AMAPCEO
ONTARIO'S PROFESSIONAL EMPLOYEES

1 Dundas Street West, Suite 2310
PO Box 72 Toronto ON M5G 1Z3

416.595.9000
Toll-free 1.888.262.7236

September 2, 2022

Charlotte Ward
Senior Manager Policy & Evaluation, IT Governance Branch, Office of the Treasury Board
Treasury Board Secretariat
222 Jarvis St.
Toronto, ON M7A 0B6

To Ms. Ward,

The Ontario Public Service has long prided itself as a competitive, exciting employer with a commitment to excellence. Maintaining this reputation requires continually updating policy to reflect changing technological norms.

AMAPCEO appreciates being provided a copy of the Employer's *Acceptable Use of Information Technology (IT) Resources Policy & Guidelines Refresh* ("Policy" and "Guidelines"). Drawing from the experiences of our membership and expertise of our staff, we have reviewed the documents and recommend four key revisions:

1. Apply an Equity Lens to the Policy and Guidelines;
2. Permit reasonable discretionary personal use of IT resources;
3. Incorporate employee's reasonable expectation of privacy; and
4. Incorporate an enhanced electronic monitoring policy consistent with the recent *Employment Standards Act, 2000* (ESA) digital monitoring amendment.

1. Applying an Equity Lens

We are concerned that the *IT Resources Policy & Guidelines 2022 Refresh* fails to achieve the goals of the 2018 OPS *Anti-Racism Policy*. Removing systemic racism requires taking stock of every action, idea, policy, and program we have in the workplace. In the *Anti-Racism Policy*, the employer explicitly recognizes that, "Racism and power imbalances can be hidden or deeply embedded in government policies, practices and procedures." An equity lens needs to be applied to the 2022 Policy "Refresh" to ensure the Policy does not unintentionally perpetuate racism or power imbalances.

Specifically, the Policy permits the employer to individually monitor any employee's work computer/laptop, smartphone, or other IT resource at any time when an employer representative has a *reasonable expectation* that a specific person has violated the Policy.

The OPS' concerns about inappropriate use of IT resources are shared by our members. Our members do not want OPS IT resources to be used to perpetuate discrimination and they welcome rules to prohibit unwelcome behaviour. There are no guidelines for managers, however, as to what constitutes a *reasonable expectation*. This leaves us wondering *who* may be targeted for monitoring, *why* they may be monitored, how often they may be monitored and whether they will know they are being monitored. With this vague language and in the absence of socio-demographic data about who is being individually monitored, we are concerned racialized and Indigenous staff may be targeted.

2. Permitting reasonable discretionary personal use of IT resources

The Policy permits employees to have "reasonable and limited personal use of OPS IT resources" *provided* they receive permission from their manager first. The documents also say that managers must approve reasonable and limited personal use of OPS IT resources, as may be appropriate[1]. If managers *must* approve this time, why aren't Ontario's best and brightest simply given the right to reasonable and limited personal use of resources? It is odd employees aren't permitted to check a bus schedule or to review the weather while on a break, or to store a picture of their family on their computer without prior managerial approval.

The other concern about zero discretionary personal use is that currently, *any* use of government IT resources for a non-work related purpose, unless explicitly approved by a manager, is in violation of the Policy. Even with explicit managerial approval, the only acceptable use of IT resources, as per the Policy Guidelines, are "minimal" amounts of personal business, such as a single personal banking transaction.

It is unrealistic to expect this highly restrictive approach to use of IT resources to be applied with any consistency. Adhering to the Policy imposes an incredible burden on managers to approve potentially dozens of IT requests every week, creating unnecessary inefficiency. In our experience, many managers in the OPS are more likely to take a common-sense approach to the use of IT resources, encouraging technical breaches of this Policy.

We also note the comments of the Grievance Settlement Board on the practical difficulties that would arise if all technical breaches of such a policy were subject to enforcement:

"The problem, of course, is that a literal application and enforcement of [the I&IT

[1] "Acceptable Use of IT Resources Policy" 2022, Ontario government, pg. 12.

policy] has the potential to grind the wheels of government to a halt or at least limit government activity to little more than enforcement of the policy. The policy clearly, simply and without any enumerated exception, prohibits use of government resources for personal use, without a manager's approval. Thus, if an employee, without specific managerial authorization, sends an email home (perhaps in lieu of using the phone) to advise of a late return or to ask if s/he should pick up some milk on the way home, that would appear to be, strictly speaking, in violation of the I&IT Policy.[2]"

The fact that the current Policy encourages widespread technical breaches suggests the Policy will be selectively enforced. This further exacerbates our concerns that, as, written, the Policy may have unintended, inequitable consequences. We are very concerned about *which* individual employees will find themselves in conflict with the Employer. This is unfair and unacceptable. Moreover, it seems completely out of line with the OPS' interests and values.

The OPS should permit reasonable personal use of IT resources during personal time, while safeguarding the legitimate interests of the Employer (which also happen to be employee interests in many cases). This is also in line with the approach taken in several comparable Canadian jurisdictions including our federal counterparts, and the provincial governments of Alberta and British Columbia. For example, the Government of Canada permits limited personal use during personal time. Its *Guideline on Acceptable Network and Device Use, 2016* defines "Acceptable Use" of IT resources as the following:

"For limited personal use that is conducted on personal time; that is not for financial gain; that does not incur any additional costs for the department; and that does not interfere with the conduct of business.[3]"

The federal policy goes further to specifically list personal social media as an appropriate use of IT resources, when conducted on personal time and not infringing on other unacceptable uses[4]. We would urge the OPS to adopt a similar policy direction.

