USE OF TECHNOLOGY AND DIGITAL CITIZENSHIP	**OPERATING POLICY:**	**I-43**
	DATE:	November 18, 2014
	AMENDED:	June 16, 2015
	SCHEDULED FOR REVIEW:	June 2018

PURPOSE

The Halton Catholic District School Board (the "Board") is committed to providing and maintaining safe and appropriate environments conducive to learning and working for all. To improve student success and achievement, we must ensure that all students feel safe, welcomed, respected and included.

We want our students to be well-prepared to be successful in an evolving society. Fundamental to such success is the ability to use technology responsibly to gather, evaluate, construct and share knowledge in a 21st Century world. It is imperative that we support our students as 21st Century learners to help them become collaborative contributors, responsible citizens, and self-directed, responsible, lifelong learners.

Digital citizenship is defined as the norms of legal, ethical and responsible behaviour related to the appropriate use of technology. These norms and responsibilities are an expectation in all Halton Catholic District School Board (HCDSB) locations and are clearly outlined in each school's Code of Conduct. As individuals, we live and work in a world where many people are connected to their devices at all times so we need to use technology effectively and respectfully. Digital citizenship is an important part of what the Board helps students learn in school.

APPLICATION AND SCOPE

The Board provides users with access to appropriate technology to support teaching and learning, and to enable efficient Board administration and communication. Technology, including personally owned devices, must be used appropriately for these intended purposes.

This Use of Technology and Digital Citizenship policy supports the principles and expectations of the Board's Safe Schools policies (II-39, II-40), and the Board's commitment to providing education that is distinctively Catholic, nurturing the call to love and serve by creating positive climates for learning and working.

This Use of Technology and Digital Citizenship policy is aligned with and supports the principles and expectations of the Board's Equity and Inclusive Education policy (II-45). At all times, this policy should be interpreted to be consistent with the Board's other policies and the Ontario *Human Rights Code*.

Students will see teachers incorporate digital resources into their lessons where appropriate and students will use digital resources to demonstrate their learning. Educational online resources will be able to be accessed wirelessly through the Board's networks. As such, students will be encouraged to BYOD (Bring Your Own Device). When relevant to curriculum and instruction, teachers may permit the use of any personal electronic device in a manner that meets the current policy as a classroom learning device. A personal electronic device is any technology device that is brought into a school and owned by a user. A user may include students, a student's family, a staff member, volunteer, visitors, contractors, individuals employed by service providers or a guest.

Students will also be able to access educational resources using their personal electronic devices outside the classroom, in libraries, learning commons, cafeterias and other common areas. By accessing the Internet while on Board property or by logging in with a Board login, students accept all terms and conditions of theBoard network and Internet use, as well as the terms outlined in this policy.

This Policy applies to all Board technology and to all personally owned technology, as defined below, and includes:

- the use of all Board-owned technology, such as computers, tablets, phones and mobile devices, networks, applications, and websites regardless of where they are used. This includes the use of Board-owned technology when used off Board property.

- the use of personally owned technology, including personally -owned computers and mobile devices, when used on Board property or when used to access Board resources. Inappropriate use of personally owned technology, while on or off school property, which has a negative impact on school climate will result in a full investigation and necessary action will be taken, where appropriate. Consequences for inappropriate use are outlined both in the Code of Conduct as well in the Board's Safe Schools policies (II-39, II-40).

- any access to Board technology resources regardless of the location and ownership of the device used to access Board resources. Specifically, the Policy applies to home, remote, or wireless access to the Board network, websites and applications.

- the use of third-party information technology services provided to the Board. This includes Internet services provided by the Ministry of Education.

PRINCIPLES

There are five guiding principles for the use of technology, digital citizenship and responsibility:

I. Intended use: Board technology is provided for educational and administrative purposes. Technology should be used for these intended purposes only.

II. Security and safety of Board data: Users should take reasonable precautions to ensure that the data that they use is secure and safe. Data should be used for the intended purposes only.

III. Responsible resource usage: The Board's technology resources are shared and limited. Users should use technology resources responsibly and should not waste resources.

IV. Legal compliance and adherence to Board Policies: Users are expected to comply with federal and provincial legislation, as well as Board policies and corresponding Operating Procedures.

V. Ownership and use of data:

(a) Personal materials not relevant to educational and administrative purposes should not be stored on Board servers at any time, for any reason, by a user.

(b) Board technology and all data stored on Board technology by the Board are owned and may be accessed by the Board. In addition, users should have no

expectation of privacy in anything they create, store, send or receive using Board technology and any such data may be used, accessed and otherwise shared by the Board in such manner as it may solely determine.

