Rainy River District School Board	**SECTION 2** *Organization & Administration*
DIGITAL CITIZENSHIP AND ELECTRONIC MONITORING	**2.64**

POLICY

The Rainy River District School Board will provide for and monitor effective and appropriate use of technology by students and staff to foster safe working and learning environments conducive to student achievement and well-being.

RATIONALE

The Rainy River District School Board prepares students and supports staff to be successful in a world where people connect through evolving technology.

IMPLEMENTATION

As per Procedure 2.64 Digital Citizenship; Procedure 2.62 Unified Information Technology; Procedure 2.82, Information Security; Procedure 2.86 Working Outside the School or Office

GUIDELINES

1.0 General Guidelines

1.1 This Policy applies to:
- the use of all Board-owned technology resources, both on and 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.
- 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.

2.0 Technology Use

2.1 Users will access and employ technology for educational and administrative purposes only. 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.
- using technology in a lawful, responsible, and ethical manner.
- protecting personal network logins and passwords.
- ensuring the care and security of Board-owned devices.
- reporting any inappropriate use of email, data, or unauthorized technology to an educator or administrator immediately.

2.2 Technology resources shall not be used for:
- union business, unless approved by the Board.

- cyberbullying.
- creating, displaying, storing, or sending fraudulent, harassing, sexually explicit, profane, obscene, intimidating, defamatory or otherwise inappropriate or unlawful materials.
- copying, downloading, transferring, renaming, adding, or deleting information protected under copyright law.
- any activities 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.
- unauthorized access, alternation, 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.
- the licensing or downloading of material for which a fee is charged to the Board.

Use must not violate Board Policies and/or procedures, federal or provincial laws and involve commercial or political activities.

3.0 Security and Safety of Board Data

3.1 Data shall be used for the purposes intended. Other uses of data are strictly prohibited.

3.2 Users shall take reasonable precautions to ensure Board data is always secure and safe.

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

3.4 Users must comply with and not gain any authorized access to any security measures implemented by the Board.

4.0 Responsible Resource Usage

4.1 The Board's technology resources must be used efficiently and responsibly.

4.2 The Board reserves the right to limit any activity that may impact the Board services or other users.

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.

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*). The storage of unlawful materials on Board property is strictly prohibited.

5.2 Photos, videos or images of an individual/group are not to be taken, posted online, or 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**.**

6.0 Electronic Monitoring

6.1 Board technology resources and data stored on Board technology are Board property and will be reviewed, monitored, and accessed by authorized individuals, as needed.

All data is 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 Board technology resources, networks, and internet connectivity.

The use of passwords or account numbers should not create a reasonable expectation of privacy and confidentiality of information being maintained or transmitted.

6.3 The Board reserves the right to review, retrieve, read and disclose any data, files, messages or communications that are created, sent, received or stored on the Board's technology resources 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.

Policy violations will be investigated, and appropriate action will be taken.

6.4 Information stored on personally owned devices is the responsibility of the device owner and/or user. However, personally owned devices used for creating, displaying, storing, or sending inappropriate or unlawful materials that impact school climate will be investigated, and appropriate action will be taken.

7.0 Digital Citizenship

7.1 Digital citizenship is an important part of the work within classrooms and schools across the Board and is reflected in the Ontario curriculum. Students must learn to use technology effectively, responsibly and respectfully as digital resources will be incorporated into their learning.

7.2 Educators may permit the use of personal mobile devices

- for educational purposes,
- for health and medical purposes as outlined in a Plan of Care, and
- in support of special education needs.

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

8.0 Policy Violations and Appropriate Actions

8.1 All users who do not comply with this policy will be subject to appropriate actions, which may include, but are not limited to the following:

- 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 employee disciplinary measures (staff), up to and including dismissal;
- Appropriate student progressive discipline measures within the School Code of Conduct and the Safe Schools Policy; and
- Legal action and prosecution by the relevant authorities.

Definitions:

Technology Resources – Technology resources include, but are not limited to, computers, phones, cellular/mobile technology, servers, networks, Internet services, computer applications, email and collaboration tools, as well as third-party Internet services provided to the Board. Examples of third-party web services include online textbook providers. Shared technology resources include examples such as file storage, network bandwidth, and Internet access.

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.

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 behavior related to the appropriate use of technology.

Personal Mobile Device refers to any personal electronic device that can be used to communicate or to access the Internet, such as a cellphone or a tablet.

CROSS-REFERENCE	Date Approved	LEGAL/MINISTRY OF EDUCATION REFERENCE
Policies: ▪ 2.20 Information Security ▪ 2.80 Freedom of Information and Protection of Privacy ▪ 3.02 Progressive Discipline for Employees ▪ 3.86 Code of Conduct for Employees ▪ 4.16 Safe Schools Procedures: ▪ 2.62 Unified Information Technology	2022 11 01 Board Motion 310 Review 2027	*Freedom of Information and Protection of Privacy Act* *Personal Health Information Protection Act* *Education Act, Part XIII* *Copyright Modernization Act* Ministry of Education Policy/Program Memorandum 128, The Provincial Code of Conduct Bill 88, *Working for Workers Act 2022*