



FOR INFORMATION

PUBLIC

OPEN SESSION

TO: Academic Board

SPONSOR: Kelly Hannah-Moffat, Vice-President,
CONTACT INFO: People Strategy, Equity & Culture 416-978-4865,
vp.psec@utoronto.ca

PRESENTERS: Same as above
CONTACT INFO:

DATE: November 3, 2022 for November 17, 2022

AGENDA ITEM: 4

ITEM IDENTIFICATION:

Policy on Transparency in Electronic Monitoring

JURISDICTIONAL INFORMATION:

Pursuant to Section 5.9 of its *Terms of Reference* the Business Board has authority for approval of human resources policies for non-union administrative staff; and under Section 5.10, authority regarding terms and conditions of employment for unionized administrative staff ... and approval of agreements and changes to agreements outside the *Labour Relations Act* with respect to terms and conditions of employment, subject to any limitations established by law or contract.

GOVERNANCE PATH:

1. Academic Board [For Information] (November 17, 2022)
2. Business Board [For Approval] (November 23, 2022)

PREVIOUS ACTION TAKEN:

n/a

HIGHLIGHTS:

The [Employment Standards Act, 2000](#) (ESA) was amended in April 2022 to require organizations with 25 or more employees to have in place a written policy on the electronic

monitoring of employees no later than October 11, 2022. The amendment to the ESA was made with a view to requiring transparency where electronic monitoring may occur, and does not require employers to begin monitoring, nor does it preclude employers from conducting such activities.

The Act does not provide a clear definition of electronic monitoring, requiring employers to assess which activities might be captured. The legislation requires that an employer's policy must state whether the employer electronically monitors employees. If the employer does monitor employees, the policy must include: a description of how and in what circumstances the employer may electronically monitor employees and the purposes for which the information obtained through electronic monitoring may be used by the employer.

The legislated requirements left room for individual institutions to interpret and create their policies based on their practices and context. The University of Toronto's labour relations environment is the most complex among all Ontario universities – accounting for 27 bargaining units and 5 non-union employee groups. Accordingly, the University's *Policy* has been written to provide high-level information regarding electronic monitoring that could apply across all employee groups. Other Ontario universities have taken a more detailed approach, setting out in their policies definitions of active versus passive monitoring or including more extensive lists of electronic monitoring tools.

It is important to note that with or without this policy, the University upholds the protection of academic and personal freedoms as an institutional priority and it does not use system surveillance to monitor academic work or impose limitations on academic freedoms, or use video surveillance in areas where privacy or comfort is expected, such as in washrooms or changerooms, nor does it monitor employee activity through keystrokes or length of log-in to University systems.

The *Policy on Transparency in Electronic Monitoring* (the *Policy*) affirms that electronic monitoring of employees is limited to contexts and situations that ensure the protection, management, and security of the University's digital and physical resources and the safety of the University community. To that end, employee access to, and usage of, University property (including information technology, digital assets, and systems) may be electronically monitored. Electronic monitoring may also be used to respond to health and safety concerns; in investigations; under court orders; or in other situations required by law. The *Policy* stipulates that employees be notified if electronic monitoring will be used in other situations, such as recording a meeting.

The *Policy* includes a non-exhaustive list of possible types of electronic monitoring such as the use of GPS monitoring of University-owned vehicles, the use of cards or fobs to access to University premises, the use of video surveillance/closed-circuit television (CCTV), and the use of information technology, digital assets, and systems.

The Division of People Strategy, Equity and Culture (PSEC) consulted widely in the development of the University's policy. Consultations spanned our three campuses and involved divisional HR managers and CAO offices, IT security, Data Governance, the CIO Office,

Freedom of Information and Protection of Privacy Act Office (FIPPA), Office of Safety and High Risk, and Office of the Vice-President and Provost (including the Office of the Vice-Provost, Faculty and Academic Life). A copy of the draft policy has been shared in advance with UTFA and unions.

Our policy is called the *Policy on Transparency in Electronic Monitoring* to signal the University's ongoing commitment to communicate openly about the extent to which employee activity is monitored electronically. It does not represent a change of practice; rather, it makes current practice more transparent for employees.

The Division of People Strategy, Equity and Culture will continue to work with internal subject matter experts on resources that may set out additional examples of types of electronic monitoring such as a chart of electronic monitoring tools and how they may be used. We will work with internal stakeholders to develop resources for individuals that are not captured under this *Policy*, including visitors, contracts, and students. Key stakeholders in this continuous approach to implementation include the Information Security Council.

The Division of People Strategy, Equity & Culture (PSEC) will monitor the implementation of such policies at peer institutions and broader public sector employers to ensure that resources are effective in communicating the *Policy*, that these resources remain relevant to the community, and to determine whether additional resources or amendments to the *Policy* are warranted to support transparency in electronic monitoring practices at the University.

RECOMMENDATION:

For Information.

DOCUMENTATION PROVIDED:

- Proposed *Policy on Transparency in Electronic Monitoring*



UNIVERSITY OF TORONTO GOVERNING COUNCIL

Policy on Transparency in Electronic Monitoring

Approval Date	
Approving Authority	Business Board
Effective Date	November 23, 2022
Responsible Office	Vice-President, People Strategy, Equity & Culture
Next Review Date	

PREAMBLE

This Policy on Transparency in Electronic Monitoring provides information regarding how, and in what circumstances, the University may electronically monitor employees, and the purposes for which the University may use information obtained through Electronic Monitoring.

