



**Brant Haldimand Norfolk
Catholic District School Board**

ELECTRONIC COMMUNICATIONS AND SOCIAL MEDIA USE

		Policy Number:	600.01
Adopted:	September 9, 2003	Former Policy Number:	n/a
Revised:	October 22, 2013	Policy Category:	Information Technology
Subsequent Review Dates:	n/a	Pages:	2

Belief Statement:

The Brant Haldimand Norfolk Catholic District School Board believes that the electronic communication medium is integral to the education environment and that electronic communication capability should be made available to staff and students for the purpose of student learning and the business of the Board. Further, the Board believes in the benefits that the electronic communication medium can bring to support its daily operating activities and student achievement. As a Catholic learning community, we commit to use electronic communications, social media and all technologies in a manner that is consistent with the Mission and Vision of Catholic education.

Policy Statement:

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

- Information and communication technology tools and resources, including the use of electronic communication and social media by staff, is a viable means to involve colleagues, parents and other staff of the Board in academic dialogue and for the business of the Board.
- Information and communication technology tools and resources are utilized to support staff use of electronic communication and social media such that users interact knowledgeably and responsibly via the internet.
- Teachers and other Board employees are role models in their use of information and communication technology tools and resources, including electronic communication and social media. Parents entrust educators with the duty to educate their children. The Board recognizes that the use of the internet and social media has the potential to affect this trust.
- Information and communication technology tools and resources must be used such that they provide a safe and nurturing environment for learning and working.

Glossary of Key Policy Terms:

User

All employees, students, trustees, members of Board committees, school council chairs and all other persons given authorized access to the Brant Haldimand Norfolk Catholic District School 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 and its employees 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.

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 consistent with Board policies and procedures at all times. Users are expected to use the Board's internet and email services in a lawful 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 of the email or internet systems. Misuse of these systems may, in some instances, subject the Board to lawsuits.



Brant Haldimand Norfolk Catholic District School Board

Social Media

Media designed to be disseminated through social interaction, created using highly-accessible and scalable publishing techniques. Examples include, but are not limited to, LinkedIn, Twitter, Facebook, YouTube, Blogger, MySpace, Instant Messaging and postings on video or picture-sharing sites and elsewhere on the internet.

Primary / Junior Students

Students who are enrolled in a Kindergarten to Grade 6 program.

Intermediate / Senior Students

Students who are enrolled in a Grade 7 to Grade 12 program.

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, CHAPTER 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

Bill 168, Occupational Health and Safety Amendment Act

Workplace Harassment Policy, Reference No. 300.01, Brant Haldimand Norfolk Catholic District School Board

Workplace Violence Prevention Policy, Reference No. 300.20, Brant Haldimand Norfolk Catholic District School Board

Information and Communications Technology Use, Reference No. 600.02, Brant Haldimand Norfolk Catholic District School Board

Electronic Websites Policy, Reference No. 600.03, Brant Haldimand Norfolk Catholic District School Board

Laptop / Netbook / Portable Device Usage for Staff Procedure, Reference No. 600.31, Brant Haldimand Norfolk Catholic District School Board

Laptop / Netbook / Portable Device Support for Staff Procedure, Reference No. 600.32, Brant Haldimand Norfolk Catholic District School Board

Laptop / Netbook / Portable Device Security for Staff Procedure, Reference No. 600.33, Brant Haldimand Norfolk Catholic District School Board

Social Media Playbook, Brant Haldimand Norfolk Catholic District School Board

Social Media Protocol, Brant Haldimand Norfolk Catholic District School Board



Electronic Communications and Social Media Use AP600.01

Procedure for:	All Staff and Students	Adopted:	September 9, 2003
Submitted by:	Superintendent of Business & Treasurer	Revised:	October 22, 2013
Category:	Information Technology		

Purpose

The Brant Haldimand Norfolk Catholic District School Board believes that the electronic communication medium is integral to the education environment and that electronic communication capability should be made available to staff and students for the purpose of student learning and the business of the Board. Further, the Board believes in the benefits that the electronic communication medium can bring to support its daily operating activities and student achievement. As a Catholic learning community, we commit to use electronic communications, social media and all technologies in a manner that is consistent with the Mission and Vision of Catholic education.

