niagara Catholic.

MONITORING TOOL	CIRCUMSTANCES, METHODS AND PURPOSE
Internet Filtering	<ul style="list-style-type: none">• All internet traffic is filtered by firewalls at every site and at the core of our network.• The method for filtering internet traffic is by utilizing devices called firewalls.• The purpose of the filtering employed is to protect users from unauthorized access as well as harmful and inappropriate content.
eMail Filtering	<ul style="list-style-type: none">• All email traffic is filtered for cyber protection and data loss prevention.• The method for filtering email traffic is by utilizing cloud services provided by Google and Microsoft and by utilizing additional email security and cyber protection technology implemented into the Niagara Catholic private cloud.• The purpose of the filtering employed is to prevent the transmission of private/confidential data over insecure email and to prevent malicious emails such as phishing emails from reaching the Niagara Catholic email platforms.

Account Authentication	<ul style="list-style-type: none"> ● All account authentication (login services) identifies user interaction at the time of login and usage of any integrated services. ● The method for processing account authentication is our Directory Services platform. ● The purpose of the account authentication is to prevent against unauthorized access.
Device Management	<ul style="list-style-type: none"> ● All endpoint devices such as desktop and laptop computers, Chromebooks, tablets and other devices are managed by Niagara Catholic IT Services ● The method for managing devices is leveraging device specific electronic management platforms. ● The purpose of the device management platforms is to protect against loss/theft and enforce operating system, application and security settings.
Video Surveillance	<ul style="list-style-type: none"> ● Some schools and other Board sites have video surveillance in place. ● The method for video surveillance is video recording cameras and recording systems. ● The purpose of the video surveillance is for safety, to monitor potential theft, illegal activity, and for behavioural/incident monitoring and review.
GPS (Global Positioning System)	<ul style="list-style-type: none"> ● Some Board-owned vehicles have GPS capability employed. ● The method of GPS tracking is by leveraging GPS tracking systems and associated supporting software. ● The purpose of the video surveillance is to protect against loss and theft, to provide for staff safety in case of breakdown and to perform administrative investigations.
Door Key Fobs	<ul style="list-style-type: none"> ● All Board buildings have door key fobs which facilitate secure access into Board facilities. ● The method of leveraging the key fobs is by leveraging the facilities door key fob platform. ● The purpose of the door key fobs is to facilitate, control and monitor access to buildings.
Telecommunications Call Accounting	<ul style="list-style-type: none"> ● All Board buildings have telecommunications call accounting capability employed. ● The method used to manage call accounting is by using the school board call accounting platform. ● The purpose of the call accounting platform is to identify and track all inbound and outbound calls for safety and fiscal accountability purposes.

Adopted Date:	January 31, 2006
Revision History:	May 9, 2006 June 12, 2012 October 23, 2018 April 25, 2023 May 28, 2024