

Network Access and Electronic Monitoring

Adopted under the Privacy Policy

1.0 Objective

- 1.1 This procedure is adopted under the DDSB's Privacy Policy to provide transparency as to Electronic Monitoring of employees in the workplace, in accordance with recent amendments to the *Employment Standards Act, 2000*.
- 1.2 This procedure summarizes Electronic Monitoring of employees that occurs as of this procedure's effective date, which includes any amendments to this procedure. Please refer to the applicable DDSB policy or procedure for details relating to specific forms of Electronic Monitoring (sections 5.1 and 5.2 of this procedure).
- 1.3 This procedure does not impact current employee privacy rights with respect to Electronic Monitoring, establish a right for employees not to be electronically monitored by the DDSB, create any new privacy rights for employees, or affect or limit the DDSB's ability to use information obtained through the Electronic Monitoring in accordance with the DDSB's policies and procedures and applicable legislation or regulation (including the DDSB's obligations to protect and retain Personal Information collected for monitoring purposes).
- 1.4 This procedure is to be interpreted and applied in accordance with the DDSB's commitment to promoting and upholding Indigenous rights and human rights in all its learning and working environments. This includes anti-colonial, anti-discriminatory and anti-racist approaches and actions to provide services and employment that are safe, welcoming, respectful, inclusive, equitable, accessible and free from discrimination and harassment consistent with the DDSB's Indigenous Education Policy, Human Rights, Anti-Discrimination and Anti-Racism Policy (the "Human Rights Policy"), Safe and Respectful Workplace Harassment Prevention Policy, and related procedures.

2.0 Definitions

In this procedure,

- 2.1 "Cloud Services" means a specific service offering computing, networking, application, or storage function made available to users on demand via the Internet from a cloud service provider as opposed to being provided from an organization's own on-premise servers and equipment.
- 2.2 "Electronic Monitoring" means all forms of employee monitoring that is done electronically.
- 2.3 "Network" means the hardware, software, and services (including Cloud Services) that the DDSB provides to employees, vendors, contractors and volunteers so they can perform work for the DDSB, as well as to other users connecting to the DDSB guest Network.

- 2.4 “Personal Information” means information about an identifiable or potentially identifiable individual as defined in the Municipal Freedom of Information and Protection of Privacy Act and includes, but is not limited to, personal health information and opinions about the individual.

3.0 Access to Network

- 3.1 The DDSB provides use of the Network to employees to enable the DDSB to fulfill its statutory mandate. The DDSB has access to user accounts and information for certain legitimate purposes, which may include (but are not limited to):
- Performing routine and non-invasive Network maintenance and repair (e.g., troubleshooting network performance issues);
 - Investigating Network misuse and employee misconduct where reasonable cause arises;
 - Proactively monitoring and auditing for Network misuse (e.g., suspicious user account activity, such as multiple concurrent logins from different locations that signals that a user account may be compromised);
 - Complying with a legal obligation;
 - Supporting work continuity; and
 - Data analysis to support compliance with DDSB policies and procedures and applicable laws.
- 3.2 The DDSB provides use of the Network to employees for professional purposes. The DDSB recognizes that there may be times when employees use the Network for personal purposes during the business day when on breaks. There is no expectation of privacy given the Network’s purposes. If employees require privacy, they need to use a personal device that is not connected to the Network. Use of the Network can be tracked to the individual signed in.

