Algonquin & Lakeshore
Catholic District School Board

ADMINISTRATIVE PROCEDURES

DIGITAL CITIZENSHIP (Policy Statement: Digital Citizenship)

Purpose

The Algonquin and Lakeshore Catholic District School Board supports access to technology to enhance learning and teaching, to improve student success and achievement, and to enable efficient Board administration and communication. Technology, including personally owned devices, must be used for these intended purposes. The purpose of the Administrative Procedures for Digital Citizenship is to establish the guidelines under which these conditions are supported.

References

Great to Excellent: Launching the Next Stage of Ontario's Education Agenda
Caring and Safe Catholic Schools, S-2013-05-4
Ottawa Catholic School Board Policy Statement
Peel District School Board Policy #78
Digital Citizenship: Samaritans on the Digital Road
Ontario Catholic School Graduate Expectations

Procedures

1. 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.

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.

Digital Citizenship – Responsible digital citizenship is the expectation of the Algonquin and Lakeshore Catholic District Board. Staff and students live, learn and work in a world where they use technology effectively and respectfully. Digital responsibility is an important part of what the Board helps students learn in school and what the Board expects from staff. By accessing the Internet while on Algonquin and Lakeshore Catholic District School Board property, by logging in with a board login, or when using digital tools as a student or employee of the Algonquin and

Lakeshore Catholic District School Board, staff and students accept all expectations and conditions of the Algonquin and Lakeshore Catholic District School Board Digital Citizenship Policy and Procedures, as well as the terms outlined in related Board Policy and Procedures.

2. Scope

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

2.1.1. the use of all Board-owned technology, such as computers, 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.

2.1.2. 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 the 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.

2.1.3. 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.

2.1.4. the use of third-party information technology services used by staff and students.

3. Responsibilities

3.1. All users are responsible for:

3.1.1. ensuring that technology is used in accordance with Board policy, administrative procedures, and relevant Code of Conduct.

3.1.2. ensuring that technology is used to support teaching and learning in accordance with ALCDSB's teaching and learning expectations.

3.1.3. using technology in a lawful, responsible and ethical manner consistent with the purposes for which it is provided.

3.1.4. their personal network login and password—it should not be shared with anyone other than a parent/guardian (students).

3.1.5. ensuring that photos, videos, images or audio 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.

3.1.6. technology is not used for political or union business unless approved by the Board.

3.2. Superintendents, principals and managers/supervisors are responsible for:

3.2.1. ensuring that staff are aware of the Board Policy and Administrative Procedures.
3.2.2. establishing and monitoring digital citizenship and responsibility through the Board's Policy and Administrative Procedures and through the school's Code of Conduct.
3.2.3. instructing and modeling, for staff and students, digital citizenship and responsibility.

3.3. Teachers are responsible for:

3.3.1. supervising student use of technology during supervised instruction.
3.3.2. instructing and modeling, for students, digital citizenship and responsibility.
3.3.3. determining when students are able to access Board technology or their personally owned devices.

3.4. Students are responsible for:

3.4.1. using Board technology for curriculum-related/educational purposes only.
3.4.2. demonstrating digital citizenship through the appropriate use of technology, as outlined in Board Policy and Administrative Procedures and the schools' codes of conduct.
3.4.3. reporting any inappropriate use of email, data or unauthorized technology to a teacher or administrator immediately.

3.5. Students will:

3.5.1. be permitted to Bring Your Own Device (BYOD), and when relevant to curriculum and instruction, teachers may permit the use of a personal electronic device as a classroom learning device.
3.5.2. may use personally owned technology devices to access curriculum and educational related resources while on Board property (eg., outside the classroom, in libraries, cafeterias and other common areas).
3.5.3. are responsible for the care, maintenance and security of their personal devices—the Board is not responsible for the replacement of lost, stolen or damaged items.

4. Intended Use

Board technology is provided for educational and administrative purposes. Technology should be used for these intended purposes only. Prohibited uses of technology include, but are not limited to:

4.1. use that violates federal or provincial laws.
4.2. use of Board technology for commercial or political party purposes.
4.3. use that contravenes Board Policies and/or Administrative Procedures.
4.4. unauthorized access, alteration, destruction, removal and/or disclosure of data, including the unauthorized disclosure of Board email addresses, distribution lists, and user account information.
4.5. unauthorized access or disclosure of confidential information.

4.6. creating, displaying, storing or sending fraudulent, harassing, sexually explicit, profane, obscene, intimidating, defamatory or otherwise inappropriate or unlawful materials.
4.7. cyberbullying.
4.8. copying, downloading, transferring, renaming, adding or deleting information protected under copyright law.
4.9. 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.
4.10. agreeing to license or download material for which a fee is charged to the Board without obtaining express written permission from the appropriate Supervisor. Purchasing of materials and services must comply with all procurement policies and procedures.

5. 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.

5.1. 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.
5.2. 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.
5.3. 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.
5.4. Users must exercise reasonable care to ensure the safety of the data entrusted to them.
5.5. Users must comply with any security measures implemented by the Board. Disabling virus scanning is strictly prohibited. Any downloaded software that inhibits normal operation of the technology will be removed.
5.6. 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.

6. Responsible Resource Usage

The Board's technology resources are shared and limited.

6.1. 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.
6.2. 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.
6.3. With respect to information stored for the intended purposes, the Board may impose retention periods for various information classes, either temporarily or permanently.

7. 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), as well as Board Policies and corresponding Administrative Procedures

7.1. 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.

8. Ownership of Data and Expectation of Privacy

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.

8.1. 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.

8.2. 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.

8.3. Information stored on personally owned devices is the responsibility of the device owner/user. 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.

9. Digital Responsibility

Individuals who do not comply with this Policy and associated or related Administrative Procedures will be subject to appropriate consequences consistent with the Board's Policies and Administrative Procedures, and any other associated legislature and policies. Consequences may include, but are not limited to, the following, either singularly or in combination depending on the individual circumstances:

9.1. limitations being placed on access privileges to personal and Board technology resources.
9.2. suspension of access privileges to personal and Board technology resources.
9.3. revocation of access privileges to personal and Board technology resources.
9.4. appropriate disciplinary measures (staff), up to and including dismissal.
9.5. appropriate progressive discipline measures (students).
9.6. legal action and prosecution by the relevant authorities.

Appendices
Forms
Associated Documents

Approved: May 27, 2014
Revised: May 2019