Responsibilities

Superintendents, Principals and Managers

- Ensure that staff, upon hiring and annually thereafter, are made aware of Board Information Technology Policies and Procedures, the expectations regarding the use of any Board-supplied technology or the use of any personal device, which connects to the Board's network and / or Board-provisioned technology services (this is applicable regardless of the location from which the services are accessed, i.e., Board location, home, etc.).
- 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.
- Take steps to ensure compliance with the *Municipal Freedom of Information and Protection of Privacy Act*. Student and staff information is personal and private and is, therefore, protected under this *Act*. The Board is obligated by this *Act* to carefully manage all personal information within its custody and control, i.e., how this information is collected, used and released. Personal information belonging to students, parents or staff, such as home addresses, telephone numbers, age, religion or family status, etc., **shall not** be shared without prior permission. Individual consent to post personal information on the internet is necessary as the information is outside of the Board's custody and control once it is on the web.

Principals (or Designates)

- Coordinate and manage electronic communication and social media technologies within their school in accordance with the directives from the District School Achievement Team (DSAT) to promote student achievement.
- Develop an understanding amongst staff for the acceptable use of electronic communication and social media technologies when using Board equipment.

Teachers

- Manage the student use of electronic communication and social media technologies and resources within their assigned teaching areas.
- Instruct and model for students the appropriate use of electronic communication and social media technologies. Instruct all students to comprehend and adhere to all Board Information Technology Policies and Procedures.
- Teachers are responsible for teaching proper techniques and standards for participation, for guiding student access to electronic communication and social media sites and for assuring that students understand that if they misuse access of electronic communications and social media technologies and resources, they may face disciplinary or legal action. Particular concerns include issues of privacy, copyright infringement, email etiquette, cyber bullying and intended use of network resources.
- Consult with the school principal and / or vice principal, 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.
- Take steps to ensure compliance with the *Municipal Freedom of Information and Protection of Privacy Act*. Student and staff information is personal and private and is, therefore, protected under this *Act*. The Board is obligated by this *Act* to carefully manage all personal information within its custody and control, i.e., how this information is collected, used and released. Personal information belonging to students, parents or staff, such as home addresses, telephone numbers, age, religion or family status, etc., **should not** be shared without prior permission. Individual consent to post personal information on the internet is necessary as the information is outside of the Board's custody and control once it is on the web.
- When using electronic communication social networking tools; do so with the appropriate understandings of the effective educational use of these tools and avoid personal use when engaging with students. Use electronic communication and social networking tools with parents and colleagues for professional purposes only.

Students

- Abide by the Board's Information Technology Policies, Procedures and Acceptable Use Agreement.
- Access to the Board's technology resources will be denied to students that do not have *Student Information and Communications technology Use Agreement* forms 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 principal of their 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 of Education or his / her designee and prosecuted to the fullest extent of the law. Computer use by students is a privilege, not a right.
- Students are to obtain permission from a teacher to use Board computer systems and access to the internet.
- Students, who have permission to post information to the internet, must ask the classroom teacher to review the work before it is posted to the internet so that the teacher can verify that the work is consistent with the Municipal Freedom of Information and Protection of Privacy Act and consistent with this Administrative Procedure.
- The use of Board computers and Internet access is a privilege and any breach may result in the closure of user accounts, cancellation of computer and internet privileges and disciplinary action in accordance with Board Policy and the Code of Conduct.

Trustees

- Are responsible for the establishment and governance of Board policies.
- There is an expectation, at all times, of confidentiality with respect to trustee electronic communication accounts. Should access to a trustee account be considered, the procedure defined for trustees in the *Confidentiality – No Expectation of Privacy* section shall be followed.

All Users

- A signed acknowledgement form (Appendix A: 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. Student users of the Brant Haldimand Norfolk Catholic District School Board's technology resources must complete, with applicable signatures, a Brant Haldimand Norfolk Catholic District School Board Student Information and Communications Technology Use Agreement.
- Familiarize themselves with the technology resources provided to them, including administration procedures.
- Ensure that electronic communication and social media technologies are used in an appropriate manner in accordance with Board policies and procedures.
- When required, ensure that strong passwords are created and utilized for accessing electronic communication and social media technologies. Maintain password and user identification confidentiality and restrict access to passwords.
- Use electronic communication and social media technologies in a lawful and ethical manner consistent with the educational, informational and recreational purposes for which they are provided.
- Use technology resources in ways that do not disrupt other users or compromise the functionality of the system.
- Ensure records retention requirements are met, i.e., the minimum amount of time to retain a record and what the actual authority for that period of retention is, by referring to the Classification and Retention Schedule for advice on information ownership within the Board
- All electronic communications systems, its data and messages generated on or handled by Brant Haldimand Norfolk Catholic District School Board equipment are the sole property of the Board and can be traced, viewed and stored.
- Brant Haldimand Norfolk Catholic District School Board staff will notify and fully cooperate with authorities in any investigation relating to activities conducted through the Board's electronic communications systems.

