



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 essential to what the Limestone District School Board helps students learn in school.

Digital Hygiene

Digital hygiene refers to the consistent and responsible practices that individuals follow to protect their personal information, maintain the security of digital devices, and ensure safe participation in online environments. Digital hygiene includes habits such as using strong passwords, logging out of shared devices, avoiding suspicious links, separating personal and school/work-related content, and using only Board-approved tools and platforms. Practicing good digital hygiene helps students and staff contribute to a safe, respectful, and secure digital learning and working environment.

When accessing any Limestone District School Board networks or services, users accept all terms and conditions of Administrative Procedure 351 (Safe Schools; The Use of the Internet and Electronic Devices by Students) and 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 using technology responsibly to gather, evaluate, construct, and share knowledge in an interconnected world. We must ensure that our students use technology safely and responsibly, understanding how technology impacts our lives and



taking care of their physical, mental, and emotional well-being.

The Board provides users access to technology to support teaching and learning, enabling efficient Board administration and communication. To this end, the Board provides all students in Limestone with Microsoft 365 education apps, Google Suite for Education, the Desire 2 Learn Brightspace Virtual Learning Environment (Minds Online in Limestone), and some access to educational apps via Apple devices. Through the @limestone.on.ca domain, user accounts provide access to 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 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 and digital hygiene:** The Board's technology resources are shared and limited. Users should use technology resources responsibly and maintain high standards of digital hygiene, including separating work-related data from personal content and using only LDSB-managed digital tools. 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, 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 about their potential content or as part of an investigation.

1. Responsibilities

1.1. 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
- changing their default/initial system password to a new, secure password that should not be shared
- securing their personal network login and password that should not be shared with anyone other than a parent/guardian (students)
- using technology in a lawful, responsible and ethical manner consistent with the purposes for which it is provided
- ensuring that technology is used to support teaching and learning in



accordance with Limestone's teaching and learning expectations

- ensuring that audio, photos, videos or images of an individual or group are not taken or posted online or 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 that while using any form of artificial intelligence (AI), and generative AI in particular [e.g. ChatGPT, Copilot, Gemini (formerly Bard), etc.,] that no LDSB information, including school or Board name, staff or student-related information, or personal information is entered into the platform(s)
- ensuring technology is not used for political or union business unless approved in advance by the Board
- reporting any lost or damaged Board-owned devices to your superintendent, principal or manager/supervisor
- Students in Grades 7 to 12 must keep their personal mobile devices stored out of sight and either powered off or set to silent mode during instructional time, except when an educator grants explicit permission for use under the specified circumstances
- Students in Grade 6 and below, the policy is even more stringent, requiring that personal mobile devices remain stored out of view and powered off or set to silent mode throughout the entire instructional day, except in the cases outlined by the educator.
- All members of the school community are prohibited from using personal mobile devices during instructional time, except under the following conditions:
 - For educational purposes, as directed by an educator

- For health and medical reasons
- To support special education needs
- Users must report suspicious emails and online activities to security@limestone.on.ca and participate in ongoing digital citizenship education and phishing simulations, as provided by ITS.

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

- ensuring that staff and students and student caregivers are aware of the Board policy and administrative procedures
- establishing and monitoring digital citizenship and responsibility through schools' codes of conduct
- modelling for staff and students, digital citizenship, and responsibility
- restricting screen time for students in Kindergarten to Grade 6 may not use mobile devices at school during the school day, except in certain cases at the discretion of a teacher.
- Principals may make exceptions to allow for the live streaming of events of local, provincial, national, or global interest that occur during non-instructional time or for short-term educational purposes
- reducing screen time in Grades 7 -12(Board-owned and personal devices) during non-instructional time (i.e., lunch/nutrition break and recess), emphasizing healthy eating habits, promoting physical activity and face-to-face communication during outdoor recess
- protecting the privacy of staff and students' information and helping maintain the security of all LDSB data



- providing communications to student caregivers so they are aware of students' digital citizenship responsibilities on and off school property, and providing resources for caregivers to support students' digital citizenship outside of the school environment

3. Teachers are responsible for:

- the supervision of student use of technology within the teacher's assigned teaching area
- instructing and modelling for students, digital citizenship, and responsibility
- determining when students can access Board technology or personal devices for educational purposes during instructional time
- appropriate, professional use of technology
- protecting the privacy of staff and students' information and helping maintain the security of all LDSB data

4. Students are responsible for:

- using Board technology for curriculum-related/educational purposes only.
- using personally owned technology during instructional/class time only under the classroom teacher's direction for curriculum-related/educational purposes. Use is restricted during instructional/class time to prevent distractions and maximize learning. The only exceptions to this are when a student requires a personal, mobile device for health and/or medical reasons or to support special education needs. Formal documentation from the parent is required for these exceptions.
- respecting restricted use of technology for students in Kindergarten to Grade 6 during designated eating and/or break times as outlined in this



administrative procedure and in schools' codes of conduct

- 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.
- protecting the privacy of staff and students' information and helping maintain the security of all LDSB data

5. Cybersecurity and Network Access

The Board is committed to maintaining safe and secure digital environments in support of teaching, learning, and operational excellence. Users shall access the LDSB network only through Board-approved digital services and devices. The use of unauthorized devices, including but not limited to personal laptops, USB drives, and external storage devices, on internal Board networks is strictly prohibited. Personal devices are permitted on the BYOD network. Internet of Things (IoT) devices must be approved by Information Technology Services (ITS) prior to being connected to the LDSB network.

Remote access via Virtual Private Network (VPN) or Remote Desktop Protocol (RDP) is not permitted unless explicitly authorized by ITS under exceptional circumstances.



6. 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 using 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 disciplinary 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.

7. 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 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 (See Section 5 for approved access expectations)
- 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, but is not limited to, 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.

- Online behaviours, actions, or expressions that discriminate on the basis of race, racial characteristics, culture, age, religion, gender, gender expression, language, disability, sexual orientation, or any other attribute, will not be tolerated as per the Code of Conduct.

8. Consequences for Unacceptable Use

Unacceptable use will be dealt with in accordance with the school's code of conduct and relevant Board administrative procedures. This could result in losing network access privileges, temporarily confiscating devices and/or other disciplinary actions.

Reference:

Education Act, s. 306(1)

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

Digital media: Promoting healthy screen use in school-aged children and adolescents. (2019).

Paediatrics and Child Health, 24(6), 402–408. <https://doi.org/10.1093/pch/pxz095>