| Oak Valley Health | **Title: Workplace Monitoring Policy** |
|---|---|
| Location: Administrative (ADM)\Administration and Organization (ADM-ORG) | Revision: 1.0 |
| Document Owner: Director Privacy | Original Approval Date: 10/04/2022 |
| Farrow, Mark (Chief Technology and Privacy Officer) | Approval Date: 10/05/2022 |
| Review Frequency: Annual | Next File Review Date: 10/04/2025 |
| IMPORTANT NOTICE: Unless a policy refers to the Markham Stouffville Hospital, operating at 381 Church Street, Markham, ON in particular, reference to "Markham Stouffville Hospital" on a policy with an approval date of on or before August 18, 2021, shall be interpreted to mean the corporate entity Oak Valley Health. Any reference to "Markham Stouffville Hospital" on a policy with an approval date on or following August 18, 2021, shall be interpreted to mean only the hospital located at 381 Church Street, Markham, ON. | |

## PURPOSE AND SCOPE:

This policy applies to everyone who works at or on behalf of the Oak Valley Health, including all employees and affiliates (including but not limited to Professional Staff, students, learners, residents, fellows, volunteers, and researchers), external users, contractors, vendors and suppliers.

## POLICY STATEMENT(S):

Oak Valley Health is committed to maintaining a transparent and fair workplace. Through the Workplace Monitoring Policy, Oak Valley Health will communicate it's intent to monitor staff, provide information about the type of data collected, how it's used and secured, and to clarify workplace privacy expectations.

### Expectation of Privacy in the Workplace

Monitoring employee usage of technology resources is an essential part of enforcing organizational policies, maintaining a respectful work environment, and ensuring that technology assets that are owned and managed by Oak Valley Health are used safely and appropriately. This applies to information technology for which the Oak Valley Health has responsibility, and all information and information technology it owns or uses in the conduct of its work.

Staff must not expect privacy when using Oak Valley Health technology resources. While all personal information collected by Oak Valley Health will be used fairly and appropriately as per this policy, all activities that take place via Oak Valley Health's technology resources should be considered monitored.

### Collection of Monitoring Data

The type of data collected through monitoring activities can include but is not limited to the following:

| | |
|---|---|
| **Video Surveillance** | Closed Circuit Television (CCTV) cameras are deployed, and in use, across all Oak Valley Health buildings. All camera footage across Oak Valley Health is retained for a period of 30 days, after which time, it records over itself |

| | |
|---|---|
| | CCTV cameras are never installed or used in areas where people have a reasonable expectation of privacy, such as washrooms, change rooms, showers, or other private areas |
| **Information Technology Resources and Applications** | Logons used on a given endpoint, for example but not limited to storage devices, wireless devices, communication ports, imaging devices, and mobile phones<br><br>Logs of user actions to patient information systems, date/time, name of patient accessed, information viewed, modified or deleted, and duration of the access<br><br>Internet usage, website content category, web page headers, search engine queries, timestamps, bandwidth consumption and browsing time<br><br>Application usage, including software downloads<br><br>IP addresses and system information of client computers |
| **Telephones** | All incoming and outgoing calls to the telecommunications department, including both 905-472-7373 and 905-472-7000 may be monitored for quality assurance and performance monitoring. The goal is to improve consistency of customer service provided by our employees, while supporting them against mistreatment |
| **Email** | All email communications that are sent through Oak Valley Health owned networks, equipment, or user accounts are subject to monitoring. This does NOT include personal email accounts when those accounts are accessed through Oak Valley Health owned assets<br><br>A manager or supervisor may be given short-term access to an Oak Valley Health e-mail account in order to support business activities, to investigate suspected misconduct, to respond to a freedom of information request, to support a legal investigation, or in a user's absence following termination |
| **Website and Social Media** | General and ongoing monitoring of Oak Valley Health social media accounts for appropriate behaviour. This does NOT include personal social media accounts |

| | |
|---|---|
| | when those accounts are accessed through Oak Valley Health owned assets.<br><br>General analytics tracking on the website for which pages are viewed and for how long, etc.<br><br>Analytics for the internal Connections newsletters tracks general data such as opens, clicks |
| **Facilities Access Monitoring** | Oak Valley Health monitors access to secured areas including parking facilities through, access card/employee badge |