Information

Network and computer systems are the property of the Brant Haldimand Norfolk Catholic District School Board. As such, they should be used for Board purposes only. Use of the network is considered consent to the Board's Electronic Communication and Social Media Policy and to management's right to review correspondence.

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

Commercial uses of Board network and computer systems are specifically excluded. All students, teachers, staff and administrators are responsible for ensuring that computing facilities are used in an effective, efficient, ethical and lawful manner.

The Board assumes no liability and is NOT responsible for the:

- appropriateness of Internet content.
- accuracy or reliability of information located on the internet.
- loss, damage or inaccessibility of information due to technical or other difficulties or costs or losses incurred by users.

Email is not private communication because others may be able to read, access and monitor email (email may best be regarded as a postcard rather than as a sealed letter). The Board may monitor and access email communication in a reasonable manner to;

- maintain and ensure the efficient use of the Board's email services.
- ensure compliance with Board policies and acceptable use.
- assist the user in the event of prolonged absence.

The Brant Haldimand Norfolk Catholic District School Board retains ownership, control and copyright over any work-related 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 or a student's principal, who will then forward the request to the appropriate Superintendent of Education for approval.

Online Social Networking is a process whereby online users are able to connect to other users in a variety of ways and for a variety of purposes, including educational purposes. Current tools include, but are not limited to, Facebook, Twitter, MySpace, LinkedIn, YouTube, Blogger, Instant Messaging and postings on video or picture-sharing sites and elsewhere on the internet.

Blended learning is a model of instructional delivery that includes the use of a learning management system and /or digital online tools. Blended learning promotes:

- improved communication between the teacher and students.
- greater collaboration and critical thinking among students.
- differentiated learning and assessment for all students.

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. Users should be aware that the use of passwords or account numbers does not create a reasonable expectation of privacy and confidentiality of information, which has been maintained or transmitted. The Board reserves the right to review, retrieve, read and disclose any files, messages or communications that are created, sent, received or stored on the Board's computer systems and / or equipment. It is the Board's right to monitor or review all information, which has been maintained or transmitted using the Board's computer and / or telecommunication systems or services 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

System administrators or other support technicians may need to access user files or electronic communication and social media accounts in the normal course of their employment when necessary to protect the integrity of computer systems.

If policy violations are discovered, they will be reported immediately to the appropriate system administrator. The Administrator is not permitted to, intentionally, see or read the contents, to read document information where not germane to the foregoing purpose or disclose or otherwise use what they have seen, unless authorized by a Senior Administrator of the Board. One exception, however, is that of systems personnel who may need to inspect a damaged document in an effort 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.

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

Electronic Communication and Social Media Procedures:

