Brant Haldimand Norfolk
Catholic District School Board

Administrative Procedure

Digital Citizenship and Bring Your Own Device
AP 600.34

Procedure for:	Administrators and School Staff	**Adopted**:	July 14, 2015
Submitted by:	M. Shypula, Superintendent of Education	**Revised**:	N/A
Category:	Information / Technology		

Purpose

The Information and Technology Services Department, in collaboration with the Student Achievement Team, is working to provide infrastructure, devices, and software resources that will support the broadest range of effective learning activities. We believe that by providing the opportunity to bring one's own electronic device (BYOD), we are further enhancing the opportunities for success that information and communication technology can help realize. Teachers will permit the use of personal electronic devices when that use supports and enhances learning.

The goals we seek to achieve through the use of Information and Communication Technology, as well as through the introduction of BYOD for students, are as follows:

- Students use their BYO Devices and those provided by the Board to help build organization and self-regulation skills.
- Students use their BYO Devices and those provided by the Board in authentic, inquiry-driven learning.
- Teacher's role changes from one who delivers content to one who facilitates learning.

In our schools, students will see teachers using technology to support, enhance, and redesign their instructional practices to improve student learning. Many of the new opportunities that students will be engaging in exist in the digital environment of the Internet. When working and interacting in the digital environment of the Internet, it is important that all users understand that their actions impact others, just like in the physical world. When people interact with others, they share themselves, their view of the world, their hopes, and their ideals. When students make use of digital resources, it is expected that their actions will be honest, open, responsible, and respectful of others and consistent with the mission and vision of Catholic education. As Catholic learners, our students must always act in accordance with the Board's Catholic Code of Conduct regardless of whether they are interacting in the digital or physical world.

Responsibilities

All Users are responsible for:

- Completing the age-appropriate informed consent requirement to learn their responsibilities with respect to the use of technology provided by the Board
- Accepting the electronic Acceptable Use Agreement.
- Complying with the Board and School Codes of Conduct and complying with the Board's Electronic Communications and Social Media and Information and Communication Technology Use Policies and Procedures.
- Ensuring that technology is used to support teaching and learning in accordance with the Brant Haldimand Norfolk Catholic District School Board's teaching and learning expectations.
- Using technology in a lawful, responsible and ethical manner consistent with the purposes for which it is provided.
- When required, creating a strong personal password and ensuring that it is not shared with anyone other than a parent/guardian (students).
- Understanding that the Board's Information and Technology Services Department will not perform diagnostics, repairs or updates on personally-owned devices.

All Users are responsible for:

- Understanding that the use of personally-owned devices is prohibited in places or situations where their use is deemed to interfere with student learning.
- Understanding that the use of personally-owned devices with recording ability are absolutely prohibited in areas where there is an increased expectation of privacy, such as a change room or restroom.
- Ensuring that photos, audio recordings, videos or images of an individual/group are not recorded, posted online/shared digitally unless consent from the individual(s) - over the age of 18 - or parental consent (for those under the age of 18) has been obtained. Photos, audio recordings, videos or images cannot be collected using any device unless authorized.
- Understanding that the Board accepts no responsibility or liability for loss or damage to personal devices and that it is the owner of the device's responsibility to safeguard their belongings.
- Understanding that BYO Device is not mandatory.
- Understanding that the Board accepts no responsibility for ensuring that students who have not been provided with parent/guardian permission to bring a device to school comply with their parent(s)/guardian(s) wishes.
- Understanding that the Board accepts no responsibility or liability for the outcomes of actions taken by students when using any software or access to Board information technology, or using of any personal device on school premises, and that it is the user of the software or service or device who must ensure their use is consistent with the mission and vision of Catholic education and in accordance with Board policies and procedures.

Superintendents are responsible for:

- Ensuring that staff, upon hiring and annually thereafter, are made aware of Board Information Technology Policies and Procedures including this Board Administrative Procedure, the expectations regarding the use of any Board-supplied technology or the use of any personal device (BYOD) 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.) so they can in turn support appropriate student use.
- Supporting Principals in determining appropriate action, corrective and disciplinary measures to address student violations of this procedure as necessary, on a case-by-case basis, for situations where students are not in compliance with Board Information Technology Policies and Procedures.
- Taking 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.

Principals are responsible for:

- Coordinating the use of 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.
- Developing an understanding amongst staff for the acceptable use of electronic communication and social media technologies when using Board equipment and personally-owned devices (BYOD).
- Ensuring that staff are aware of Board Information Technology Policies and Procedures including this Board Administrative Procedure.
- Working with staff to develop guidelines for securing devices when staff and students are not in classrooms (i.e., at recess, when at assemblies, etc.). Ultimately, though, students are responsible for lost, stolen and/or damaged personal electronic devices just as they are for any other personal items they bring to school.
- Recognizing that not all children can bring their own device and ensuring there are sufficient devices at school to support all learners.
- Establishing and monitoring digital citizenship and responsibility through the school's Code of Conduct.
- Instructing and modeling, for staff and students, digital citizenship and responsibility.
- Being able to respond to parents /guardian inquiries regarding effective use of BYOD to support student learning.
- Promoting the understanding and collection of parent(s)/guardian(s) consent for their child(ren) bringing personal devices to school.

Teachers are responsible for:

- Along with parents, making every reasonable effort to ensure that students understand how to interact appropriately as Digital Citizens, the Board Information Technology Policies and Procedures and this Administrative Procedure, so they are equipped to use technology appropriately.
- Recognizing that not all students can bring their own device and ensuring there are sufficient devices at school to support all learners.
- Responding to inappropriate use of technology and taking appropriate action, including notifying the principal in cases where the teacher's professional judgment deems it necessary.
- Determining when students are able to access Board technology or their personally-owned devices while the students are under the teacher's supervision.
- Consulting with the principal to determine the extent to which students will be permitted to use their own devices within the classroom.
- Providing guidance to students regarding where they can securely store their devices when staff and students are not in the classroom (e.g., when at recess, when at assemblies, etc.).

