Halton District School Board

Electronic Monitoring

Administrative Procedure

Status:	**Active**
Effective:	October 2022
Revision Date:	September 2025
Review Date:	September 2029
Responsibility:	Superintendent of Information Services Superintendent of Human Resources

INTENDED PURPOSE:

The Halton District School Board (HDSB) is committed to transparency with respect to automated electronic monitoring. This administrative procedure explains how and when the HDSB may electronically monitor HDSB technology, networks and other infrastructure, and how any information collected may be used by the HDSB. This administrative procedure is in alignment and support of the Cyber Security and Data Protection Administrative Procedure.

Part XI.1 of the *Employment Standards Act (ESA)* requires employers to inform employees whether the employer electronically monitors employees. If the employer does, the policy must contain a description of how, and in what circumstances, the employer may electronically monitor employees and must set out the purposes for which the information obtained through electronic monitoring may be used by the employer.

DEFINITIONS

a. **Electronic Communication and Information Systems:** Corporate network, email system, file storage, learning management systems, collaboration systems, social media and other applications, software and hardware tools used for business and learning.

b. Electronic Monitoring: Includes all forms of monitoring that is done electronically, generally through automated means.

c. **Employee:** Employees of the HDSB as defined by the Ontario *Employment Standards Act, 2000.* In addition, this procedure also applies to trustees where access to board facilities, infrastructure or devices is available.
d. **Endpoint:** Any device connected to a network, such as a laptop, desktop or mobile device.
e. **Endpoint Detection and Response (EDR):** A type of security technology designed to detect, identify and address security threats at the endpoint level, continuously monitoring endpoint activities and analyzing data to detect potential threats in real time.
f. **Extended Detection and Response (XDR):** A security solution that integrates data from multiple sources (endpoints, networks, servers, etc.) to detect, investigate and respond to potential threats in real time. It helps identify security threats faster and limits the impact by providing comprehensive visibility into what has occurred and automatically taking action to protect the system.
g. **Information and Information Technology (I&IT):** Resources that include but are not limited to board information, board devices (including but not limited to phones, laptops, tablets and networked printers), HDSB servers, other HDSB infrastructure and applications and contracted cloud services and applications.
h. **Intrusion Detection System (IDS):** A tool designed to detect suspicious activity such as unauthorized access or abnormal behaviour within the network or system.
i. **Intrusion Prevention System (IPS):** A real-time tool designed to prevent malicious activity from affecting the network by analyzing incoming and outgoing data (traffic) and looking for patterns or anomalies and automatically taking action to block or reject suspicious traffic.
j. **Managed Detection and Response (MDR):** A cyber security service that combines technology, including artificial intelligence (AI), with human expertise to rapidly identify and limit the impact of threats by performing threat hunting, monitoring and response.
k. **Managed Security Services (MSS):** The proactive outsourcing of cyber security monitoring and management to specialized providers, called a Managed Security Service Provider (MSSP). These providers leverage

advanced technologies and security expertise to safeguard HDSB infrastructure and sensitive data against evolving cyber threats. Services include a comprehensive range of security functions including threat detection and response, vulnerability management, security information and event management (SIEM) and compliance monitoring. This enables the HDSB to maintain a robust security posture while optimizing internal resources.

l. **Mobile Threat Defence (MTD):** A security solution that protects mobile devices such as smartphones, laptops and tablets from threats such as malware, phishing, network attacks and data breaches. It ensures device, app and data security through real-time monitoring and risk mitigation, network security, app scanning and device hardening.

m. **Network Access Controls (NAC):** A security solution that controls who and what can access a network by checking devices trying to connect and making sure they meet security standards before allowing access, thereby ensuring only trusted devices and users can access sensitive network resources.

n. **Operational Technology (OT):** Resources include network infrastructure (e.g., access points, switches, routers) and building facilities automation equipment which are increasingly internet connected (e.g. Industrial Internet of Things (IIoT) or Internet of Things (IoT), building sensors, key scan cards and HVAC systems).

o. **Packet Sniffing:** A technique used to monitor network packets (data moving through a network) to assist network troubleshooting, performance monitoring and security analysis. It only examines basic information about the data being sent (metadata) and may not inspect the actual content of packets.

p. **Privileged Account Management (PAM):** A category of cyber security solutions that enables security and IT teams to securely manage access for all privileged identities in an enterprise environment.

q. **Secure Access Service Edge (SASE):** A cloud-based security framework that combines networking and security functions, such as firewalls and access controls, into a single platform to ensure secure access based on user identity and device and eliminating the need for traditional VPNs.