- Individuals who use the Board's electronic communication services are expected to do so responsibly. That is, to comply with local, Provincial and Federal laws, to comply with this and other policies and procedures of the Board and to comply with normal standards of professional and personal courtesy and conduct. Access to the Board's electronic communication services is a privilege that may be wholly or partially restricted by the Board; without prior notice and without the consent of the user when required by and consistent with law, when there is substantiated reason to believe that violations of policy or law have taken place or, in exceptional cases, when required to meet time-dependent, critical operational needs.
- Staff and students are not permitted to access, participate, transmit or save material that does not comply with the Mission, Beliefs, Gospel Values and policies of the Brant Haldimand Norfolk Catholic District School Board.
- Board electronic communication services may not be used for unlawful activities, commercial purposes, personal financial gain and correspondence inappropriate to educational or business purposes.
- Board communication users shall not employ a false identity. Electronic mail bears a number of marks of identification, i.e., domain addresses, which are traceable back to the Board.
- Board communication services shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities or unwarranted or unsolicited interference with others' use of the communication systems.
- Users should be aware that during the performance of their duties, network and computer operations personnel and system administrators need from time to time to observe certain transactional addressing information to ensure proper functioning of Board communication services, and on these and other occasions, may inadvertently see the contents of electronic messages. They are not permitted to see or read the contents intentionally; to read transactional information where not germane to the foregoing purpose; or disclose or otherwise use what they have seen. One exception, however, is the System Postmaster who may need to inspect electronic messages when re-routing or disposing of otherwise undeliverable e-mail. This exception is limited to the least invasive level of inspection required to perform such duties. Furthermore, this exception does not exempt Postmasters from the prohibition against disclosure of personal and confidential information of the previous paragraph, except insofar as such disclosure equates with good faith attempts to route the otherwise undeliverable e-mail to the intended recipient. Re-routed mail normally should be accompanied by notification to the recipient that the e-mail has been inspected for such purposes.
- Users of electronic mail or social media services should be aware that although the sender and recipient have discarded their copies of an electronic record, there may be back-up copies that can be retrieved. Systems are *backed-up* on a routine basis to protect system reliability. The storage media may be retained for periods of time and in locations unknown to the originator or recipient of electronic mail or social media services.
- During normal business hours, email and social media communication may only be used for valid work-related or educational reasons. Email and social media communication should not be used to solicit or to advocate non-Board or purely personal interests. Foul, offensive, defamatory, pornographic or other inappropriate communication is prohibited.
- The employer reserves the right to monitor the e-mail network at any time, without prior notice, to ensure that system is being used for Board purposes only.

- The inadvertent disclosure, accidental transmission to third parties or purposeful re-transmission to another user's internal mailing list can occur in email systems. Users should take reasonable precautions to ensure this does not occur.
- Confidentiality rules for regular mail should be followed for email messages. Disclosure to unauthorized persons is prohibited.
- Electronic messages take up storage space and affect system performance, so users should always delete or save messages to media. Always keep messages remaining in your electronic mailbox to a minimum.
- Be professional and careful about what you say to and about others. Email and social media communication is easily forwarded and shared.
- Misinterpretation of an email message may occur. What was meant as a casual or humorous message can be taken other than intended because body language and tone are missing from the message. Without face-to-face communications, your joke may be viewed as criticism.
- Limit message attachment size and content. Do not use the electronic communication system to transfer large files, i.e., graphics, software, database files, etc. Always note in the body of the message the file format and software version of the attached file to help facilitate access to the attachment.
- Do not use your access or the network in such a way that you could disrupt the use of the facilities by other users.
- At the first indication of a virus, immediately stop the use of the electronic communication service and notify Information Technology technical support. Deliberate transmission of viruses is strictly prohibited.
- An email message can be a record if made or received in connection with the transaction of Board business and must be retained in accordance with the Record Retention Guidelines of the Board and the Freedom of Information and Protection of Privacy Act (MFIPPA). Individual users are responsible for keeping and archiving their own business-related email. Retention of these files is subject to Ontario Provincial laws.
- The Board is obligated to keep records for set periods of time to satisfy statutory, legal, audit, administrative or historical needs.

Conduct which violates this Policy and Procedure includes, but is not limited to:

- Unauthorized use of an electronic communication or social media account.
- Deliberately wasting / overloading computing resources, such as emailing many copies of a document.
- Using Board resources for commercial activity, such as creating products or services for sale.
- Any use that is illegal or in violation of other Board policies, including sending, receiving or storing messages that a *responsible person* would consider to be offensive, disruptive, harassing, threatening, derogatory, defamatory, pornographic, indicative of illegal activity or any that contain belittling comments, slurs or images based on race, color, religion, sex, sexual orientation, age disability or national origin.
- Sending or storing messages or images that would offend or harass on the basis of race, sex, sexual orientation, religion, age, political belief or disability.
- Initiating or propagating electronic chain letters.
- Forging the identity of a user or machine in an electronic communication.
- Deliberately transmitting viruses.

