

Purpose

At Extend-A-Family Waterloo Region, we are committed to being a transparent and fair workplace. We take our employees' privacy seriously and ensure we protect their data (see Computer policy). Pursuant to the Employment Standards Act, 2000 (ESA), provincially regulated employers must put in place an "Electronic Monitoring Policy" that states whether or not the employer electronically monitors employees. This requirement was added to the *Employment Standards Act, 2000 (ESA)* on April 11, 2022.

Scope

This policy applies to all EAFWR employees including but not limited to salaried staff, Direct Support People (DSPs), students, consultants and independent contractors of EAFWR, where applicable by law. This policy also applies to all working arrangements: in-person, remotely, or in a hybrid/ flexible arrangement (see Remote Access Policy).

Statement

EAFWR does not engage in *active* electronic monitoring of any kind; authorized Information Technology (I.T.) staff do not collect, track, or monitor any activity taking place on devices connected to EAFWR's network for the purpose of employee tracking or performance. However, any activity where agency technology is used, the information resulting in its use falls under the purview of the organization. And so, under certain circumstances such as when an abnormal activity is flagged, EAFWR reserves the right to investigate the activity. The ESA does not limit the employers' use of the information gathered to the intended purposes of the investigation. *Passive* monitoring, which collects data automatically, is integrated into several electronic systems and tools used by EAFWR. An example of passive monitoring is computer monitoring (see definitions section). A list of programs and tools available to EAFWR, and the specific information passively monitored, can be found as an attachment to this policy. Should EAFWR begin to use electronic monitoring software in the future; an amendment to this policy would be communicated to all employees.

Responsibilities

- Leadership: Review and approve updates and sign annual reviews.
- Human Resources: Ensure that the policy is compliant with Employment Standards Act and other provincial legislation. Communicate the written policy to all employees within 30 calendar days of the policy being prepared and/or the policy being changed. And provide a copy of the written policy to new employees within 30 calendar days of being hired.
- Information Technology (I.T.): Regular analysis of electronic network to assess traffic flow, security, and usage patterns.

- Employees: All employees must operate under the assumption that all traffic over EAFWR networks, servers, and internet access, whether it is a company device or a personal device, is passively monitored and conduct themselves accordingly (see Mobile Devices & Security Policy).

Definitions

The ESA defines Electronic Monitoring as all forms of employee and assignment employee monitoring that is done electronically. Examples include but are not limited to GPS tracking, email tracking, and website browsing.

Computer Monitoring refers to the practice of collecting user activity data on company-owned devices, 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 employees' computer.

Questions

Any questions or concerns relating to this policy can be directed to HR and/or I.T.

References

Bill 88, Working for Workers Act, 2021
Bill C-27, Digital Charter Implementation Act, 2022
Employment Standards Act, 2000 (ESA)
Bring your Own Device (BYOD) Policy
Computer policy
Mobile Devices & Security Policy
Remote Access Policy
HR Policy Review Process

Effective Date

October/ 11/2022

Review Date

JAN/01/2023.

Notes: Beginning in 2023, and in the years that follow, employers that employ 25 or more employees on January 1 of any year must have a written policy on electronic monitoring in place before March 1 of that year. This policy may be updated or amended based on direction from the Government of Ontario.

Approval

Approved by: Leadership Team and Executive Director
Approved on: 10 /11/2022

Name of System or Tool – What information is passively monitored

EAFWR Provided Google Accounts – Logins, communication history, # of sent and received emails, calendar events, IP address in use, chat logs and times, storage used, google drive files, aggregated reports.

EAFWR Provided laptops – Logins, IP addresses, activity, computer usage information (storage, processing power usage, software installed)

EAFWR Provided Intranet Access (including guest wifi) – User logins, login / logout times, files accessed, IP address

Building Access and Alarm systems – Code entries, times of arming and disarming, times of entry and exit

Avaya phone system – Call times, sent/received call history

Pritunl VPN – IP address, times of access

EMHware – Logins, times, all activity while using the database

Synerion – Attendance tracking, PTO usage, leaves of absence

Mailchimp – Aggregate data for mass email communication open rates. Specific user open status for mass email communications