r. **Security Information and Event Management (SIEM):** A system that monitors, collects and analyzes data from various sources within an organization's network, such as servers, firewalls and other devices, helping to detect potential security threats by leveraging AI and identifying unusual activity and generating alerts.
s. **Security Orchestration, Automation and Response (SOAR):** A set of tools and services that help automate and streamline the response to cybersecurity incidents, combining three key components: orchestration (coordinating various security tools and processes), automation (automating repetitive tasks) and response (managing and responding to security incidents).
t. **User and Entity Behaviour Analytics (UEBA):** A cyber security approach that leverages machine learning and artificial intelligence to analyze user and entity behaviour patterns. UEBA identifies anomalies that might indicate a potential threat, such as a data breach or insider threat. UEBA is built into advanced cyber security tools including but not limited to EDR, XDR, SIEM and SOAR.

GUIDING PRINCIPLES:

a. The HDSB is committed to adopting CIS Critical Controls (CIS Controls) adhering to the requirements of the provincial Cyber Security Wellness Architecture (CSWA) and meeting the standards set out in the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 Core and Reference Architecture (RA) 3.0.
b. The HDSB shall ensure that appropriate technical and administrative safeguards are implemented to secure HDSB I&IT and network-connected OT resources. Technology resources and data stored on board technology remain the property of the HDSB and will be reviewed, monitored and accessed as necessary by authorized individuals to maintain data security.
c. Employees should be aware that HDSB technology, networks and other infrastructure are monitored to maintain security and privacy when using these tools should not be expected.
d. In an effort to ensure the security of data and records, when required the HDSB reserves the right to review, retrieve, read and disclose any data, file, messages or communications that are created, sent, received or stored on

the board's technology resources for the purposes of ensuring the security of data and records.

e. The HDSB routinely monitors electronic systems and may monitor and access files, documents, electronic communications and the use of network infrastructure to:

i. ensure compliance with the requirements of HDSB administrative procedures (APs) including but not limited to the Cyber Security and Data Protection AP, the Staff Responsible Use of ICT AP, the Student Responsible Use of ICT AP and the Board Assigned Mobile Cellular Device AP;

ii. ensure the safety and security of HDSB students and staff;

iii. provide safeguards against vandalism, theft, damage, and/or loss of property;

iv. protect HDSB buildings from unauthorized access;

v. facilitate regular or special maintenance of and/or upgrades to electronic information and communication systems;

vi. comply with disclosure requests or orders issued to fulfill legal requirements for sharing information, including those made under the authority of the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), the *Personal Health Information Protection Act* (PHIPA) and other relevant legislation;

vii. comply with obligations to disclose relevant information in the course of a legal proceeding; and/or

viii. monitor the use of electronic communication and information systems.

f. With proper authorization in accordance with the Information Services Investigation Standards & Protocols, Information Services may review employee usage of board technology and/or leverage Electronic Communication and Information Systems only under the following circumstances:

i. to ensure appropriate use of HDSB technology resources including I&IT and OT;

ii. to comply with the requirements of HDSB administrative procedures (APs) including but not limited to the Cyber Security and Data Protection AP, the Staff Responsible Use of ICT AP, the Student Responsible Use of ICT AP and the Board Assigned Mobile Cellular Device AP;

iii. when the board has a business-related need to access an employee's board provided device and/or account (e.g., when the employee is absent from work or otherwise unavailable);
iv. to facilitate regular or special maintenance of and/or upgrades to electronic information and communication systems; and/or
v. to assist with the investigation of a privacy breach and/or cyber incident.

g. The Human Resources Department may authorize access to employee usage of board technology and/or leverage Electronic Communication and Information Systems in accordance with HR investigation standards when there is a reason, as determined by the Superintendent of Human Resources, to believe there has been staff misconduct, a violation of policy, or when an administrative, legal and/or disciplinary investigation is underway. Inquiries of this nature will include the Human Resources Department and follow applicable practices and procedures such as Progressive Discipline, Workplace Investigations and Respectful Workplaces Free of Discrimination and Harassment and be conducted in accordance with the Information Services Investigation Standards & Protocols.

SCOPE

This procedure applies to all employees of the HDSB when using the board's I&IT, OT and services regardless of location.

PROCEDURES:

The following tables provide a non-exhaustive list of electronic monitoring technologies used by the HDSB. The HDSB reserves the right to modify this list without further notice as available technologies change and cyber security and data protection continue to evolve. These tables should be considered dynamic and will be updated regularly.

