

<i>Rainy River District School Board</i>	SECTION 2 <i>Organization & Administration</i>
DIGITAL CITIZENSHIP	2.64

POLICY

The Rainy River District School Board will provide for and monitor effective and appropriate use of technology in its commitment to fostering safe working and learning environments conducive to achievement and well-being.

RATIONALE

The Rainy River District School Board endeavours to prepare students and staff to be successful in an evolving society. Students and staff live and work in a world where people connect through technology. Therefore, it is imperative that the Board provide access to technology for business and educational purposes. It is equally imperative that technology be used safely, appropriately, effectively, and respectfully. All educators are responsible for instructing and modelling digital citizenship and responsibility for students.

IMPLEMENTATION

This Policy applies to:

- 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 or off Board property or when used to access Board resources;
- 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 or by the Board. This includes services provided by the Ministry of Education.

GUIDELINES

1.0 Digital Citizenship

- 1.1 Digital citizenship and responsibility is an expectation in the Board's Code of Conduct and each school's Code of Conduct.
- 1.2 Users will use technology for educational and administrative purposes only. By accessing the Internet while on Rainy River District School Board property or by logging in with a Board login, users accept all terms and conditions of the Board network and Internet use, as

well as the terms outlined in this policy.

1.3 All users are responsible for:

- ensuring that technology is used in accordance with Board policies and procedures;
- complying with the school or employee 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 lawful, responsible and ethical manner consistent with the purposes for which it is provided;
- protecting their personal network login and password - it should not be shared with anyone;
- information stored on their own personal device or with personal online storage systems;
- ensuring that photos, videos or images of an individual/group are not posted online/shared digitally unless consent from the individual(s), if 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.

1.4 The use of personal or Board-owned technology, while on or off school property, that has a negative impact on school climate and student and staff well-being, will result in a full investigation and necessary action will be taken, where appropriate. This includes the use of technology for the purposes of accessing, creating, displaying, storing, and/or sharing

- fraudulent
- harassing
- sexually explicit
- profane
- obscene
- intimidating
- defamatory or
- other inappropriate or unlawful information/materials that negatively impact school climate, student and staff well-being, and/or the Board's reputation.

All individuals who do not comply with this Policy will be subject to appropriate consequences consistent with the appropriate Code of Conduct, progressive discipline, and Safe Schools legislation.

1.5 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 for staff and volunteers, up to and including dismissal;
- appropriate progressive discipline measures within the appropriate Code of Conduct and the Safe Schools Policy;
- legal action and prosecution by the relevant authorities.

2.0 Intended Use

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

2.2 Intended use of technology does not include:

- use that violates federal or provincial laws;
- commercial or political activities;
- union business, unless approved by the Board;
- use that contravenes Board Policies and/or procedures;
- 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 Information Technology Department staff. Purchasing of materials and services must comply with all procurement policies and procedures.

2.3 Internet access will be blocked and/or restricted, as appropriate, for staff and students to prevent access to inappropriate materials.

3.0 Security and Safety of Board Data

3.1 Staff are provided access to data in the course of their employment. Data shall be used for the purposes intended. Other uses of data are strictly prohibited.

3.2 Staff shall take reasonable precautions to ensure Board data is secure and safe at all times.

3.3 Users will not attempt to gain unauthorized access to Board technology or data nor will they attempt to disrupt, steal, distribute or destroy data.

3.4 Users must comply with any security measures implemented by the Board. Users will not attempt to bypass the Board's security.

4.0 Responsible Technology Resource Usage

4.1 The Board's technology resources are shared and limited. Therefore, technology resources must be used efficiently and responsibly.

4.2 The Board reserves the right to limit any activity that consumes a high level of technology resources.

4.3 Personal materials not relevant to educational and administrative purposes will not be stored on Board servers at any time, for any reason.

- 4.4 With respect to information stored for the intended purposes, the Board may impose retention periods for various information classes, either temporarily or permanently.
- 4.5 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.

5.0 Legal Compliance and Adherence to Board Policies

- 5.1 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*) and corresponding procedures. The storage of unlawful materials on Board property is strictly prohibited.
- 5.2 Board resources shall 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.

6.0 Expectation of Privacy

- 6.1 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 will 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.
- 6.2 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.
- 6.3 Use of passwords or account numbers by users does not create a reasonable expectation of privacy and confidentiality of information being maintained or transmitted.
- 6.4 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.
- 6.5 If policy violations are discovered, this will result in an investigation and necessary action will be taken, where appropriate.
- 6.6 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 inappropriate or unlawful materials that impact school climate will result in a full investigation and necessary action will be taken, where appropriate.

7.0 21st Century Learning

- 7.1 Teachers will incorporate technology into their lessons where applicable and relevant.
- 7.2 Educational online resources will be available wirelessly through the Board's networks. When relevant to curriculum and instruction, teachers may 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.

Definitions:

Technology Resources – 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. Shared technology resources include examples such as file storage, network bandwidth, and Internet access.

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 is defined as the norms of responsible behaviour related to the appropriate use of technology.

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.

<u>CROSS REFERENCE</u>	<u>Date Approved</u> December 3, 2013	<u>LEGAL/MINISTRY OF EDUCATION REFERENCE</u>
Policy 4.16 Safe Schools		
Policy 7.22 Emergency Response	<u>Board Motion</u> 397	
Policy 3.02 Progressive Discipline for Employees	<u>Review Prior to</u> 2019	
Policy 3.86 Code of Conduct for Employees		
Policy 2.80 Freedom of Information and Protection of Privacy		
Policy 11.70 Information Security		
Procedure 2.05 Communication		
Procedure 2.62 Unified Information Technology		
Procedure 2.64 Digital Citizenship		