1. **POLICY**

Ongwanada will ensure that the privacy, confidentiality and security of all personal and/or personal health information of staff, individuals served and their families and service users under its control are protected. Ongwanada complies with all applicable laws and is committed to the standards outlined in the *Personal Health Information Protection Act (2004)* and the *Personal Information Protection and Electronic Documents Act (2001).*

Ongwanada electronically monitors employees through various means and for various reasons to ensure compliance by monitoring activity as outlined below.

**2.0 DEFINITIONS**

*The Employment Standards Act, 2000* was revised to include the employer requirement for an Electronic Monitoring policy which specifies how employees’ use of computers, cell phones, GPS systems and other electronic devices are being tracked.

This policy describes how and in what circumstances electronic monitoring occurs at Ongwanada workplaces, and sets out the purposes for which the information obtained through electronic monitoring may be used.

**3.0 PROCEDURE**

1. **General Provisions**
   1. Electronic monitoring is used by Ongwanada to protect corporate assets, and to deter/detect malicious threats, criminal activity, vandalism or other misconduct. Electronic monitoring may directly or indirectly enhance employee, resident, and/or public safety.
   2. In addition to the specific purposes identified within this policy by type of electronic monitoring, the information obtained may be used to:
      * Ensure appropriate use and security of Ongwanada assets
      * Monitor for policy compliance
      * Audit for clinical and legislative compliance
      * Investigate and respond to work related incidents, complaints or concerns
   3. No employee shall knowingly disable any network software or system identified as a monitoring tool.
   4. Third party requests for access to or production of electronic monitoring data shall be directed to the Privacy Officer to be addressed in accordance with PIPEDA and PHIPA;
   5. Failure to adhere to or violations of this Policy may be subject to discipline up to and including dismissal in accordance with Discipline and Dismissal policies and respective Collective Agreements, as applicable.
2. **Types of Electronic Monitoring Conducted and Their Purpose**
3. **Computer Monitoring**

Monitoring network activity and employee computer usage is essential to ensuring Ongwanada information technology infrastructure is used in accordance with policy and in a safe, secure and appropriate manner. Computer monitoring collects user activity data on Ongwanada-owned computers, networks and other IT infrastructure. This data may include websites accessed, files downloaded, network traffic, logons to corporate systems, peripheral device usage and information about the employee’s computer.

More specifically, all traffic from a user computer is logged.

These logs capture:

* Logging on and off of a computer
* Use of Virtual Private Networks (VPN) to access the Ongwanada network
* Connecting to wireless access points

Log data does not indicate precisely what a user was doing, with the exception of:

* + All traffic passing through a firewall is logged. This log captures information about the source and destination of the traffic, what website was being accessed by whom, and for how long. These logs do not necessarily provide details as to what the user was doing on the server or website.
  + Occasional, use of a “traffic sniffer” to assess a segment of the network for performance issues and/or malicious traffic.
  + Some Division/Department/Program specific applications provide greater visibility of user actions for audit and security purposes by tagging changes/actions taken with the user’s name. Electronic files within and reports from these applications are routinely audited by supervisory employees for clinical, legislative, and policy compliance. Audit results may inform feedback to employees. Examples include but are not limited to, eCIMS; Great Plains, Staffright; EPS

Computer activity data collected by the IT Department as described above is used to monitor network performance, troubleshoot issues, detect malicious or high-risk activities and to prevent security incidents from occurring. Where data might provide general information about specific user activity, such data may only be accessed and shared in accordance with the System Access and Security Policy (1-4-10)

1. **Telephone Monitoring**

All Ongwanada owned mobile and landline phones may be monitored to ensure appropriate use of telephony in the workplace. Specifically,

* + For land line and Ongwanada provided cell phones, call source, destination, duration and the amount of cellular data used are routinely captured.
  + Voicemail passwords on internal land lines may be reset to facilitate coverage and client service in the event of unplanned employee absence.
  + Ongwanada reserves the right to remotely wipe all data on Ongwanada provided cell phones in the event the device is lost, stolen or compromised, or the device is in the possession of a person no longer employed with the Ongwanada.
  + Ongwanada issued mobile devices have location services enabled in order to locate lost or stolen devices, and is accessed at the request of either the user or HR. Location history may be enabled at the request of HR, which stores and displays the list of locations traversed by the device over a period of time.

1. **Email Monitoring**

All email communications sent through Ongwanada-owned networks, equipment, or user accounts are subject to monitoring or review in accordance with the IT Audit Guidelines.

Ongwanada reserves the right to retrieve messages in order to assess whether Ongwanada assets are being used for legitimate business purposes, to retrieve information following suspected computer failures or to investigate alleged acts of wrongdoing.

1. **Building Access Monitoring**

Access to Ongwanada facilities is monitored where there is key card or fob access. The identity, date, time and location of access are captured by onsite software and hardware. This information is collected and may be used for investigation of incidents relating to theft, vandalism, other forms of misconduct, or the general safety and security of employees and Ongwanada owned facility assets.

1. **Video Surveillance**

Video surveillance system means a video, physical or other mechanical, electronic or digital surveillance system or device that enables continuous or periodic recording and/ or monitoring.

