Information and Communications Technology Use

#600.02

Adopted:	September 9, 2003
Last Reviewed/Revised:	September 28, 2021
Responsibility:	Superintendent of Education, Information/Technology
Next Scheduled Review:	May 2025

POLICY STATEMENT:

The Brant Haldimand Norfolk Catholic District School Board (the 'Board') believes that the network, computer systems and associated resources provided by the Board are integral to the education environment and must be made available to students and staff for the purpose of student learning and the business of the Board. 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

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 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.

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.

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.

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.).
- 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 network and computer systems are provided for the use of the students, teachers, staff, and administrators in support of the programs of the Board and are to be used for education, research, academic development, and Board related business only.

A signed acknowledgement form (600.02.01F – Information and Communications Technology Use and Electronic Communications and Social Media Use Acknowledgement Form) must be submitted by all staff, board members and community members who will use technology resources.

The Board retains ownership, control and copyright over all items created, composed, or otherwise developed using board technology resources unless specifically waived or transferred in writing. All requests for waivers or transfer of ownership should be made through an employee's immediate supervisor who will then forward the request to the Superintendent for approval.

The Board assumes no liability for any direct or indirect damages arising from the user's connection to the internet. The Board is not responsible for the accuracy of information found on the internet and only facilitates access and dissemination of information through its systems. The Board's role in managing the network and computer systems is only as an information carrier. Transmission through these systems is not an endorsement of said transmission by the Board.

The Board's network provides users access to outside networks, both public and private, which furnish electronic mail, information services, conferences, social media sites, etc. Users are advised that they may encounter material which may be considered offensive or objectionable in nature or content. Users are further advised that the Board does not assume responsibility for the content of any of these outside networks.

The user agrees to comply with the Acceptable Use Guidelines for all outside networks or services they may access through Board systems.

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 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.

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.