Human Resource Policy 1.17

Subject: **ELECTRONIC MONITORING POLICY**

Scope: **COUNTY COUNCIL, LIBRARY BOARD, COUNTY EMPLOYEES, INCLUDING STRATHMERE LODGE AND MIDDLESEX COUNTY LIBRARY, AND VOLUNTEERS**

Issued:

Revised:

Purpose:

The Corporation of the County of Middlesex (the "County") values trust, discretion, and transparency and believes employees deserve to know when and how their work is being monitored. This policy is intended to advise employees on the County practices relating to electronic monitoring of employees.

Policy:

The County is committed to maintaining a transparent and fair workplace. In this policy, the County identifies the types of electronic monitoring in place, provides information about the categories of data collected, informs employees about how their data will be secured and used, and clarifies workplace privacy expectations when using County assets.

Definitions:

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.

Electronic 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, facility access card monitoring, electronic employee time tracking, video surveillance, web browsing history, files downloaded, data input, network traffic, logons to corporate systems, interactions with data, peripheral (printer, mouse, keyboard, external drive) device usage, and information about the employee's computer.

Employee refers to any Members of Council, Library Board, directors, officers, managers, employees, contract employees, volunteers, other representatives, and agents including consultants and independent contractors of the County of Middlesex.

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

Personal Use refers to an employee using County-owned devices, networks, and other assets for work or personal purposes.

Procedure:

1. Electronic Monitoring conducted by the County

a) Computer and Network Monitoring

The County monitors the computer and network activity of employees to ensure that County-owned IT resources are used in accordance with the following IT Policies:

- IT Policy 1.01, Network Systems;
- IT Policy 2.02, Acceptable Use of Technology; and
- IT Policy 10.1, Remote Access (Teleworking).

The County monitors computer and network activity data of employees on a continuous basis. Computer and network activity data may be used to detect malicious or high-risk activities, monitor network performance, prevent security incidents from occurring, troubleshooting and diagnostics and evaluate employee performance.

Computer and network activity data may include, but is not limited to:

- Timestamps of computer power states: Start-up, 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 operations to file servers including department drives, shared drives and home drives (files copied, created, renamed, and/or deleted to/from these drives);
- Internet usage data including URLs/domains, timestamps, bandwidth consumption, and browsing time;
- Application usage, including software downloads and time spent using each software;

- IP addresses and system information.

b) Email Monitoring

The County may monitor at any time employee emails and use the information obtained through the electronic monitoring of employee emails to detect malicious or high-risk activities, prevent security incidents from occurring, troubleshooting and diagnostics and may be used to evaluate employee performance.

All email communications that are sent and received through County-owned networks, equipment, or user accounts are subject to monitoring. This may include an employee's personal use of their County-issued email account.

c) Mobile Device Monitoring (Corporate or Personal Devices)

The County monitors mobile devices that have access to corporate email on a continuous basis and may use the information obtained to monitor device performance, prevent security incidents from occurring, and troubleshooting and diagnostics. All mobile devices (cellphones and/or tablets) which have access to corporate email are monitored in accordance with the Mobile Device Management (MDM) system as referenced in IT Policy 5.01, Cellphone and Mobile Device.

The County-owned mobile devices with the Management (MDM) system installed monitors the physical location, applications installed, and the connectivity/online status of the mobile device. Personal mobile devices which are provisioned under the Policy 5.01, Cellphone and Mobile Device do not have physical location tracking enabled; however, the Management (MDM) system installed monitors applications installed, and the connectivity/online status of the mobile device.

d) Perimeter Access Control Monitoring (key fobs/access cards/key codes)

The County monitors all employee usage of key fob, access card and/or key codes which are used for entry to a site or facility, including the date and time of access and location through software monitoring programs. The County monitors perimeter access of employees to ensure that employees and County-owned assets are kept secure from theft, vandalism, and other forms of misconduct.

e) Telephone Monitoring

All County-issued desk and conference phones, including software-based telephones, are monitored each day for inbound and outbound call logs, including time of call, duration, call origin and destination through a software monitoring program. The County conducts telephone monitoring to assist with troubleshooting and diagnostics. Telephone conversations are not recorded.

f) Security Camera Monitoring

Video surveillance equipment is used on a continuous basis on the County's premises to ensure that employees, patrons, and County-owned assets are kept secure from theft, vandalism, and other forms of misconduct.