- Sending copies of documents in violation of copyright laws or licensing agreements.
- Attempting to modify or gain access to files, passwords or data belonging to others.
- Using abusive or objectionable language in either public or private messages.
- Misrepresenting oneself or the Board.
- Any use as a forum for communicating by email or any other medium with other school users or outside parties to solicit, proselytize, advocate or communicate the views of an individual or non-school sponsored organization; to solicit membership in or support of any non-school sponsored organization or to raise funds for any non-school sponsored purpose, whether profit or not-for-profit.
- Knowingly provide school email addresses to outside parties whose intent is to communicate with school employees, students and / or their families for non-school purposes.
- Lobbying elected officials and sending material promoting political positions or actions.
- Using electronic communication or social media accounts for personal use *during regularly-scheduled working hours*. (Note: personal use of the internet outside of regular business hours is allowed, provided that it is not being used to generate income for personal business or to promote personal initiatives, provided that all other acceptable use criteria as outlined in this procedure are adhered to).
- 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.
- Any inappropriate communications with students or minors.

Usage of Social Media Sites:

- Staff may use the Board network to access social media sites that are work-related. Staff will not access personal social media sites during school / work hours.
- Students may not use the Board network to access social media sites at any time.
- All users should regularly monitor any content posted to your social media accounts by yourself or others and remove any content that is not appropriate.

Interactions Representing the Brant Haldimand Norfolk Catholic District School Board

- Unless given written permission from a principal or supervisor, staff are not authorized to use electronic social media sites to speak on behalf of the school, department or the Board.
- Personal sites and comments not related to the Brant Haldimand Norfolk Catholic District School Board will clearly state that staff are not representing the views of the school, department or the Board. Any such personal comments should be consistent with this Administrative Procedure, in any event.

Respect, Privacy and Confidential Information

- Staff will not disclose confidential student information or confidential school, department or personnel records without first obtaining written consent from the principal, supervisor or guardian for students under the age of 18 or from students aged 16 or 17 who have removed themselves from parental control.
- Staff will not use electronic social media sites that reflect poorly or are defamatory towards themselves students, Board employees or Board policies and procedures.

- Staff will not engage, electronically, in behavior or comments that would negatively reflect on the school, staff or the Board's reputation.
- Staff may be disciplined if their electronic and / or social media comments and posting, whether personal or school / Board related, result in a disruption to the school or Board environment or negatively impact the staff's ability to perform his or her duties.
- Board and school logos will not be used without first obtaining permission from the school principal or supervisor.
- Staff will use only their own name, when participating in an online social media group.
- Staff will ensure that their online comments respect Catholic values and adhere to the procedures as outlined in the Equity and Inclusive Schools policy.
- Staff can be disciplined for electronic commentary, content or images that are defamatory, pornographic, proprietary, harassing or that create a negative work environment.
- Staff participating in social media activities will respect copyright laws; not only with respect to the content produced on the social media sites, but also to the software which enables it
- Staff participating in social media activities acknowledge that all information posted to sites is subject to the provisions of the Municipal Freedom of Information and Protection of Privacy Act.
- Principals and other supervisors may monitor employee use of social media and social networking websites.

Compensation for Losses, Costs and / or Damages

- Users shall be responsible for any losses, costs or damages incurred by the Board related to violations of this policy and procedure.

Definitions

User

All employees, students, trustees, members of Board committees, school council chairs and all other persons given authorized access to the Brant Haldimand Norfolk Catholic District School 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 and its users are responsible for any misuse of its technology. If a user sends personal views, they must provide appropriate disclaimers so that the remarks are not taken as representative of the Board. In any event, any such personal communications should be consistent with this Administrative Procedure.

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 consistent with Board policies and procedures at all times. Users are expected to use the Board's information technology systems and resources, as well as internet and email services in a lawful 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.

Electronic Communication

Electronic communication include, but are not limited to, email, electronic conferencing, personal and group electronic chat sessions, video conferencing, text messaging and any other means of electronic communication.

System Administrator

The individual responsible for the maintenance of server software, global conferences and other related duties.

Computer Operations Personnel

Personnel employed to provide software and hardware support for computer systems, i.e., Network Technicians, Computer Technicians, Software Technicians and Team Leaders for the Information Technology Services Department.

Postmaster

The person responsible for maintenance of user accounts.

Social Media

Media designed to be disseminated through social interaction, which is created using highly-accessible and scalable publishing techniques. Examples include, but are not limited to, LinkedIn, Twitter, Facebook, YouTube, Blogger, MySpace, Instant Messaging and postings on video or picture-sharing sites and elsewhere on the internet.