I. INTENDED USE

Prohibited uses of Board technology and related data include:

(a) personal use that is not limited and/or occasional / use that violates federal or provincial laws, including:

- use of Board technology for commercial or political purposes.
- use that contravenes Board Policies and/or Operating Procedures; and
- theft of resources, including electronic data theft.

(b) unauthorized access, disclosure or use of data or Board technology, including:

- unauthorized access, alteration, destruction, removal and/or disclosure of data. This includes the unauthorized disclosure of Board email addresses, distribution lists, and user account information;
- creating, processing, displaying, storing, accessing or distributing fraudulent, harassing, sexually explicit, profane, obscene, intimidating, defamatory or otherwise inappropriate or unlawful materials;
- cyberbullying , including but not limited to, sending/receiving defamatory, abusive, obscene, profane, sexually oriented, threatening or racially offensive messages;
- copying, downloading, transferring, renaming, adding or deleting information protected under copyright law;
- use that could reasonably be expected to impair, disable or compromise the Board's computing facilities or the security of information contained on the Board's computer systems, or otherwise interfere with others' use of Board technology (e.g. viruses, spam) including the sending of electronic "chain" mail;
- conducting business activities which are unrelated to the staff member's duties and responsibilities at the Board;
- attempting to access another person's account or private files or misrepresenting yourself as another person in electronic communications; and
- agreeing to license or download material for which a fee is charged to the Board without obtaining express written permission from Curriculum Services or the

appropriate departmental supervisor. Purchasing of materials and services must comply with all procurement policies and procedures.

II. SECURITY AND SAFETY OF BOARD DATA

Users should take reasonable precautions to ensure that data that they use is secure and safe. Each user shall take reasonable precautions to protect the integrity of the Board's computer systems and to prevent unauthorized access to the technology. Staff are given access to data in order to perform their job functions. Data should be used for the purposes intended. Other uses of data are strictly prohibited. Data may include but is not limited to student records, employee records, confidential assessments, and other personal information. Data may be held in more than one format, such as an electronic document (e.g. Word Document) or in a system such as email or the Student Information System. All Board data is included in this Policy.

Users are responsible for managing the accounts and passwords that provide access to data. Users are responsible for applying passwords to any personal electronic device that accesses or holds Board data. Users will not attempt to gain unauthorized access to Board technology or data nor will they attempt to disrupt or destroy data. Users must exercise reasonable care to ensure the safety of the data entrusted to them. All confidential data not held on Board-owned servers must be fully encrypted. This applies to all confidential data stored on Board and personally owned computers. The storage of confidential Board data on the Internet is strictly prohibited.

Users must comply with any security measures implemented by the Board. All files downloaded from the Internet must be scanned with Board-approved virus detection software disabling virus scanning is strictly prohibited. Users are responsible for implementing virus scanning on personally owned devices that hold or access Board technology. Users downloading or placing software or media, including open source software, from the Internet on the Board network must obtain approval in advance by Curriculum Services and must abide by the terms of all license agreements relating to the Board's technology.

Remote or wireless access to Board resources is only permitted through the Board's approved infrastructure. Users will not attempt to by-pass the Board's security.

III. RESPONSIBLE RESOURCE USAGE

The Board's technology resources are shared and limited. Users should use technology resources responsibly and should not waste resources. As such, the Board reserves the right to limit any activity that consumes a high level of resources that may impact Board services or other users. Examples of shared resources include file storage, network bandwidth, and Internet access. Access to Internet websites and services that significantly impact the Board Internet or network performance will be limited. Users are not permitted to circumvent the Internet and network controls put in place.

Personal materials not relevant to educational and administrative purposes should not be stored on Board servers at any time, for any reason, by a user.

With respect to information stored for the intended purposes, the Board may impose retention periods for various information classes, either temporarily or permanently. A user should not download, copy or store files that exceed the user's data storage limit; users that do so will experience data loss.

IV. LEGAL COMPLIANCE AND ADHERENCE TO BOARD POLICIES

Users are expected to comply with all federal and provincial laws and regulations (e.g. *Criminal Code*, *Education Act*, *Municipal Freedom of Information and Protection of Privacy Act*, *Copyright Act*). The storage of unlawful materials on Board property is strictly prohibited. Board resources may not be used in any manner to create, store, send, display or make available to others material that contravenes federal or provincial laws or regulations.

V. EXPECTATION OF PRIVACY

Board technology resources and all data stored on Board technology by the Board, including hosted and cloud-based, are owned and may be accessed by the Board. In addition, users should have no expectation of privacy in anything they create, store, send or receive using Board technology and any such data stored on Board technology may be used, accessed and otherwise shared by the Board in such manner as it may solely determine. Data is also subject to relevant legislation and may be accessed through Freedom of Information requests.