Halton District School Board

Electronic Monitoring

Administrative Procedure

1. Facility Safety and Security

Tool	When	How	Purpose
Electronic Key System	Each scan	Electronic sensors create a record each time an authorized user scans their card key and enters HDSB premises.	Facility Safety and Security Workplace Investigations
Video Surveillance	Continuous or motion activated	Video cameras in schools and other work locations to provide security footage, protection from vandalism, etc.	Facility Safety and Security Workplace Investigations

2. Device Management

Tool	When	How	Purpose
Device Management (iPads, board cell phones)	Continuous	Secures employee mobile devices and uses geofencing to ensure security measures when devices move outside Canada.	Data Protection Cyber Security
Device Management (Chromebooks)	Continuous	Allows the HDSB to manage, configure and monitor Chromebooks. Geofencing may be used to ensure security measures are in place if the device travels outside Canada.	Data Protection Cyber Security
Device Management (Laptops, Desktops)	Continuous	Using an endpoint security tool & management console to manage, configure and monitor devices. May include geofencing to ensure security measures are in place for travel outside Canada.	Data Protection Cyber Security
HDSB Supported Applications	Continuous	Through network management and monitoring tools, Software and Technology Catalogue reviews	Network Security Data Protection Cyber Security

		(technical, security, privacy) and an approval process for all digital platforms. Includes geofencing of some applications.	
Phone Logs	Continuous	Monitors call quality (e.g., bandwidth, latency, jitter, packet loss, compression), call volume and voicemail storage.	Data Protection
Endpoint Detection and Response (EDR)	Continuous	Identifies and remediates security threats at the endpoint level (such as laptops, desktops and mobile devices). Continuously monitors and analyzes endpoint activities, behaviour, connections and data to detect potential threats in real time.	Network Security Data Protection Cyber Security
Mobile Threat Defence (MTD)	Continuous	Protects mobile devices from threats like malware, phishing and network attacks. It ensures device, app and data security through real-time monitoring and risk mitigation.	Network Security Data Protection Cyber Security

3. Integrated Cyber Security Management Systems

Tool	When	How	Purpose
Account Authentication (Login / Logout Procedures) *	Upon login / logout	Records when employees sign in to online platforms for work purposes*	Network Security Data Protection Cyber Security Workplace Investigations

Network Access Controls (NAC)	Upon login / logout	Authenticates devices to ensure they are trusted and meet security standards before allowing access to sensitive network resources	Network Security Data Protection Cyber Security
Google Workspace for Education Archiving	Continuous	Retains in Vault copies of all messages, including Chat and Gmail, sent or received by addresses within the HDSB domain.	Network Security Data Protection Cyber Security Workplace Investigations
Data Loss Prevention (DLP)	Continuous	Detects, prevents, and responds to the unauthorized transmission, sharing, or exposure of sensitive data. DLP solutions help organizations protect data from accidental leaks, insider threats and cyber attacks by enforcing security policies and monitoring data in use, in motion, and at rest.	Data Protection Cyber Security
Data and Document Sensitivity Classification	Continuous	Process of categorizing data and documents based on their level of sensitivity and importance, such as public, confidential or highly sensitive, which then correlates to the appropriate handling, access control and protection measures put in place to protect each classification level.	Data Protection

Privileged Account Management (PAM)	User accounts with elevated privileges	Controls and monitors access to critical systems and sensitive data by managing privileged accounts. It minimizes the risk of misuse, unauthorized access or breaches by enforcing strict access controls and session monitoring.	Network Security Data Protection Cyber Security
Internet / Web Filtering	Continuous	Using firewalls and Fortigates.	Network Security Data Protection Cyber Security
Network Monitoring / Network Traffic Analysis	Continuous	Through packet sniffing, troubleshooting or detecting security threats. Identifies issues or unauthorized activities by analyzing the content and flow of network traffic.	Network Security Data Protection Cyber Security
Intrusion Detection System (IDS)	Continuous	Monitors network traffic and host activity logs to detect suspicious activity or intrusions and generate alerts.	Network Security Data Protection Cyber Security
Intrusion Prevention System (IPS)	Continuous	Monitors data in real time and takes action to block or drop packets, connections or IP addresses.	Network Security Data Protection Cyber Security
Extended Detection and Response (XDR)	Continuous	Monitors for abnormalities across multiple layers and systems (e.g., network performance, endpoints, servers, etc.). Rapidly identifies and limits the impact of	Network Security Data Protection Cyber Security

