ADMINISTRATIVE PROCEDURE PERSONNEL AND STAFF	
Effective:	October 11, 2022
Last Revised:	September 15, 2023

Protection of Digital Security and Communication

1. PURPOSE

Employers with more than 25 employees in Ontario are required to have an administrative procedure in place with respect to monitoring for the Protection of Digital Security and Communication

Rainbow District School Board is required by the Ministry of Labour and the Employment Standards Act to advise how they actively manage digital communication, information and protection systems to:

a) Ensure the safety of staff, students, intellectual property, and business process technology, safeguarding them from any potential harm or threats.

b) Maintain a safe and secure environment for our facilities and property, preventing unauthorized access or any form of damage.

c) Implement measures to safeguard electronic resources, preventing unauthorized access or breaches of security.

d) Protect against any potential loss, theft, or vandalism to ensure the integrity of our resources.

e) Prevent the misuse of board resources for inappropriate activities, as defined by the Administrative Procedure "Acceptable Use of Information and Communication Technologies."

2. DEFINITIONS

Routine Management:

The Board routinely monitors its electronic systems using electronic tools. If an electronic tool indicates a concern, authorized personnel may access employee files, documents, or electronic communications to ensure system integrity in accordance with Board policies and procedures.

Demand Management:

The Board may access data or traffic on its electronic systems, whether on Board-owned technology or traffic from personal devices, when using Board-provided digital identities. Strict approvals from authorized personnel are required for demand management situations to comply with legislative, legal, business, and maintenance requirements.

3. APPLICATION

This administrative procedure applies to all employees of the Rainbow District School Board. This procedure aims to clarify the purpose and scope of the document for better understanding.

4. ACTIVITIES

Video Protection Systems

- Purpose: Facility Security and Safety.
- Tools: Cameras and video facility surveillance and storage systems.
- How: Cameras record digital video footage of specific areas within Rainbow District School Board facilities.
- Circumstances: Continuous. Examination on demand for the purpose of safety or investigation.

Web Traffic Filtering - All Internet Protocol (IP) based Communications

- Purpose: Protection from unauthorized access or breaches of security.
- Tools: Firewalls, Secure Access Service Edge (SASE) software, EDR/XDR software.
- How: Scans of all inbound and outbound network traffic for malware signatures, anomalies and indicators of compromise.
- Circumstance: Continuous. Traffic is subject to decryption and automated evaluation to determine risk and inappropriate use. Connections that are evaluated to be violations are blocked.

Email Filtering - All Google Workspace Messaging Systems

- Purpose: Detecting SPAM and other external threats to the network.
- Tools: Gmail email service, Chat messaging.
- How: Automated detection through Google's built-in filters.
- Circumstance: Continuous. Monitoring for SPAM and malicious content.

Device Management - Asset Protection

- Purpose: Remote configuration management of all Board-owned devices.
- Tools: Mobile Device Management (Meraki, Mosyle) and Asset Management (K Box).
- How: Automated device reporting to verify location, review of device properties, installed software, device updates and license entitlements.
- Circumstance: Continuous. Daily maintenance for device inventory.

GPS Vehicle Geolocating

- Purpose: Location services for Board-owned vehicles.
- Tools: GPS, Geofencing (Geotab Software).
- How: Automated alerts based on geofencing restrictions.
- Circumstance: Examination on demand in the event of theft, accident or any incident involving a Board-owned vehicle.

Building Access Controls

- Purpose: Prevent unauthorized access to Board facilities, ensuring safety and security for staff and students.
- Tools: Controlled door entry systems through Building Access Controller System.
- How: A digital log of each time an authorized user accesses a Board facility with the access card they have been provided.
- Circumstance: Continuous. Examination on demand for the purpose of safety or investigation.

5. COMPLIANCE

- To comply with legislative disclosure or access requirements under the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and the Personal Health Information and Protection of Privacy Act (PHIPA) to assist with the investigation and resolution of a privacy breach. (Requested by the Senior Advisor of Corporate Communications / Information and Privacy Officer, and approved by the Director of Education).
- To maintain electronic information systems on Board owned technology, including regular and special maintenance. (Requested by authorized staff in Information Services and approved by the Manager of Information Services).
- To comply with a business-related need to access an employee's Board owned technology, including, for example, when the employee is absent from work or otherwise unavailable. (Requested by a Supervisor and approved by the Manager of Information Services).
- To comply with obligations to disclose relevant information in the course of a legal matter. (Requested by the Manager of Human Resources or Supervisory Officer and approved by the Director of Education or Superintendent of Business).
- To investigate a possible violation of the Code of Conduct, Board Policy, or an administrative legal and/or disciplinary matter if the Board has reason to believe such action is warranted. (Requested by the Manager or Assistant Manager of Human Resources and approved by a member of the Executive Council)."

REFERENCE DOCUMENTS

Legal:
Ontario Employment Standards Act, 2000, S.O. 2000, C. 41
Ontario Occupational Health and Safety Act, R.S.O. 1990, c. 0.1

Board References:
Board Policy No. GOV-01 Board Vision, Mission, and Values
Administrative Procedure: Acceptable Use of Information and Communication Technologies
Video Security Surveillance (2013)
Network Security Plan