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. Additional information on the County's use of surveillance cameras can be found in IT Policy 6.01, Security Camera System.

g) Biometric Time Clock

The County utilizes a biometric time clock for all scheduled shift that a staff member works by enrolling four (4) fingerprints for each employee as the primary sign in and sign out procedure for time and attendance at Strathmere Lodge. This time clock is used for payroll reporting purposes to a time keeping database and the data may be used to evaluate employee attendance.

h) Fleet GPS Location Tracking

The County uses in-vehicle GPS location tracking to monitor the movement of County fleet vehicles (snowplows, paint truck, pickups) to determine compliance with minimum maintenance standards for winter operations and for dealing with claims and complaints against the County by the public. The information is often utilized as part of the County's legal defense for claims against the corporation.

The in-vehicle GPS location tracking has the capability to provide warnings if fleet vehicles are stopped for an excessive period of time, travelling at an unusual rate of speed, or have left the County unexpectedly or without authorization.

The tracking devices are in service at all times whether the vehicles are active or parked. The County may place some aspects of the GPS tracking devices on standby outside of the winter season.

2. Prohibited Forms of Monitoring

The following forms of electronic monitoring are strictly prohibited:

- Keylogging (recording individual keystrokes);
- Video monitoring in private spaces, such as offices and bathrooms;
- Covert surveillance, such as actively monitoring computer activity without due notice;
- Covert recording or streaming of webcam or audio feeds;
- Covert recordings, such as office telephones calls, corporate and mobile devices calls.

3. Personal Use of Corporate Assets

The County recognizes that its employees may occasionally desire to use County-owned systems for personal tasks during their normal course of business. This may include non-work web browsing, making personal phone calls, or sending emails from personal accounts.

While personal use is permitted, the County reserves the right to monitor personal use on County-owned assets to the same extent that it monitors business use. Employees must operate under the assumption that all traffic over company networks is monitored and conduct themselves accordingly.

All personal use of company equipment and systems must abide by IT Policy 2.02, Acceptable Use of Technology.

4. Personal Electronic Equipment/Bring Your Own Device ("BYOD")

For employees who are permitted to use personal electronic equipment for work purposes ("Bring Your Own Device" or "BYOD"), the County will make every reasonable effort to not monitor the personal activities that take place on that device.

Employees participating in the BYOD program will be monitored when accessing the County's IT infrastructure, cloud-based applications, and other resources. For example, data collection will occur when personal electronic equipment is used on County-owned wireless networks, virtual private networks ("VPN"), and any other interaction from personal electronic equipment with County-owned IT systems.

The County reserves the right to remotely wipe all County-owned data from personal electronic equipment. This will most commonly occur when a BYOD-eligible employee is no longer employed by the County or personal electronic equipment is lost or stolen.

5. Privacy and Confidentiality

The County's electronic monitoring is aimed at collecting information related to its business. However, some information collected by electronic monitoring may be considered personal information. When personal information is under the County's control, it is the responsibility of the County to protect it.

All information collected through electronic monitoring will be securely stored and protected. If any personal information is collected, its use and disclosure will be limited to achieve the stated purpose of its collection.

The County has the appropriate control measures in place regarding any information collected under this policy to ensure it is only accessible by authorized individuals as set out in IT Policy 10.1, Collection and Use of Electronic Monitoring Information.

The County will adhere to all privacy and confidentiality legislation that applies to the collection, use, and disclosure of personal information obtained by electronic monitoring in accordance with the *Municipal Freedom of Information and Protection of Privacy Act* and Legislative Policy 3.01, Protection of Privacy and Confidentiality of Information.

6. Complaint Process

An employee can only file a complaint to the Ministry of Labour, Training and Skills Development, where there is an alleged contravention of the County's obligation to provide a copy of the written policy to its employees within the required timeframe as set out in the *Employment Standards Act*.