		threats by performing threat hunting, monitoring and response.	
Managed Detection and Response (MDR)	Continuous	Provides continuous monitoring, threat detection, and rapid response to mitigate cyber risks, leveraging advanced tools, AI and expert analysts. It detects and addresses threats before they cause significant damage by performing threat hunting, monitoring and response.	Network Security Data Protection Cyber Security
Security Information and Event Management (SIEM)	Continuous	Recognizes and remediates potential security threats and vulnerabilities. Collects, analyzes and correlates security data from various sources, such as firewalls, intrusion detection systems and servers. Identifies potential security threats, tracks security incidents, leverages AI and provides insights for incident response.	Network Security Data Protection Cyber Security
Security Orchestration, Automation and Response (SOAR)	Continuous	Automates repetitive security tasks, integrates with existing tools and orchestrates security workflows. Speeds up incident response time, reduces human error and improves overall security efficiency.	Network Security Data Protection Cyber Security

Secure Access Service Edge (SASE)	Continuous	Combines networking and security functions together into a single, cloud-based platform ensuring access based on the identity of users and devices rather than relying only on network perimeter security and, therefore, removing need for traditional Virtual Private Networks (VPNs). A key element of SASE is an environment of Zero Trust.	Network Security Data Protection Cyber Security
User & Entity Behaviour Analytics (UEBA)	Continuous	Leverages AI (machine learning, behavioural analytics, and algorithms) to analyze user and entity behaviour patterns and deviations from normal activity, identifying anomalies that might indicate a potential threat such as a data breach, compromised account or insider risk. Embedded in many advanced cyber and network security tools and is a core function of SIEM, SOAR, EDR and XDR.	Network Security Data Protection Cyber Security
Managed Security Services (MSS)	Continuous	External security support to leverage advanced technologies and security expertise. Includes threat detection and response, compliance monitoring, vulnerability scanning, firewall management, log monitoring,	Network Security Data Protection Cyber Security

		security information and event management (SIEM) and basic incident response.	

To ensure HDSB employees of a reasonable degree of privacy, the HDSB prohibits the following:

- Keylogging (recording individual keystrokes)
- Video monitoring in washrooms and/or changerooms
- Use of external camera devices to record computer activity
- Data stored by the use of the Microsoft Authenticator app for the purpose of authentication

Information shared with Microsoft for authentication purposes via the Microsoft Authenticator app is neither shared with nor recorded by the HDSB.

ELECTRONIC MONITORING ASSURANCE: MONITORING, ASSESSING AND AUDITING

Monitoring and assessments including but not limited to cyber risk assessments, vulnerability assessments, audits and other industry established practices may be conducted centrally across the organization or locally at specific sites or with specific user or staff groups as approved by the Superintendent of Information Services in consultation with the Manager of Cyber Security and Data Protection.

Halton District School Board

Electronic Monitoring

Administrative Procedure

Cross-Reference:

Legislation

Employment Standards Act, 2000, S.O. 2000, c. 41
Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), R.S.O. 1990, c. M. 56
Personal Health Information Protection Act (PHIPA), 2004, S.O. 2004, c. 3, Sched. A
Criminal Code of Canada

Ministry Policy & Program Memoranda and Other Policies

Ministry of Education Community Services I&IT Cluster & Ministry of Public and Business Service Delivery and Procurement K-12 Cyber Protection Strategy (CPS)
Ministry of Education Community Services I&IT Cluster & Ministry of Public and Business Service Delivery and Procurement Cyber Security Wellness Architecture (CSWA)

Board Policies, Procedures & Protocols

Board Assigned Mobile Cellular Device Administrative Procedure
Code of Ethics Administrative Procedure
Cyber Security and Data Protection Policy
Cyber Security and Data Protection Administrative Procedure
Responsible Use Procedures for Information and Communication Technology (ICT) Administrative Procedure
Positive School Climate Administrative Procedure
Privacy Breach Protocol Administrative Procedure
Privacy Statement for Employees
Progressive Discipline Administrative Procedure
Respectful Workplaces Free of Workplace Harassment
Social Media and Electronic Use for Staff Administrative Procedure
Video Surveillance Administrative Procedure
Workplace Investigations Process Administrative Procedure

Halton District School Board

Electronic Monitoring

Administrative Procedure

Industry Standards

Guide to the NIST Cybersecurity Framework: A K-12 Perspective
National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 Core
NIST Special Publication 800-63
Reference Architecture (RA) 3.0

Revision History

- September 2025 - Comprehensive: updated to align with Cyber Security and Data Protection Administrative Procedure, Board Assigned Mobile Cellular Device, and the Responsible Use Procedures for ICT administrative procedures