Students are responsible for:

- Using Board and personally-owned technology for curriculum-related/educational purposes only while on Board property.
- Demonstrating digital citizenship through the appropriate use of technology.
- Reporting any inappropriate use of technology to a teacher or administrator immediately.
- Taking care of their personal devices. The Board is not responsible for the replacement of lost, stolen or damaged items, or usage fees incurred for school purposes, maintenance or support of the device.
- For elementary students, providing proof of parental permission to bring their personally-owned device(s) to school.
- Learning how to connect their devices to wireless networks, understanding how their device functions, and downloading or installing any apps or programs that they need to use their devices for school and learning purposes.
- Complying with the expectations of the teacher(s) regarding where, when and for what purpose personally-owned devices may be used in the classroom.
- Bringing a fully charged device to school.

Parents/Guardians are responsible for:

- Ensuring that their child is mature and responsible enough to bring a personally-owned device to school and use it appropriately.
- Providing written permission for their elementary-aged child(ren) to enable them to use their personally-owned devices at school.
- Ensuring that the device contains the necessary apps or software to support their child's learning. There is no expectation that the Board will provide or install software on personally-owned devices. The Board uses the best practice of providing software to its users (e.g. Office 365) that can be accessed via the Internet across multiple operating systems and devices without requiring any installation. The Board also promotes the use of Internet-based software that is provided through the Ministry of Education (e.g. D2L and Mindomo) as well as software from the Internet that is freely available to all users across multiple operating systems and devices.
- Ensuring that the device is in good repair and free of viruses, malware, spyware, etc., and that security patches are up to date.
- Ensuring that the student understands and respects the requirement to bring a fully-charged device to school.
- Being aware of school and Board expectations for the use of personal devices and share that understanding with their child(ren).
- Being aware of teacher expectations for classroom use of personal devices and support the teacher, child, and school to ensure that their child complies with the expectations.
- Being aware of activities the children will be engaged in during the school day (e.g., field trip) and making decisions about whether children should bring devices and how they may be secured during the day.

Procedures

1.0 Rights

Computer systems, networks, software, and services are owned and/or operated by the Board. The Board reserves all rights, including termination of service without notice, to the computing resources which it owns and/or 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.

2.0 Privileges

BYOD access and privileges on the Board's computer systems, networks, software, and services are assigned and managed by the administrators of specific individual systems. Eligible individuals may become authorized users of a computing resource (e.g., BYOD network, Office 365, D2L, etc.) 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.

3.0 Accounts

Users do not own accounts on the Board's computers, network, or the software resources that the Board provides access to, but are granted the privilege of exclusive use.

4.0 Confidentiality

No Expectation of Privacy

Users should not expect privacy with respect to any of their activities when using the Board's computers, networks, software, 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 or using the Board's Information Technology resources. The Board's right to review, also called monitoring, is for the purpose of ensuring the security and protection of the Board's resources, preventing unlawful and/or inappropriate conduct, and creating and maintaining a productive learning environment. If policy violations are suspected or discovered, they will be reported immediately to the appropriate school official (e.g., teacher, school principal, Superintendent) and to the authorities as appropriate.

5.0 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. 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 http://www.accesscopyright.ca for more information.

6.0 Violations

A student's device/network/account use privileges may be suspended immediately upon the discovery of a possible violation of Board policies or procedures. Such suspected violations will be confidentially reported to the school principal. The school principal 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, suspension and legal action. Violations of some of the above policies may constitute a criminal offense.

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:

I. Using personally-owned devices or those provided by the Board during instructional time for purposes other than those identified to support their learning.
II. Using personally-owned devices or those provided by the Board in prohibited areas where there is an increased expectation of privacy, such as a change room or restroom.
III. Using personally-owned devices or those provided by the Board in a manner that is inconsistent with the mission and vision of Catholic Education.
IV. Using personally-owned devices or those provided by the Board in a manner that is inconsistent with the terms and conditions of the Board's Information and Communication Technology Acceptable Use Policy, as well as the terms outlined in this Administrative Procedure.

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 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. Students who have questions regarding whether a particular activity or use is acceptable should seek further guidance from their parent/guardian, teacher, or school principal. Teachers and school principals have access to a range of Board staff who can support them and their students in their work to become responsible digital citizens. 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 suspension and/or expulsion. Illegal uses of the Board's Information Technology will also result in referral to law enforcement authorities.

Definitions

BYOD
BYOD is an acronym for Bring Your Own Device, which refers to students bringing their own computing devices (e.g., smartphones, laptops, tablets, and other electronic devices) to schools for use to support their learning.

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 considered to be 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.

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, 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.

Electronic Communication
E-mail, electronic conferencing, personal and group electronic chat sessions, video conferencing, text messaging, and any other means of electronic communication.

System Administrator
Personnel responsible for maintenance of server software, global conferences, and other related duties.

Information and Technology Services Department
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.

References

Bill 13, Accepting Schools Act, 2012
Policy/Program Memorandum No. 128 - The Provincial and School Board Code of Conduct
Policy/Program Memorandum No. 144 - Bullying Prevention and Intervention
Policy/Program Memorandum No. 145 - Progressive Discipline and Promoting Positive Student Behaviour
Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), R.S.O. 1990, CHAPTER M.56
BHNCDSB Student Behaviour, Discipline and Safety Policy 200.09
BHNCDSB Electronic Communications and Social Media Policy 600.01
BHNCDSB Information and Communications Technology Use Policy 600.02