DIGITAL CITIZENSHIP

Digital Citizenship

Digital citizenship is defined as the norms of responsible behaviour related to the appropriate use of technology. These norms and responsibilities are an expectation in all Peel District School Board locations and are clearly outlined in each school's Code of Conduct. As individuals, we live and work in a world where 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.

Students will see teachers incorporate digital resources into their lessons. 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 will permit the use of any personal electronic device as a classroom learning device.

Students will also be able to access educational resources using their personal devices outside the classroom, in libraries, cafeterias and other common areas.

By accessing the Internet while on Peel board property or by logging in with a board login, students accept all terms and conditions of the Peel board network and Internet use, as well as the terms outlined in this policy.

Statement of Policy

The Peel District School 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 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.

The Board provides users with access to 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.

The Digital Citizenship policy supports the principles and expectations of the Board's Safe Schools policy (Policy #48) and the Board's character attributes—caring, respect, cooperation, honesty, responsibility, inclusion—to create positive climates for learning and working, and school Codes of Conduct.

The policy is aligned with and supports the principles and expectations of the Board's Human Rights policy (Policy #51) and the Equity and Inclusive Education policy (Policy #54). At all times, this **policy** should be interpreted to be consistent with the Board's policies and the *Human Rights Code*.

Definitions

Technology – Technology resources include, but are not limited to, computers, phones, cellular/mobile technology, servers, networks, Internet services, computer applications, data, email and collaboration tools, as well as third-party Internet services provided to the Board. Examples of third-party web services include E-Learning Ontario and online textbook providers.

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

A. Responsibilities

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 Peel's teaching and learning expectations*
- *using technology in a lawful, responsible and ethical manner consistent with the purposes for which it is provided*
- *their personal network login and password—it should not be shared with anyone other than a parent/guardian (students)*
- *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. Photos, videos or images cannot be taken using any device unless authorized.*
- *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*

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

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*

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

B. Scope

This Policy applies to all Board technology and to all personally owned technology, as defined above. The application of this Policy includes:

- the use of all Board-owned technology, such as computers, 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. The policy also applies to use of personally owned technology when off board property. Inappropriate use of personally owned technology, while on or off school property, that 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 policy (Policy #48).
- 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.

C. Guiding Principles

There are five guiding principles for digital citizenship and responsibility:

1. **Intended use:** Board technology is provided for educational and administrative purposes. Technology should be used for these intended purposes only.
2. **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.
3. **Responsible resource usage:** The Board's technology resources are shared and limited. Users should use technology resources responsibly and should not waste resources. Personal materials should not be stored on Board property.
4. **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.

5. **Ownership of data:** Board technology and all data stored on Board technology are owned and may be accessed by the Board. Users should have no expectation of privacy in anything they create, store, send or receive using Board technology.

C.1 Intended Use

Technology is provided for educational and administrative purposes and should be used for these intended purposes only.

Prohibited uses of technology include, but are not limited to:

- personal use that is not limited and/or occasional
- use that violates federal or provincial laws
- use of Board technology for commercial or political party purposes
- use that contravenes Board Policies and/or Operating Procedures
- theft of resources, including electronic data theft
- 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.
- unauthorized access or disclosure of confidential information
- creating, displaying, storing or sending fraudulent, harassing, sexually explicit, profane, obscene, intimidating, defamatory or otherwise inappropriate or unlawful materials
- cyberbullying
- copying, downloading, transferring, renaming, adding or deleting information protected under copyright law
- use that could reasonably be expected to impair the Board's computing facilities or interfere with others' use of Board technology (e.g. viruses, spam) including the sending of electronic "chain" mail
- agreeing to license or download material for which a fee is charged to the Board without obtaining express written permission from the Board's Learning Technology Support Services staff. Purchasing of materials and services must comply with all procurement policies and procedures.

C.2 Security and Safety of Board Data

Users should take reasonable precautions to ensure that data that they use is secure and safe. 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 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. All downloading of software from the Internet must be approved in advance by the Board's Learning Technology Support Services staff.

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.

C.3 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 will not be stored on Board servers at any time, for any reason.

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.

C.4 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.

C.5 Expectation of Privacy

Board technology resources and all data stored on Board technology are owned and may be accessed by the Board. Data stored on Board technology, including email, electronic files, and information in computer systems, is Board property and may be reviewed, monitored and

accessed by authorized individuals, as needed. 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. If policy violations are discovered, this will result in an investigation and necessary action will be taken, where appropriate.

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.

D. Digital citizenship

Digital citizenship and responsibility is an expectation in each school's Code of Conduct. Students live and work in a world where people are connected to their devices at all times so they need to learn to use technology effectively and respectfully. Digital responsibility is an important part of what the Board helps students learn in school.

Students will see teachers incorporate digital resources into their lessons. 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 will permit the use of any personal electronic device as a classroom learning device.

Students will also be able to access educational resources using their personal devices outside the classroom, in libraries, cafeterias and other common areas. Students will use technology for educational purposes only.

By accessing the Internet while on Peel board property or by logging in with a board login, students accept all terms and conditions of the Peel board network and Internet use, as well as the terms outlined in this policy.

E. Consequences: Remedial and Disciplinary Action

Individuals who do not comply with this Policy will be subject to appropriate consequences consistent with the school Code of Conduct, progressive discipline and Safe Schools legislation. 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 Bill 212 (Progressive Discipline and School Safety)
- legal action and prosecution by the relevant authorities

(Bold print together with underlining indicates new language)
(** signifies removal of language)

Approved: April 26, 2011
Approved: February 12, 2013 *(replaces former Policy #78 – Appropriate Use of Technology)*