Niagara Catholic District School Board

ELECTRONIC COMMUNICATIONS SYSTEMS POLICY (EMPLOYEES)

STATEMENT OF POLICY

200 – Human Resources **Policy No 201.12**

Adopted Date: January 31, 2006 Latest Reviewed/Revised Date: October 23, 2018

In keeping with the Mission, Vision and Values of the Niagara Catholic District School Board (the "Board"), the Board provides access to, and recognizes the value of, staff utilizing electronic communications systems to share information and knowledge in support of the Board's mission.

Electronic communications systems and all data and messages generated on or handled by Board equipment are considered to be the property of the Board and are not the property of the users of the information technology.

Employees are accountable for the appropriate use of the Board's electronic communications systems in an ethical and appropriate educational manner, which must be in compliance with all relevant federal and provincial legislation. This includes, but is not limited to, the following: the Education Statutes and Regulations of Ontario, Ontario Charter of Rights and Freedoms, Ontario Code of Conduct; Ontario Human Rights Code and the Municipal Freedom of Information and Protection of Privacy Act and all relevant policies of the Niagara Catholic District School Board.

Employees must make a concerted effort to protect their passwords and not share them with anyone. Employee passwords represent the electronic employee identity and provide access to a wide variety of privileged services, applications and data that should not be accessible by any other person than the employee.

The confidentiality of employee, student, and other personal data must always be maintained.

There is no expectation of privacy on the part of any user when communicating using any of the Board's electronic communication systems.

Access to the Board's electronic communication services is a privilege that may be wholly or partially restricted by the Board at any time.

Any breaches of this policy may lead to discipline up to and including dismissal.

The Director of Education will establish Administrative Procedures for the implementation of this policy.

References

- ***Canadian Charter of Rights and Freedoms***
- ***Education Statutes and Regulations of Ontario***
- ***Municipal Freedom of Information and Protection of Privacy Act***
- ***Ontario Code of Conduct***
- ***Ontario College of Teachers, Professional Advisory: Maintaining Professionalism-Use of Electronic Communication and Social Media UPDATED, September 2017***
- ***The Ontario Human Rights Code***
- ***Niagara Catholic District School Board Policies/Procedures***
  - ***Records and Information Management Policy 600.2***
  - ***Electronic Communications System Policy (Students) 301.5***
  - ***Employee Code of Conduct and Ethics Policy 201.17***

Niagara Catholic District School Board

ELECTRONIC COMMUNICATIONS SYSTEMS POLICY (EMPLOYEES)

ADMINISTRATIVE PROCEDURES

200 – Human Resources **Policy No 201.12**

Adopted Date: January 31, 2006 Latest Reviewed/Revised Date: October 23, 2018

In accordance with the Electronic Communications Systems (Employees) Policy No. 201.12, all employees shall be governed by the administrative procedures in this policy.

DEFINITIONS

1. Electronic communications systems refer to any electronic means used to send and receive information, including graphic images and photographs. They include, but are not limited to, Internet, Intranet, Cloud, E-Mail, Messaging Services, Social Media, Fax, Telephone, Pagers, Personal Electronic Devices, TV, Optical Disc Media and Radio.
2. Common areas will be defined and outlined by the Principal or person in charge of that building.
3. Personal Electronic Devices are defined as a piece of electronic equipment such as a laptop computer, tablet, mobile phone, wearable technology (e.g. smart watches) and medical monitoring devices (e.g. Wi-Fi enabled blood glucose monitors, etc.).

ETIQUETTE

1. The use of the Board's electronic communications systems must reflect the highest standard of courtesy and professional conduct and should be used only if there is a valid work-related reason.
2. While security and firewall filters are in place, employees are prohibited from knowingly accessing or participating in religiously, racially, or culturally offensive sites or e-mail, and commercial, gambling, racist, abusive, profane, pornographic, violent, discriminatory or harassing activities.

RECORDS

All messages sent on 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.

DESK PHONES AND CELL PHONES

1. Staff are expected to focus their full attention on their work duties.
2. Notwithstanding emergency situations, staff is not to place or accept personal calls or messages by classroom phones or cell phones nor otherwise utilize a personal electronic device or utilize a Board issued device for personal means during scheduled work times.