**Use of Monitoring Data**

The information collected through monitoring activities may be used for the following purposes:

- to ensure the appropriate use of Oak Valley Health equipment;
- to reduce, deter and investigate incidents of violence, crime, or vandalism;
- to investigate an incident involving the safety or security of people, facilities, or assets, including parking lots and outdoors grounds;
- to investigate patient or staff complaints and concerns;
- to reduce, deter and investigate incidents of malicious or high-risk activities, monitor network performance, and prevent information security incidents from occurring in accordance with the Acceptable Use Policy, Identity and Access Management Policy;
- to reduce, deter and investigate incidents of unauthorized access, use or disclosure in accordance with the Privacy Audit Policy;
- to investigate an incident or allegation of employee misconduct, including but not limited to ensuring work is being performed during working hours, or to evaluate an employee's work performance;
- to provide evidence as required to protect the Hospital's legal rights;

**Access to Monitoring Data**

All access to workplace monitoring data is restricted to an as-needed basis for a legitimate purpose as outlined in this policy.

**Disclosure of Monitoring Data**

Records obtained must only be released according to the standards set under the Freedom of Information and Protection of Privacy Act ("FIPPA),this policy and other applicable law. Any monitoring data retained by Oak Valley Health will be handled in a manner that provides continued security of the recorded information.

**Prohibited Monitoring Activities**

To provide Oak Valley Health staff with a reasonable degree of privacy, the following forms of surveillance are strictly prohibited

- Keylogging (recording individual keystrokes)
- Video monitoring in private spaces such as bathrooms or change rooms
- Covert surveillance, such as monitoring computer activity without due notice unless there are exceptional circumstances and a legitimate business reason to do so.

- Covert recording or streaming of webcam feeds

**DEFINITION(S):**

**Personal Use:** refers to an employee using Oak Valley Health -owned devices, networks, and other assets for personal tasks such as non-work web browsing and sending personal emails.

**Record:** any record of information however recorded, whether in printed form, on film, by electronic means or otherwise includes: (a) correspondence, a memorandum, a book, a plan, a map, a drawing, a diagram, a pictorial or graphic work, a photograph, a film, a microfilm, a sound recording, a videotape, a machine readable record, any other documentary material, regardless of physical form or characteristics, and any copy thereof, and (b) subject to the regulations, any record that is capable of being produced from a machine readable record under the control of an institution by means of computer hardware and software or any other information storage equipment and technical expertise normally used by Oak Valley Health; ("document")

**Technology Resources**: refers to all Oak Valley Health owned devices and network equipment that allows electronic devices to connect to and communicate with each other. Including but are not limited to desktops, notebooks and laptops and other type computing equipment.

**Unauthorized Access:** Access to personal health information that is not required to carry out a user's duties and responsibilities as defined by Oak Valley Health. Unauthorized access includes, but is not limited to, accesses by a user to: their own personal health information, a co-worker's PHI unless necessary to do his/her job, the PHI of family, friends, neighbours or other individuals known or unknown to the individual, unless necessary to do his/her job.

**Video Surveillance System**: refers to a video, physical or other mechanical, electronic, digital or wireless surveillance system or device that enables continuous or periodic video recording, observing or monitoring of personal information about individuals in open, public spaces.

**REFERENCE(S):**
Bill 88, Working for Workers Act, 2022
Employment Standards Act, 2000

**RELATED DOCUMENTS:**
Acceptable Use Policy
Video Surveillance Policy
Privacy Audit Policy

**RESPONSIBILITY:**

| Required Endorsements | Sponsor | Approval Authority |
|---|---|---|
| Managers Meeting<br>Operations Committee | Chief Technology and Privacy Officer | Senior Leadership Team |

**DOCUMENT HISTORY:**

| Type | Individual/Committee | Date | Outcome |
|---|---|---|---|
| New | Director, Privacy | 10/04/2022 | Approved |

| | | | |
|---|---|---|---|
| | Chief Technology and Privacy Officer<br>Chief Human Resource Officer | | |

**APPENDIX: N/A**