

# ADMINISTRATIVE PROCEDURE 146

## Digital Citizenship

---

### Digital Citizenship

Digital citizenship is defined as the norms of responsible behaviour related to the appropriate use of technology. As individuals, we live and work in a world where people are connected to their devices so we need to use technology effectively and respectfully. Digital citizenship is an important part of what the Board helps students learn in school.

When accessing any Limestone DSB networks or services, users accept all terms and conditions of the Administrative Procedure 351 (Safe Schools; The Use of the Internet and Electronic Devices by Students), as well as the terms outlined in this procedure.

### Statement of Vision

The Limestone 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. Students need 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 and ensure they use technology appropriately.

The Board provides users with access to technology to support teaching and learning, and to enable efficient Board administration and communication. To this end, students in Limestone will be provided with the Google Suite for Education, Microsoft tools, and the Desire 2 Learn Virtual Learning Environment (Minds Online in Limestone). These accounts, through the @limestone.on.ca domain, provide access to a set of online tools for communication, collaboration, time-management, document creation, and file storage. Email services for Kindergarten to Grade 6 will be limited to internal LDSB (student to student, or student to staff). Email services for Grades 7-12 will be internal and external. Technology, including personally owned devices, must be used appropriately for these intended purposes.

### Guiding Principles

There are six 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. Personal materials should not be stored on Board property.

# ADMINISTRATIVE PROCEDURE 146

## Digital Citizenship

---

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 Administrative 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 the expectation that anything they create, store, send or receive using Board technology may be monitored, or accessed, under circumstances where an investigation is required.
  6. Privacy: While personal files and communications are not regularly or routinely monitored, personal files and messages can be accessed if credible concerns are raised related to the content of either as part of an investigation.
- A. Responsibilities
- 1.0 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 Limestone’s teaching and learning expectations
    - changing their default/initial system password to a new, secure password that would never be shared
    - using technology in a lawful, responsible and ethical manner consistent with the purposes for which it is provided
    - securing their personal network login and password—it should not be shared with anyone other than a parent/guardian (students)
    - ensuring that audio, photos, videos or images of an individual/group are not taken or 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.
    - ensuring technology is not used for political or union business unless approved by the board
  - 2.0 Superintendents, principals and managers/supervisors are responsible for:
    - ensuring that staff and students are aware of the Board policy and Administrative Procedures
    - establishing and monitoring digital citizenship and responsibility through the school’s Code of Conduct
    - modeling, for staff and students, digital citizenship and responsibility
  - 3.0 Teachers are responsible for:
    - the supervision of student use of technology within the teacher’s assigned teaching area

## ADMINISTRATIVE PROCEDURE 146

### Digital Citizenship

---

- 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
- appropriate, professional use of technology during the instructional day

#### 4.0 Students are responsible for:

- using Board technology for curriculum-related/educational purposes only
- using personally owned technology (under the discretion of the classroom teacher) for curriculum-related/educational purposes 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, texting, 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
- notifying a staff member if they believe their password has been compromised
- using electronic communication for school/curriculum-related educational purposes with the understanding the students from Kindergarten to Grade 6 will only have email privileges for internal communication within the Board, and students from Grades 7-12 will have email privileges for internal/external communication.

#### 5.0 Scope

This Administrative Procedure applies to all Board technology and to all personally owned technology. The application of this Administrative Procedure 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.
- 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.

# ADMINISTRATIVE PROCEDURE 146

## Digital Citizenship

---

### 6.0 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 or that incurs costs to the board.
- use that violates federal or provincial laws
- use of Board technology for commercial or political party purposes
- use of Virtual Private Networks (VPN) to circumvent network settings
- 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 a Board account without obtaining express written permission from the Principal/Manager/Supervisor who oversees the account. Purchasing of materials and services must comply with all procurement policies and procedures.

### 7.0 Consequences for Unacceptable Use

Unacceptable use will be dealt with in accordance to the school's Code of Conduct and/or relevant Board administrative procedures. This could result in the loss of network access privileges, temporary confiscation of devices, and/or other disciplinary actions.

#### Legal References:

Education Act, s. 306(1)

Municipal Freedom of Information and Protection of Privacy Act, s. 14.(1),(2)

December 2018