PRIVACY

1. The confidentiality of employee, student, and other personal data must always be maintained.
2. In the process of operating and maintaining the Board’s network and services, privacy cannot be guaranteed.
3. All Electronic communications using the Board’s devices and/or services are property of the Board.
4. Electronic communications are neither private nor secure.

5. Users should be aware that all electronic records are Board documents that may be subject to disclosure under the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA). The confidentiality of employee, student, and other personal data must always be maintained.
6. There are occasions when it may be necessary to access an employee's electronic files, whether they are transmitted to onsite Board storage or Board provisioned Cloud storage.
7. There are occasions when it may be necessary to access an employee's e-mail messages.
8. In the process of operating and maintaining the e-mail systems, privacy cannot be guaranteed.
9. There may be occasions when records of telephone calls will be reviewed to ensure appropriate use.

LEGISLATION

1. Internet and computer use are subject to applicable legislation and Board policies, including the Human Rights Code and the Municipal Freedom of Information and Protection of Privacy Act.
2. As with other written resources, there is an obligation to consider copyright and material use limitations where documents, pictures or other media are downloaded from the Internet.

PERMITTED USE OF THE BOARD'S ELECTRONIC COMMUNICATION SYSTEMS

1. All electronic communications systems provided by the Board are the property of the Board. The electronic systems including hardware and software are the Board's property.
2. While the use of the Board's electronic communications systems are intended for legitimate Board-related purposes only, the Board recognizes that there may be times when occasional non-work related use is acceptable. Such usage must be minimal, be in compliance with this policy, not interfere with an employee's work responsibilities, not adversely affect performance or productivity, and not be for personal gain of any type.

INAPPROPRIATE/UNACCEPTABLE USE OF THE BOARD'S ELECTRONIC COMMUNICATION SYSTEMS

1. Inappropriate use of the Board's electronic communications systems and computer network systems can result in the removal or suspension of these privileges at any time by the Board. Some inappropriate use may lead to discipline up to and including dismissal
2. The following chart of inappropriate uses of the Board's electronic communications systems is not exhaustive and is only used as a guideline for governing conduct in general.

INAPPROPRIATE USE	DESCRIPTION
Acting on Behalf of the Board	• Negligent misrepresentations on behalf of the Board or making statements on behalf of the Board when you are not authorized to do so is prohibited.
Chain Mail	• Initiating or forwarding chain mail is prohibited.
Confidential Information	• Accessing and/or disseminating contact information or confidential information for improper purposes is prohibited.
Controversial Material	• Users of the internet may occasionally encounter material that is controversial and which other users, parents or staff might consider inappropriate or offensive. • It is the responsibility of the individual user not to intentionally access such material.

Criminal Activity	• Any activity that constitutes a violation of the Criminal Code (e.g. child pornography, hate crimes, etc.), and/or other laws is prohibited.
Cryptocurrency	• Cryptocurrency mining or other forms of computing processing power or storage capability mining or exploitation is prohibited.
Defamatory Statements	• Making or distributing inappropriate statements about other employees, unions, departments and/or the Board (defamation and insubordination) is prohibited.
Disruptive Technology	• Usage of devices or technologies which are known to cause or could reasonably be expected to cause service disruption to Board electronic communication systems services are strictly prohibited.
Dissemination of any Material that does not Benefit the Board	• Disseminating or storing commercial or personal advertisements, solicitations, personal promotions, political lobbying, destructive programs (i.e. viruses) or uses of this nature are prohibited.
Hacking	• Computer hacking, even hacking one considers to be "ethical" in nature is prohibited.
Hardware Modification	• Modification (upgrading or removing) of hardware components and peripherals by non-IT Services support staff is prohibited, except by managers or other individuals as designated by a member of Senior Administrative Council or a management member of IT Services. • Any damages and / or labor charges resulting from unauthorized modifications will be the responsibility of the individual involved.
Hardware Movement	• Movement of hardware and peripherals (from its assigned location in the school) is prohibited, except by computer technicians, managers or other individuals as designated by a member of Senior Administrative Council or a management member of IT Services. • Principals may authorize an individual to borrow a laptop, LCD projector or other devices on a temporary basis. All permanent relocations are the responsibility of the IT Services personnel, managers or other individuals as designated by a member of Senior Administrative Council.
Identity Fraud	• Sending email or other electronic communications which hide the identity of the sender or represents the sender as someone else. • Borrowing, copying or reusing other's information without their consent and/or knowledge.
Inappropriate Material	• Users of the internet shall not intentionally access inappropriate material on the internet.