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 that are 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. Users will not necessarily be notified when such monitoring is to take place, or whether monitoring has occurred. If policy violations are discovered, this will result in an investigation and necessary action will be taken, where appropriate.

In certain situations, the Board may be compelled to access, read, copy, reproduce, print, retain, move, store, destroy and/or disclose messages, files or documents stored in or sent over its email, Internet or computer systems. These situations may include the following:

- in the course of regular maintenance of the Board's computer system;
- in the event of a request for documents as part of litigation or similar proceedings; or
- where the Board has reason to believe that the Board's computer system is being used in violation of this policy.

Information stored on personally owned devices is the responsibility of the device owner/user. However, personally owned devices which are used for creating, displaying, storing or sending fraudulent, harassing, sexually explicit, profane, obscene, intimidating, defamatory or otherwise inappropriate or unlawful materials that impact school climate will result in a full investigation and necessary action will be taken, where appropriate.

REQUIREMENTS

DEFINITIONS

Technology – Technology resources include, but are not limited to, computers, tablets, phones, cellular/mobile technology, servers, networks, Internet services, computer applications, data, email and collaboration tools, as well as third-party Internet service providers to the Board include E-Learning Ontario and online textbook vendors. The examples of the services they provide are software, virtual learning environments and digital textbooks.

User – A user is any individual granted authorization to access technology, as defined above. Users may include students, students' family, staff, volunteers, visitors, contractors, ~~or~~ individuals employed by service providers or a guest.

(a) All users are responsible for:

- ensuring that technology is used in accordance with Board policies and procedures;
- complying with the school's Code of Conduct;
- ensuring that technology is used to support teaching and learning in accordance with the Board's teaching and learning expectations;
- using technology in a legal, ethical, safe and responsible manner consistent with the purposes for which it is provided;
- security of their personal network logins and passwords - they should not be shared with anyone other than a parent/guardian (students) or, in some cases, Board personnel, such as but not limited to teachers, administrators, or IT account administrators;
- ensuring that photos, videos or images of an individual/group are not 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 at the beginning of the school year; and
- that technology is not used for political or union business unless approved by the Board.

(b) Superintendents, principals and managers/supervisors are responsible for:

- ensuring that staff are aware of the Board policy;
- 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 ; and

- ensuring that all communication is in compliance with applicable privacy legislation, and that all records in the custody and control of the Board that contain personal information that pertains to a student or staff member will be maintained in strict confidence.

(c) Teachers are responsible for:

- the supervision of student use of technology within the teacher's assigned teaching area;

- instructing and modeling~~,~~ for students~~,~~ digital citizenship, responsibility~~,~~ and the safe use of technology;

- determining when students are able to access Board technology or their personally owned devices, for educational purposes only ; and

- ensuring that all communication is in compliance with applicable privacy legislation, and that all records in the custody and control of the Board that contain personal information that pertains to a student or staff member will be maintained in strict confidence.

(d) Students are responsible for:

- using Board technology for curriculum-related/educational purposes only;

- using personally owned technology for curriculum-related/educational purposes only while on Board property (e.g. classrooms or instructional areas);

- using personally owned technology for personal use only in specific areas of Board property as designated by school administration;

- using personally-owned technology in accordance with the obligations and responsibilities outlined in this policy;

- demonstrating digital citizenship through the appropriate use of technology, as outlined in schools' Codes of Conduct;

- reporting any inappropriate use of email, data or unauthorized technology to a teacher or administrator immediately; and

- the care, maintenance and security of their personal electronic devices – the Board is not responsible for the replacement of lost, stolen or damaged items.

CONSEQUENCES: REMEDIAL AND DISCIPLINARY ACTION

Individuals who do not comply with this Policy will be subject to appropriate consequences consistent with the school's Code of Conduct, progressive discipline and Part XIII of the *Education Act* entitled Behaviour, Discipline and Safety.

Consequences may include, but are not limited to, the following, either singularly or in combination depending on the individual circumstances:

- limitations being placed on access privileges to personal and Board technology resources;
- suspension of access privileges to personal and Board technology resources;
- revocation of access privileges to personal and Board technology resources;
- appropriate disciplinary measures (staff), up to and including dismissal;
- appropriate progressive discipline measures (students) within Part XIII of the *Education Act* entitled Behaviour, Discipline and Safety; or
- legal action and prosecution by the relevant authorities.

APPROVED: Regular Meeting of the Board

Authorized by: .....
Chair of the Board