Confidential Information

Any and all files, information, materials, or communications of a personal or private nature or including information of a private or personal nature including, without limitation, any files, information, materials or communications, which include, convey or express any information protected by the Education Act, the Municipal Freedom of Information and Protection of Privacy Act or any successor or similar provincial or federal legislation relating to the protection of privacy or students or staff records and information. By way of illustration only, some examples of Confidential Data include:

- Medical records.
- Student records and other non-public student data.
- Social Security Numbers.
- Personnel and / or payroll or records.
- Individualized Education Plans.
- Any data identified by government regulation to be treated as confidential or sealed by order of a court of competent jurisdiction.

Inappropriate Information

Files, information, materials or communications include, but are not limited to, any of the following:

- Hateful, racist or discriminatory material.
- Threatening material.
- Gambling or gaming material.
- Pornographic or obscene material.
- Material which expresses opinions or beliefs of a personal nature unrelated to the educational or business objectives referred to in the policy statement.
- Commercial advertising or similar material.
- Any material deemed by the Board and / or Principal to fall within one of the categories set-out above.

Cyber Bullying

The use of information and communication technologies such as email, cell phone, pager text messages, instant messaging, defamatory personal web sites and defamatory online personal polling web sites to support deliberate behavior by an individual or group that is intended to harm others. The Education Act defines cyber bullying as including:

- Creating a web page or a blog in which the creator assumes the identity of another person.
- Impersonating another person as the author of content or messages posted on the internet.
- Communicating material electronically to more than one individual or posting material on a website that may be accessed by one or more individuals.

Primary / Junior Students

Students who are enrolled in a Kindergarten to Grade 6 program.

Intermediate / Senior Students

Students who are enrolled in a Grade 7 to Grade 12 program.

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, CHAPTER 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

Bill 168, Occupational Health and Safety Amendment Act

Workplace Harassment Policy, Reference No. 300.01, Brant Haldimand Norfolk Catholic District School Board

Workplace Violence Prevention Policy, Reference No. 300.20, Brant Haldimand Norfolk Catholic District School Board

Information and Communications Technology Use, Reference No. 600.02, Brant Haldimand Norfolk Catholic District School Board

Electronic Websites Policy, Reference No. 600.03, Brant Haldimand Norfolk Catholic District School Board

Laptop / Netbook / Portable Device Usage for Staff Procedure, Reference No. 600.31, Brant Haldimand Norfolk Catholic District School Board

Laptop / Netbook / Portable Device Support for Staff Procedure, Reference No. 600.32, Brant Haldimand Norfolk Catholic District School Board

Laptop / Netbook / Portable Device Security for Staff Procedure, Reference No. 600.33, Brant Haldimand Norfolk Catholic District School Board

Information and Communications Technology Use and Electronic Communications and Social Media Use Acknowledgement Form

I acknowledge receipt and understand the Brant Haldimand Norfolk Catholic District School Board *Information and Communications Technology Use* and *Electronic Communications and Social Media Use* Policies and Procedures.

I understand it is my responsibility to review the policies and procedures in detail and request any clarification needed from my supervisor, Human Resource Department or the Manager of Information Technology.

I agree to comply with the Brant Haldimand Norfolk Catholic District School Board Policies and Procedures as listed below.

- Electronic Communication Policy, Reference No. 600.01, Brant Haldimand Norfolk CDSB
- Information and Communications Technology Use, Reference No. 600.02, Brant Haldimand Norfolk CDSB
- Electronic Websites Policy, Reference No. 600.03, Brant Haldimand Norfolk CDSB
- Laptop/Netbook/Portable Device Usage for Staff Procedure, Reference No. 600.31, Brant Haldimand Norfolk CDSB
- Laptop/Netbook/Portable Device Support for Staff Procedure, Reference No. 600.32, Brant Haldimand Norfolk CDSB
- Laptop/Netbook/Portable Device Security for Staff Procedure, Reference No. 600.33, Brant Haldimand Norfolk CDSB

I understand that violation of any policies, procedures and standards may be grounds for disciplinary proceedings. I understand the policies, procedures and standards established herein are to be applied in both a progressive and cumulative manner. I also understand this signed acknowledgment will become a permanent part of my personnel file. I acknowledge that I can download and save or print a copy of the Brant Haldimand Norfolk Catholic District School Board Information Technology Policies and Procedures from the Brant Haldimand Norfolk Catholic District School Board Portal and Website.

I understand that failure to comply with Information Technology Policies and Procedures from the Brant Haldimand Norfolk Catholic District School Board may result in my Information and Communications Technology and Electronic Communications privileges being suspended. I understand that any offense, which violates local, provincial or federal laws, will be referred to the appropriate supervisory officer and / or law enforcement authorities. 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.

