Corporate Policy Manual

Policy Name	Policy Number	Responsible Department
Electronic Monitoring Policy	CPM-06-02	Information Technology
Approval Body	**Approval Date**	**Review Date**
Chief Executive Officer	October 11, 2022	October 11, 2025

Purpose

Niagara Parks (the “NPC”) is committed to maintaining a transparent and fair workplace. Through this Electronic Monitoring Policy NPC will communicate the company’s intent to monitor its employees, provide information about the categories of data collected, inform employees about how their data will be secured and used, and clarify workplace privacy expectations when using company IT assets.

This policy contains references to the policies, procedures, and practices that will be followed by NPC, when collecting, using, or disclosing the personal information of an identifiable individual that is a present, future, or former employee of NPC.

This Electronic Monitoring Policy constitutes a notification in accordance with Freedom of Information and Protection of Privacy Act (FIPPA). By acknowledging this policy, employees of NPC consent to the workplace monitoring and surveillance practices outlined herein.

Scope

This policy applies to all employees of Niagara Parks.

Definitions

“Employee” means an individual who is performing work for the Niagara Parks for wages per an employment agreement.

“Computer Monitoring” refers to the practice of collecting user activity data on company-owned computers, networks, and other IT infrastructure. This data includes, but is not limited to, web browsing history, files downloaded, data input, network traffic, logons to corporate systems, interactions with data, peripheral device usage, and information about the employee's computer.

"Data Collection" refers to the automated or manual processing of employee data. This includes the collection, use, and storage of employee data such as computer activity data and other forms of personal information.

"Personal Use" refers to an employee using company-owned devices, networks, and other assets for personal tasks such as non-work web browsing and sending personal emails.

"Personal Information" refers to any data collected about an identifiable individual. This includes obfuscated data that, when combined with other information, could identify the individual.

"Video Surveillance" refers to surveillance by means of a camera that monitors or records visual images of activities on company-owned property. Video surveillance does not include the capture of audio.

Policy

The Niagara Parks deploys various electronic monitoring applications/devices. A summary of the description of the monitoring, how employees are monitored and the purposes for which information obtained through electronic monitoring may be used by the employer is summarized in Appendix A.

Video Surveillance

Video surveillance equipment is used on company premises to ensure that employees, patrons, and company-owned assets are kept secure from theft, vandalism, and other forms of misconduct.
Video surveillance is also used on our WEGO bus systems to protect drivers and visitors.
Should unlawful activity be discovered, the recordings captured by video surveillance equipment will be used to the fullest extent of the law—including the possibility of disclosure to authorized third parties.

Video surveillance equipment will not be used in areas where employees have a reasonable expectation of privacy, such as bathrooms, changing rooms, and other private areas. Where video surveillance equipment is used the equipment will be made clearly visible and there will be notices indicating the presence of the equipment.

Computer Monitoring

NPC monitors the network and computer activity of employees to ensure that company-owned IT resources are used in accordance with the Acceptable IT Use policy, and other company policies where relevant.

Computer activity data may also be used to detect malicious or high-risk activities, monitor network performance, and prevent security incidents from occurring.

Employee Computer Monitoring Software

Remote access software may be used by authorized staff to remotely administer, manage and troubleshoot hardware and software when the device is connected to the network. External support may use remote access software if monitored by an It staff member.

Telephone Monitoring

All company-owned mobile and landline phones may be monitored to ensure appropriate usage and compliance with NPC’s policies surrounding the use of telephony in the workplace. NPC mobile phones are managed through mobile device management software to control releases of software and protect against malware.

Email Monitoring

All email communications that are sent through company-owned networks, equipment, or user accounts may be subject to monitoring. This includes network traffic flowing from any devices connected to the network (hard wired or via wifi) flowing to and from the internet.

Employee Data Collection & Processing Practices

Accounts accessing the NPC network are recorded for security and PCI-DSS (Payment Card Industry Data Security Standards) requirements. In the event of a data breach to the network it is required that IT be able to go back in time to determine how long a breached account has accessed the network in order to determine the scope of the breach.

Data Retention

Data is retained as required to meet business needs and retention is based on the classification of the data. For example, network access logs could be maintained for a period of three years.

Personal information will only be stored for a greater period of time under exceptional circumstances or as required by law.