Inappropriate Messaging	• Sending messages, or posting messages on social media, of a bullying, fraudulent, defamatory, discriminating, embarrassing, fraudulent, harassing, intimidating, obscene, profane, sexually explicit, threatening or otherwise unlawful or inappropriate (including graphics) nature is prohibited. • Users encountering or receiving these kinds of messages or materials should immediately report the incident to their supervisor. The supervisor, in turn, shall report the incident to the appropriate Superintendent.
Personal Information	• The dissemination of personal information contrary to the Municipal Freedom of Information and Protection of Privacy Act is prohibited.
Personal Means	• Excessive personal use is prohibited.
Pornographic Material	• Viewing pornographic material is prohibited.
Profiteering	• Using of Board devices, network or internet in order to profit is prohibited
Promotion of Controlled Substances	• Encouraging the use of controlled substances or the use of the system for the purpose of inciting crime.
Proprietary Information	• The dissemination of proprietary information is prohibited.
Software Installation	• The installation of any software that is not authorized by the Board and for which the Board does not have the appropriate license is strictly prohibited. • Users shall not install any software without express written permission from the IT Services.
Use of Non-Authorized Hardware	• Non Board owned hardware and peripherals (excluding external memory cards) may not be physically connected (hard wired) to the network or Internet at any Board site, without the express permission of IT Services, Managers or Family of Schools Superintendents.

MONITORING/CONSEQUENCES AND BOARD RIGHTS

1. While a reasonable, small, and infrequent amount of time may be spent on personal matters, the Board may monitor employees to ensure compliance with this policy.
2. As part of regular, day-to-day business operations, the Board does not monitor internal mail and communications. However, mail and communication may be monitored should a specific need arise. In addition, telephone logs may be checked occasionally.
3. Any request to carry out a forensic audit must have the approval of the Director of Education prior to such an audit being carried out.
4. The Board has the right to limit individual or organizational use of its electronic communication systems at any time, without notice and without providing any explanation except that it is in the interests of the integrity of the Board.
5. Any breaches of this policy may lead to discipline up to and including dismissal. The general principles regarding workplace discipline will be applied in a consistent manner. These principles include consideration of the seriousness of the behavior, the use of progressive discipline and consideration of mitigating factors.

MESSAGE MANAGEMENT

1. Messages that are directed to all staff including but not limited to all Elementary Principals, all Secondary Principals and all Secretaries are sent through the Director of Education, or a member of Senior Administration Council.
2. System emails, with the exception of emergencies, will be sent daily after 1:30 pm. The Office of the Director/Secretary-Treasurer (through the Board Services & Communications Department) shall receive and distribute all invitations to events, messages and general business related communication directed to the Board.
3. Where messages are concerned, senders and recipients should understand the following:
    - Consider the audience for the message and target the message in order to reduce the volume of unwanted e-mail.
    - Messages are not private.
    - Paragraphs and messages must be short and to the point so that they can be located quickly.
    - An appropriate subject title should be included in all messages so that they are easily identifiable.
    - Replying that a message is received should be limited to reduce volume of email traffic.
    - Users should check e-mail frequently and delete messages promptly (including from the Sent and Delete Boxes).
4. Where storage of messages is concerned, users should be aware:
    - For ncdsb.com on premise email services, messages are stored on Board systems and messages older than two years will be automatically deleted.
    - For ncdsb.com off-premise email services provided by Microsoft, staff is provided with email storage consisting of 50GB of space which should afford them with email storage for the duration of their employment. Email messages are stored indefinitely and will not be automatically deleted on this platform.
    - For niagaracatholic.ca email services provided by Google, messages are stored indefinitely in accordance with Google's current standard.
    - In accordance with the Records and Information Management Policy, the messages of certain employees will be archived for a seven-year period.