Print Name	Employee ID
Position Title School/Department	
Employee's Signature	Date



**BRANT HALDIMAND NORFOLK CATHOLIC
DISTRICT SCHOOL BOARD**

P.O. Box 217, 322 Fairview Drive, Brantford ON N3T 5M8
Phone 519-756-6505 -- Fax 519-756-9913

**Student Information and Communications
Technology Use Agreement
Primary Students
Junior Kindergarten to Grade 3**

Student users of the Brant Haldimand Norfolk Catholic District School Board's technology resources must complete this form with applicable signatures. Students without this signed form on file will be denied access to BHNCD SB technology resources. Students that violate this Agreement will be reported to the Principal of their school and their access to the Board's network may be blocked or removed entirely, depending on the severity of the violation. All illegal activities will be reported to the Superintendent or his/her designee and prosecuted to the fullest extent of the law. Computer use by students is a privilege, not a right.

As a primary student of the Brant Haldimand Norfolk Catholic District School Board, I promise to:

- Take proper care of the computer at all times.
- Keep food and drinks away from the computer.
- Keep any object away from the computer that may cause damage to the computer.
- Use the computer to help me learn as approved by my teacher(s).
- Ask my teacher(s) before I use the computer at school.
- Ask my teacher before I post anything to the internet from a school computer.
- Keep my password secret from other students.
- Use email properly.
- Use only my user name and password on the computer and not another student's name and password.

As a primary student of the Brant Haldimand Norfolk Catholic District School Board, I promise that I will not:

- Use bad language on the computer.
- Use the computer to make fun of another person.
- Use the computers to hurt someone's feelings.
- Use the computer to break the law.
- Use email to bully another student(s).

I understand that failure to comply with Information Technology Policies and Procedures from the Brant Haldimand Norfolk Catholic District School Board may result in my Information and Communications Technology and Electronic Communications privileges being suspended. Further, 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, and legal action. My parent(s)/guardian(s) have reviewed this Agreement with me and have helped me to understand my responsibilities.

Signed,

Student: _____

Parent/Guardian: _____

Parent/Guardian: _____

Date: _____



**BRANT HALDIMAND NORFOLK CATHOLIC
DISTRICT SCHOOL BOARD**

P.O. Box 217, 322 Fairview Drive, Brantford ON N3T 5M8
Phone 519-756-6505 -- Fax 519-756-9913

**Student Information and Communications
Technology Use Agreement
Junior Students
Grade 4 – Grade 6**

Student users of the Brant Haldimand Norfolk Catholic District School Board's technology resources must complete this form with applicable signatures. Students without this signed form on file will be denied access to BHNCDSB technology resources. Students that violate this Agreement will be reported to the Principal of their school and their access to the Board's network may be blocked or removed entirely, depending on the severity of the violation. All illegal activities will be reported to the Superintendent or his/her designee and prosecuted to the fullest extent of the law. Computer use by students is a privilege, not a right.

As a junior student of the Brant Haldimand Norfolk Catholic District School Board, I promise to:

- Properly care for hardware and software at all times.
- Keep food and drinks away from the computer.
- Keep any object away from the computer that may cause damage to the computer.
- Respect the privacy of other students and users on the local area network.
- To use the computer for instructional purposes only as approved by my teacher or adult helper.
- Be mindful to the issues of plagiarism and copyright and I will ask my teacher for direction when I am unsure.

As a junior student of the Brant Haldimand Norfolk Catholic District School Board, I promise that I will not:

- Attempt to log- in using another student's user I.D.
- Knowingly enter into the operating system of the computer or fileserver to alter system setting or configurations.
- Subscribe to chat rooms or newsgroups when on the internet or use it for inappropriate activity.
- Transmit, by electronic means including email, any information or correspondence, which will compromise the reputation of the school or other persons.
- Release my password to anyone other than my teacher, adult helpers or the technical site supervisor.
- Use bad language on the computer.

I understand that failure to comply with Information Technology Policies and Procedures from the Brant Haldimand Norfolk Catholic District School Board may result in my Information and Communications Technology and Electronic Communications privileges being suspended. Further, 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, and legal action. My parent(s)/guardian(s) have reviewed this Agreement with me and have helped me to understand my responsibilities.