Categories of Data Collected

The employee monitoring measures put in place may capture the following data:

- Timestamps of computer power states: Startup, shutdown, and sleep events
- Logons on company computers, virtual machines, and other desktops
- Logs of peripheral devices used on a given endpoint, such as storage devices (USB, DVD/CD, Tape, SD Card, etc.), wireless devices, communication ports, imaging devices, and mobile phones.
- File operations to portable storage devices (files copied, created, renamed, and/or deleted to/from these devices)
- File and data transfers to/from internet sources including the data size and bandwidth used.
- Applications with “risky characteristics” that are deemed “unapproved”
- The employee use of “remote access software” to access other computers outside the NPC domain.
- The employees use of unauthorized software.
- The employees use of social media platforms and other “software as a service” applications.
- Internet usage data including URLs/domains, pre-defined website content category, web page headers, search engine queries, timestamps, bandwidth consumption, and browsing time
- Application usage, including software downloads and time spent using each software
- IP addresses and system information of client computers
- Timeclock data to populate schedules

Who Has Access to Employee Data

Employee data is made available to a limited number of authorized NPC employees. Access to workplace monitoring data is restricted to an as-needed basis. Employee data will not be made available to managers unless the employee is their direct report and the data is required for a legitimate business reason.

Disclosure of Workplace Monitoring Data to Third Parties

Workplace monitoring data is only disclosed to third parties as is required by law or as needed to troubleshoot the workplace monitoring systems used by NPC to monitor employees in the workplace. All third parties that are provided with access to workplace monitoring data are subject to equivalent confidentiality and security requirements to ensure that employee data is not misused or disclosed without authorization.

Roles and Responsibilities

Chief Executive Officer (CEO)

- Ensure compliance and support of the policy.
- As Ethics Executive, respond to any alleged breaches of the policy

Managers/Supervisors

- Ensure employees are aware of electronic monitoring.
- Address any violations of this policy with employees.
- Report any violations.

Employee

- Be aware of the contents of this policy.
- Act in a manner consistent with this policy.

Information Technology

- Review and update this policy as required

Education and Training

Policy to be made available to employees

Related Policies

Niagara Parks Police Service General Order # 034 - Technology, Communications Systems, and Online Communities Appropriate Use

CPM 06-01 Acceptable IT Use

Related Procedures

Related Procedures

References and Consultation

Employment Standards Act 2000

Record of Changes

Version No.	Date	Section/Content Changed	Change Made / Reason for Change	Change By
1	October 11, 2022	All	New	Janice Spino Joe Shillington

Authorization

Name: David Adames
Title: Chief Executive Officer
Date: Click to select date

Appendices

Tool	Circumstance	How	Purpose
Endpoint Detection & Response	Continuous	This tool monitors the use of workstations (Programs run, files read and written, etc.) and compares it against a baseline	Network Security (to detect abnormalities and potential unauthorized use)
Network multi-factor authentication	Upon Login	Through a mobile app, or call to a voice line, Duo Security service authenticates the user.	Provides a second factor of authentication to the network.

Computer Monitoring		Monitoring of the network and computer activity of employees which may include the logging in times, and IP addresses. This also includes internet traffic monitoring to ensure employees are not abusing NPC bandwidth or breaking the Acceptable Use Policy.	Compliance with Acceptable IT Use policy; Network Performance; Detection / Prevention of malicious or high risk activities
Remote Access Software		NPC IT administrators at times may need to remote access into an employee’s device to troubleshoot an issue, configure a system or make systems adjustments to software or files.	This is to enable the Helpdesk support and ensure the employee has the working tools required to do their job.
Vehicle Telematics	All Fleet Vehicles During on Shift Use	On board sensors detect and report on vehicle location, driver behavior (hard braking, rapid acceleration, etc.) and engine diagnostics.	This is currently planned functionality for Fleet Management & Driver Safety & Security.

Video Surveillance	Continuous	Monitoring of company premises by clearly visible surveillance equipment (excluding areas where employees have a reasonable expectation of privacy). Notices, indicating the presence of the equipment, will be posted. This may include standard CCTV equipment and trail cameras along Parks trails.	Security from Theft, Vandalism & Misconduct (information may be disclosed to authorized third parties)
Telephone Monitoring		All company-owned mobile and landline phones may be monitored to ensure appropriate usage and compliance with NPC's policies surrounding the use of telephony in the workplace. NPC mobile phones are managed through mobile device management software.	For the purpose of managing mobile costs, tracking incorrect roaming charges, control releases of software, and protect against malware.

Email Monitoring		Email communications (incoming and outgoing) that are sent through company-owned networks, equipment, or user accounts may be monitored. This may include personal email accounts when those accounts are accessed through company-owned IT assets	As per Acceptable Use Policy, ensures NPC email is not abused and used for NPC business.
ADP Time Clocks	With use	The ADP time clocks identify the employee, their location, and the date and time.	To input time for payroll processing.
Card Readers	With use	Access to all NPC properties secured by a key card. Log files may track where an employee's card swipe is used.	Security from Theft, Vandalism & Misconduct