4.0 Electronic Monitoring

- 4.1 The DDSB may use the following Electronic Monitoring tools for the purposes of safety, user support, system administration and security, and compliance with DDSB policies and applicable laws:

Tool or Tool Class	Circumstances	How	Purpose
Web filtering	All internet traffic on DDSB issued laptops/computers, cellular devices and tablets connected to the Network	Firewalls	Protect from harmful and inappropriate content
E-Mail filtering	All DDSB e-mail traffic	E-mail filtering appliance	Protect from harmful content
Account Authentication	Staff login to services (e.g., account log off, log on, general location based on IP, etc.)	Active Directory, G-suite, Azure AD, standalone applications	To protect against unauthorized access

Tool or Tool Class	Circumstances	How	Purpose
Device Management (iPad/iPhone)	All Board iPads/iPhones	Mobile Device Management (IP address, hardware address, serial number, applications installed)	Protect against loss/theft, and enforce security settings
Device Management	All Board Chromebooks and Chrome Browser	Google Management Console (IP address, hardware address, model number, serial number, logon times, browser extensions installed, location based on Domain Name System entry and public IP address)	Protect against loss/theft, and enforce security settings
Video surveillance (external or public areas only)	Some schools and administrative buildings	Video surveillance cameras and recording systems	Safety, theft, illegal activity, behavioral/incident review
GPS Solution to track vehicles	In Board-owned vehicles	GPS tracking system and associated software	Protect against loss and theft. Staff safety in case of breakdown.
Door Fobs	All DDSB buildings	Door access activity through door FOB system	Control, log and monitor access to buildings
Security Information and Event Management	Suspicious activity (e.g., unusual user account activity, malware, unusual network traffic, etc.)	AD, Fortinet network appliance, External threat feeds, Google G-Suite, O365	Protect from threats and perform security investigations
Computer Application Logs	User Session Activities	Applications store the time stamps of login and IP address of users, etc.	Built into applications for security
Communication data	User activities	Communication data stored through various applications, including email, chat and messaging applications, etc.	Perform security investigations, system administration and user support

- 4.2 The DDSB collects the information in Section 4.1 routinely. DDSB does not access and analyze this information routinely but may authorize limited specific individuals to access this information only as appropriate, such as when investigating Network misuse and employee misconduct where reasonable cause arises and shall be in accordance with legal requirements as to privacy and only as permitted by law and in accordance with DDSB policies and procedures.
- 4.3 The DDSB reserves the right to employ special monitoring tools or change settings of existing monitoring tools as part of a reasonable investigation into potential breaches of DDSB's policies and/or procedures (including but not limited to, threats to employee safety and employee misconduct) and where necessary in the circumstances. These monitoring tools would be employed in accordance with applicable law, including privacy and human rights laws.
- 4.4 Electronic Monitoring applies equally where the employee works from home, on DDSB premises or other location where the employee performs work for the DDSB, or under a hybrid "workplace/home" model.
- 4.5 Any Personal Information about employees collected through Electronic Monitoring will be collected, used and disclosed only for the purposes described in the DDSB's policies and procedures and the applicable legislation, and will be subject to security, retention and access as described in the DDSB's policies and procedures and applicable legislation or regulation.
- 4.6 Information Technology Services and Legal Services are jointly responsible for the administration of this procedure. If employees have any questions regarding this procedure or any questions about Electronic Monitoring that are not addressed in the applicable DDSB policy or procedure, they may email: generaladvice.legal@ddsb.ca.
- 4.7 The DDSB expressly reserves the right to change, modify or delete portions of this procedure without notice. Any changes shall only be effective once the revised procedure is posted to the DDSB website.

5.0 Reference Documents

5.1 DDSB Policies

[Personnel – Privacy](#)

5.2 DDSB Procedures

[Personnel – Privacy](#)

[Acceptable and Safe Use Procedure for Computing Technology Safety](#)

[Guidelines for E-Mail](#)

[Staff Mobile Phones](#)

[Video Surveillance System](#)

5.3 Other Documents

[Working for Workers Act, 2022, S.O. 2022, c. 7 - Bill 88](#)

[Employment Standards Act, 2000, S.O. 2000, c. 41](#)

[Education Act, R.S.O. 1990, c. E.2](#)

[Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M.56](#)

[Personal Health Information Protection Act, S.O. 2004, c. 3, Sched. A](#)

[Human Rights Code, R.S.O. 1990, c. H.19](#)

Appendix:
None

Effective Date
2022-10-11

Amended