POLICY:	ELECTRONIC MONITORING OF EMPLOYEES	#	835
SECTION:	800 : Personnel and Employee Matters	Page	1 of 2
APPROVAL/REVISION DATE:	November 7, 2022	EFFECTIVE DATE:	November 8, 2022
REVIEW DATE:	November 8, 2027		

CROSS REFERENCE:
Employment Standards Act, 2000
Municipal Freedom of Information and Protection of Privacy ACT (MFIPPA)
Working for Workers Act, 2021
Policy 821 - Board Personnel Code of Conduct
Policy 827 - Attendance Support Program
Policy 831 - Progressive Discipline

A: STATEMENT OF PURPOSE

1.1 Thunder Bay Catholic District TBCDSB (TBCDSB) understands the importance of technological innovation and that any adoption or use of technology must be done in keeping with its values of cooperation and respect.

1.2 The purpose of this Electronic Monitoring Policy (the "Policy") is to ensure that TBCDSB's employees are aware of when and why the TBCDSB may engage in workplace electronic monitoring.

1.3 This policy seeks to meet the requirements put in place by recent legislative amendments. Nothing in this policy shall be interpreted to create any greater right or benefit than what is available under existing legislation or to restrict any of the TBCDSB's legal rights.

B: SCOPE

2.1 This policy applies to all employees of the TBCDSB, including temporary employees, trustees, contractors and other third parties who may have access to the Board's IT resources and communication systems.

C: DEFINITIONS

3.1 Electronic Monitoring is the TBCDSB's collection of information about an employee's activities through TBCDSB owned electronic devices and systems such as computers, computer networks, telephones, cell phones, software and GPS units . It may also include the monitoring of voicemail, email, text messaging, instant messaging and internet use.

3.2 Monitoring may include, without limitation, the interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of messages, communications, postings, logins, logs, recordings and other uses of IT and communication systems, including installation, removal or alteration of software or hardware and may also include keystroke capturing.

D: PRIVACY EXPECTATIONS

4.1 Employees should have no expectation of privacy in any content created, transmitted, received, accessed or stored on the TBCDSB's IT and communication systems. Employees should not use the TBCDSB's IT and communication systems for any matter that the employee wants to be kept private or confidential from the TBCDSB.

4.2 Employees are strongly encouraged to use personal devices to conduct personal business, since it may be difficult for the TBCDSB to distinguish between personal business and School Board business when conducting electronic monitoring or reviewing stored information.

4.3 Although employees should have no expectation of privacy in the use of the TBCDSB's IT and communication systems, any employee personal information collected in the process of monitoring will be used or disclosed only as required to the protect the TBCDSB's business interests or to meet its legal obligations.

POLICY:	ELECTRONIC MONITORING OF EMPLOYEES			#	835
SECTION:	800 : Personnel and Employee Matters		Page 2	of	2
APPROVAL/REVISION DATE:	November 7, 2022	EFFECTIVE DATE: November 8, 2022		REVIEW DATE:	November 8, 2027

CROSS REFERENCE:	Employment Standards Act, 2000 Municipal Freedom of Information and Protection of Privacy ACT (MFIPPA) Working for Workers Act, 2021 Policy 821 - Board Personnel Code of Conduct Policy 827 - Attendance Support Program Policy 831 - Progressive Discipline

E: POLICY

5.1 The TBCDSB regularly uses electronic monitoring as reasonably required to protect its business interests and fulfill applicable legal requirements, including, without limitation:

- Protecting the integrity of TBCDSB IT (for example, against computer viruses, damage to software or hardware, loss of TBCDSB or third-party documents or information, excessive telephone or computer usage for non-work purposes);
- Protecting against unauthorized access or disclosure of TBCDSB or third-party confidential information, proprietary information or employee personal information;
- Protecting against cyber risks through the safeguarding of the TBCDSB's technology assets and associated information;
- Regular or special maintenance of TBCDSB IT or devices;
- Providing network and device management and support;
- Locating lost messages or data or retrieving messages or data after technological or systems failure;
- Monitoring the use of email, text messaging and instant messaging and telephone systems to ensure that use is in accordance with the TBCDSB's policies;
- Following up on unresolved matters after the departure of an employee;
- When the TBCDSB has a business related need to access TBCDSB owned technology (for example, when the employee is absent from work or otherwise unavailable);
- Protecting employees against discrimination, harassment, or violent behaviour;
- Monitoring and preventing risks to health and safety;
- Monitoring the use of TBCDSB IT to ensure that use is in accordance with TBCDSB policies and applicable law;
- Assisting in investigations of alleged or potential wrongdoing (including alleged violations of TBCDSB policies);
- Monitoring productivity and time keeping;
- Investigating and responding to legal claims or demands; or
- Complying with any other legal requirement.

5.2 To achieve these purposes, the TBCDSB may use electronic monitoring with respect to any information created on, transmitted to, received or printed from, or stored or recorded on School Board IT and/or applicable service providers.

5.3 The TBCDSB may store copies of information acquired through electronic monitoring and may delete such copies from time to time without notice.

5.4 The TBCDSB may, in its discretion, use information obtained through electronic monitoring to determine if there has been a violation of its policies. Where appropriate, such information may lead to disciplinary action, up to and including termination of employment, including for cause.

F: POLICY ADMINISTRATION

6.1 The TBCDSB will maintain and revise this Policy as required to ensure it reflects current monitoring practices.