APPLICATION/SCOPE

This Policy applies to all University employees. It is subject to the provisions of all applicable laws, employment contracts, collective agreements, and memoranda of agreement, and it should also be read in conjunction with all other applicable University policies and guidelines, including any of the foregoing related to Electronic Monitoring and use of electronic devices.

This policy does not provide employees any new privacy or other rights in relation to Electronic Monitoring. Nothing in this Policy affects or limits the University's ability to conduct, or use information obtained through, Electronic Monitoring. Nothing in this Policy is intended to amend or supersede any provision of any applicable collective agreement.

The term "**Electronic Monitoring**" refers to employee monitoring that is done electronically. It includes, but is not limited to:

- the use of GPS monitoring of University-owned vehicles
- the use of cards or fobs to access to University premises
- the use of video surveillance/closed-circuit television (CCTV)
- the use of information technology, digital assets, and systems.

POLICY

The University may monitor its digital and physical resources, and their usage, for the purposes of protecting, managing, and ensuring the security of those resources and the safety of the University community. The University's systems are capable of monitoring employees' access to, and usage of, University property, including information technology, digital assets, and systems. It is the University's intention to engage in Electronic Monitoring, or use data collected through such monitoring, in limited situations, such as those involving the following:

- health and safety concerns;
- security of University property, including information technology devices and systems;
- investigations;
- when required by law (e.g., court order); and,
- other situations with notice to employees (e.g., employees will be notified when a meeting is being recorded).

ASSOCIATED GUIDELINES/PROCEDURES

N/A

RELATED DOCUMENTS

- Employment Policies: <https://people.utoronto.ca/policies/>
- Collective Agreements: <https://people.utoronto.ca/agreements/>
- [Guideline on the Appropriate Use of Information Technology](#)
- [Policy on Information Security and the Protection of Digital Assets](#)

Should a link fail, please contact governing.council@utoronto.ca

REVISION HISTORY AND UPDATES *[Secretariat will complete]*

Date	Description of Change

KEYWORD INDEX

Electronic Monitoring

Video

Information technology security



UNIVERSITY OF
TORONTO

POLICY ON TRANSPARENCY IN ELECTRONIC MONITORING

DIVISION OF PEOPLE STRATEGY, EQUITY & CULTURE

NOVEMBER 2022



BACKGROUND

- Provincial government introduced [Bill 88, the *Working for Workers Act, 2022*](#)
 - Amended the *Employment Standards Act* in **April 2022**; now requiring employers to have written policies for electronic monitoring in the workplace.
 - [Additional guidance](#) released **July 2022**
- Provides transparency to employees
 - Modelled on similar legislation from the UK

WHAT THE LEGISLATION REQUIRES

- The policy must include:
 - a description of how and in what circumstances the employer may electronically monitor employees
 - the purposes for which the information obtained through electronic monitoring may be used by the employer
- Employees must be provided with a copy of the Policy

WHAT THE LEGISLATION DOESN'T DO

- Does *not* provide any additional rights to privacy for employees;
- Does *not* prevent the employer from monitoring its employees;
- Does *not* impact existing practices around using electronically-collected data regarding employees

WHAT IS ELECTRONIC MONITORING?

- Electronic Monitoring means "all forms of **employee** monitoring that is done electronically"; for example:
 - the use of GPS monitoring of University-owned vehicles
 - the use of cards or fobs to access University premises
 - the use of video surveillance/closed-circuit television (CCTV)
 - the use of information technology, digital assets, and systems

WHAT ISN'T ELECTRONIC MONITORING UNDER THIS DEFINITION

- Any electronic monitoring (e.g., Wi-Fi usage) related to people who are **not employees**:
 - Visitors
 - Students (outside of hours they are engaged as employees)
 - Trainees
 - Contractors
 - etc.
- Capturing electronic data related to **research**:
 - Quantitative or qualitative data gathered by Principal Investigators or Researchers
 - Accessing or using external research-related services, systems, and tools
 - Research data related to U of T employees are approved through the Provost and VP PSEC and appropriate disclosures are made to participants

THE HEART OF THE POLICY

- It is the University's intention to engage in Electronic Monitoring, or use data collected through such monitoring, in limited situations, such as those involving the following:
 - health and safety concerns;
 - security of University property, including information technology devices and systems;
 - investigations;
 - when required by law (e.g., court order); and
 - other situations, provided that notice is given to employees (e.g., employees will be notified when a meeting is being recorded).

Not an
exhaustive list

High-level to
capture a
variety of
circumstances
within Divisions

WHAT WE DON'T DO

The University does *not*:

- Use devices such as keystroke counters to monitor typing or activity;
- Track how long employees are logged into University systems;
- Use video surveillance in areas where privacy or comfort is expected (e.g., bathrooms, changerooms);
- Use electronic monitoring for the purposes of performance monitoring; or
- Use system surveillance to monitor academic work or impose limitations on academic freedoms (e.g., accessing intellectual property or confidential research data)

NEXT STEPS

- PSEC will work on resources to help managers and academic leaders answer questions from their employees about how and when they might be monitored within their specific roles
 - e.g., issues of performance and productivity
- PSEC will work with other shared service portfolios to develop responses to questions from non-employees around what type of monitoring may be happening
 - Note: this is *not* included in the scope of the Policy