The Government of British Columbia also incorporates personal use of IT resources, without the necessity of managerial authorization, into its *Appropriate Use Policy*:

2.2 "Reasonable personal use of government IT resources by employees is permitted. Personal use is reasonable provided it is lawful, in line with the Standards of

[2] AMAPCEO (Egesi) v Ontario 2013 CanLii 87767 (ON GSB) (Herlich) at para 103.
[3] "Guideline on Acceptable Network and Device Use, 2016", Government of Canada, Accessed at (August 31, 2022): https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=27907.
[4] ibid.

Conduct and:

a. is limited during core business hours and does not interfere with the employee's duties and responsibilities;

b. does not compromise the security of government IT resources or government information, specifically confidential information; and

c. is not used for personal financial gain."[5]

Similarly, the Government of Alberta IT policy states:

> "Users may use the internet and email for personal purposes provided that such use is consistent with professional conduct, does not detract from the performance of the individual's employment or contractual responsibilities and is not for personal financial gain."[6]

What is common to each of the examples above is that they take as their starting point that limited or reasonable personal use during personal time (e.g., lunch, breaks) is permitted *without* explicit managerial approval every time. Given the concerns listed above, we would urge the Employer to move towards a similar structure for personal use in this IT Policy.

3. Incorporating Employee Digital Privacy Rights

There is little statutory guidance in Ontario regarding how employers are to behave with personal employee information on employer-owned IT resources. We would therefore encourage the Employer to take the current policy review as an opportunity to strengthen and clarify privacy expectations as they relate to the use of IT resources.

On privacy rights in the workplace, the Policy and Guidelines suggest our members have none. In law, however, they do have a reasonable expectation of privacy while using the Employer's IT resources or conducting Employer work on their personal IT resources. In its October 19, 2012, decision in *R v Cole* ("Cole"), the Supreme Court of Canada held that Canadians may reasonably expect privacy in information contained on workplace computers where personal use is permitted or reasonably expected. The court described such information as "meaningful, intimate and touching on the user's biographical core." They explain that workplace policies and practices and technologies in place for monitoring

---

[5] "Appropriate Use of Government Information and Information Technology Policy (Appropriate Use Policy)", May 2022, Government of British Columbia, Accessed at (August 31, 2022): https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/policies-procedures/appropriate-use-policy/appropriate_use_policy.pdf., pg. 6.

[6] "Use of Government of Alberta internet and email directive", Government of Alberta, Accessed at (August 31, 2022): https://www.alberta.ca/use-of-government-of-alberta-internet-and-email-directive.aspx.

network activity may diminish an employee's expectation of privacy, but such "operational realities" will not extinguish the expectation of privacy in its entirety.

Our members expect these privacy rights to be observed.

4. Incorporate an Electronic Monitoring Policy

The Policy and Guidelines are vague regarding the monitoring of employees and not in line with recent amendments to the *Employment Standards Act, 2000* (ESA) by this government which require employers to tell their employees if they are being monitored, how and when they are being monitored and the purpose for the collection of information.[7]

The current iteration of the Policy offers very little language that would help set expectations regarding what safeguards employees may have in respect of the Employer's use of the data and metadata (e.g., a record of websites visited, when, and by whom) that unavoidably accrues from their regular use of IT resources. Clearly, this type of information has the potential to be revealing of intimate biographical information that would typically attract reasonable expectations of privacy. The Policy makes clear that monitoring of individuals IT use may occur, but nothing more. The implication is that all activity that occurs on the employer's resources would be fair game for unrestricted examination.

The timing of this Policy and Guideline "Refresh," with the current landscape of electronic monitoring policy development happening in Ontario, offers the perfect opportunity to incorporate an electronic employee monitoring policy into the IT Policy.[8]

Accordingly, AMAPCEO recommends that:

1. Employees be provided with a statement explaining the Employer's standard network monitoring practices and for what purposes network monitoring will be used;
2. Any collection and/or monitoring of personal employee information must be subject to informed employee consent;
3. An employee's personal information so collected should only be kept for as long as it is needed to meet the stated purpose for collection;
4. Employees should have venues through which to access the personal information the employer collects, and be provided with mechanisms to challenge the accuracy or completeness of this information; and

[7]Employment Standards Act, 2000, SO 2000, c 41, Part XI.1 "*Written Policy on Electronic Monitoring*", Accessed (August 31, 2022): https://www.ontario.ca/laws/statute/00e41.

[8]"Written Policy on Electronic Monitoring of Employees, Government of Ontario", Accessed at (August 31, 2022): https://www.ontario.ca/document/your-guide-employment-standards-act-0/written-policy-electronic-monitoring-employees.

5. Exceptions to the above principles may be made where the Employer is legally required to use or disclose personal information for other purposes, or where illegal use of resources is suspected.

We appreciate the opportunity to assist the OPS in crafting effective policy. Please contact us to arrange for a meeting to discuss our suggestions.

Sincerely,

Dave Bulmer
President & CEO