Signed,

Student: _____

Parent/Guardian: _____

Parent/Guardian: _____

Date: _____



**BRANT HALDIMAND NORFOLK CATHOLIC
DISTRICT SCHOOL BOARD**

P.O. Box 217, 322 Fairview Drive, Brantford ON N3T 5M8
Phone 519-756-6505 -- Fax 519-756-9913

**Student Information and Communications
Technology Use Agreement
Intermediate/Senior Students
Grade 7 - 12**

Student users of the Brant Haldimand Norfolk Catholic District School Board's technology resources must complete this form with applicable signatures. Students without this signed form on file will be denied access to BHNCDSB technology resources. Students that violate this Agreement will be reported to the Principal of their school and their access to the Board's network may be blocked or removed entirely; depending on the severity of the violation. All illegal activities will be reported to the Superintendent or his/her designee and prosecuted to the fullest extent of the law. Computer use by students is a privilege, not a right.

As an intermediate/senior student of the Brant Haldimand Norfolk Catholic District School Board , I understand that:

- School computers are to be used for educational purposes only.
- The internet is provided so I can conduct research, complete course work and communicate with others.
- My Board email account is not private.
- My files stored on school computers and the board network is not private.
- All communications and information accessible via a school computer or the board network is not private.
- Anything created on a Board-owned computer during school hours is the property of the Board.
- Illegal activities are strictly forbidden.

As an intermediate/senior student of the Brant Haldimand Norfolk Catholic District School Board , I understand that I must:

- Ask permission before using a school computer or device and or accessing the internet at school.
- Review all information that I will be posting to the internet and I must ask permission before doing so.
- Ensure my personal information remains confidential, i.e., password, home address, telephone numbers or those of other students.
- Use school computers for school purposes only.
- Be courteous and respectful in messages to others.
- Use appropriate language on school computers.
- Abide by generally-accepted rules of *netiquette* and conduct myself in a moral and ethical and polite manner while using any school computer.
- Abide by all patent, trademark, trade name and copyright laws.
- Notify a staff member immediately if I can identify a security problem.

As a senior student of the Brant Haldimand Norfolk Catholic District School, I also understand that I must not:

- Use social media in a way that may be harmful to another person.
- Transmit, receive, submit or publish any defamatory, inaccurate, abusive, obscene, profane, sexually-oriented, threatening, offensive or illegal material.
- Use the computer in a way that can harm people or the system (physically, spiritually or emotionally).
- Store files on school computers that are illegal (i.e., downloaded music or movies).
- Use email to bully, harass or embarrass others.
- Forward spam or jokes from Board accounts or to Board addresses.
- Access a computer using another person's username and password.
- Use school or Board logos without my teacher's permission.
- Use the Board's network in such a way that would disrupt the use of the network by other users.
- Attempt to navigate around the Board internet filter.
- Post personal messages on bulletin boards or list servers.
- Use school computer resources for commercial purposes or product advertising.
- Tamper with, illegally access or hack any Board computer resources.

I understand that failure to comply with Information Technology Policies and Procedures from the Brant Haldimand Norfolk Catholic District School Board may result in my Information and Communications Technology and Electronic Communications privileges being suspended. Further, 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 and legal action.

Student's Name: _____ Incoming Grade: _____

Student's Signature: _____ Date: _____

As the parent or legal guardian of the student signing above, I have read the above Agreement and grant permission for my child to access the Information and Communication Technology resources of the Brant Haldimand Norfolk Catholic District School Board. I understand that the Brant Haldimand Norfolk Catholic District School Board's Information and Communication Technology resources are designated for educational purposes only. I also understand that it is impossible for Board staff to restrict access to all controversial materials and I will not hold them responsible for materials acquired on the internet. I understand that individuals and families may be held liable for violations.

Parent's Signature: _____ Date: _____

If student is under 18 years of age

I have read the above Agreement and understand that I will have access to the Information and Communication Technology resources of the Brant Haldimand Norfolk Catholic District School Board. I understand that the Brant Haldimand Norfolk Catholic District School Board's Information and Communication Technology resources are designated for educational purposes only. I also understand that it is impossible for Board staff to restrict access to all controversial materials and I will not hold them responsible for materials acquired on the internet. I understand that I may be held liable for violations.

Signature: _____ Date: _____

Student is over 18 years of age