Video surveillance equipment is used at several Ongwanada properties (Barclay, Elizabeth, Balsam, Sunnyside, Haig and Gore) (to provide safety and security for supported individuals. It is also used at the Resource Center and Crescent for the above mentioned reasons as well as to deter theft, vandalism and other forms of misconduct thereby keeping employees, clients and Ongwanada-owned assets secure. .

Video surveillance equipment in some locations though not disclosed through signage, has been disclosed to supported individuals and employees during on-boarding. Where video surveillance equipment is used at the Resource Center and Crescent, the equipment is visible and signage is posted in close proximity to the equipment and the area being monitored.

1. **Prohibited Forms of Surveillance.**

To provide employees with a reasonable degree of privacy on Ongwanada owned assets, the following forms of surveillance are strictly prohibited unless there are exceptional circumstances and a legitimate business reason to do so.

* Keylogging (recording individual keystrokes)
* Video monitoring in private spaces such as bathrooms
* Covert recording or streaming of webcam feeds, meaning to record without due notice and/or participant permission or agreement

1. **Use of Personal Electronic Equipment**

Where employees are permitted to use personal electronic equipment for work purposes, only activities accessed through the Ongwanada IT network will be monitored and captured. For example, data collection will occur when personal electronic equipment is used on Ongwanada owned wireless networks, virtual private networks (“VPN”), and any other interaction from personal electronic equipment with Ongwanada-owned IT systems.

1. **Roles and Responsibilities**

Chief, Director, Manager or Supervisor is responsible to:

* Notify the HR Department when an electronic monitoring system has been discontinued or installed to ensure this policy remains current and accurate.
* Ensure employee computer access is appropriate to their role and their employment status; liaise with HR and IT as applicable.
* Ensure necessary agreements are in place when working with an external Service Provider who may come in contact with workplace electronic monitoring data.
* Ensure personal information is only accessed for the purposes set out in this Policy or reasonably consistent purposes.
* Ensure real or apparent privacy breaches are reported in accordance with Ongwanada’s Privacy Policy.

Employee is responsible to:

* + - Read, understand and adhere to this policy.
    - Conduct themselves in all aspects of work in a manner which demonstrates Ongwanada’s core values and consistent with Ongwanada’s Code of Conduct.

Information Technology Department is responsible to:

* + Ensure access to electronic monitoring data is provided only to authorized parties.
  + Ensure employee/user access is appropriate to their role and their employment status; liaise with Manager/Supervisor and HR as applicable.

Human Resources Department is responsible to:

* + Ensure all employees are provided with a copy of this Policy within 30 days of implementation and subsequently within 30 days of any policy changes made.
  + Ensure all new employees are provided with a copy of the written policy within 30 days of being hired.
  + Retain a copy of every written policy on electronic monitoring that was required by the *ESA* for three years after the policy is no longer in effect.

Ongwanada Privacy Officer is responsible to:

* + - Receive and make decisions with respect to the release of information.
    - Act as resource in the event of an identified privacy breach.
    - Provide Audit results to support or refute compliance with this policy and applicable legislation

**4.0 RELATED POLICIES:**

|  |  |
| --- | --- |
| [1-4-03](file:///C:\Users\lwilson\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\1-%20Administrative%20Policies\1-4%20Information%20Management%20and%20Communication\1-4-03%20-%20STAFF%20AND%20GUEST%20NETWORK%20ACCESS%20MONITORING%20AND%20CONTROL.docx) | Network Access Monitoring and Control |
| [1-4-04](file:///C:\Users\lwilson\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\1-%20Administrative%20Policies\1-4%20Information%20Management%20and%20Communication\1-4-04%20-%20CLIENT%20NETWORK%20ACCESS%20MONITORING%20AND%20CONTROL.docx) | Client Network Access, Monitoring and Control |
| [1-4-05](file:///C:\Users\lwilson\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\1-%20Administrative%20Policies\1-4%20Information%20Management%20and%20Communication\1-4-05%20DATA%20BACKUP%20AND%20RETENTION.docx) | Data Backup and Retention |
| [1-4-07](file:///C:\Users\lwilson\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\1-%20Administrative%20Policies\1-4%20Information%20Management%20and%20Communication\1-4-07%20DATA%20SECURITY%20AND%20ASSIGNMENT%20OF%20MOBILE%20DEVICES.docx) | Data use security and assignment of mobile devices |
| [1-4-08](file:///C:\Users\lwilson\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\1-%20Administrative%20Policies\1-4%20Information%20Management%20and%20Communication\1-4-08%20PRIVACY%20%20CONFIDENTIALITY.docx) | Privacy & Confidentiality |
| [1-4-09](file:///C:\Users\lwilson\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\1-%20Administrative%20Policies\1-4%20Information%20Management%20and%20Communication\1-4-09%20SECURITY%20OF%20INFORMATION.docx) | Security of Information |
| [1-4-10](file:///C:\Users\lwilson\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\1-%20Administrative%20Policies\1-4%20Information%20Management%20and%20Communication\1-4-10%20SYSTEM%20ACCESS%20AND%20SECURITY.docx)  1-4-19 | System Access and Security  eCIMS |

**5.0 LEGISLATION SECTION:**

* *Personal Health Information Protection Act (2004)*
* *Personal Information Protection and Electronic Documents Act (2001),*
* *Employment Standards Act, 2000*

**6.0 LEAD PERSON**

Chief, Human Resources Officer