AMAPCEO
ONTARIO'S PROFESSIONAL EMPLOYEES

September 9, 2016

RE: AMAPCEO Comments on Acceptable Use of I&IT Policy

To whom it may concern:

AMAPCEO appreciates the opportunity to provide feedback regarding the Employer's Acceptable Use of I&IT Resources Policy. Drawing from the experiences of our membership and staff, we will provide comment on four areas that the Association views as particularly requiring revision. These are the following:

I) adopting a more permissive approach to the personal use of IT resources;

II) moving away from the currently restrictive rules relating to the use of web 2.0 platforms and social media in the workplace;

III) clarifying the policy's application to employee-owned devices in the workplace; and

IV) incorporating a greater recognition of employee privacy interests into the policy.

In our view, these amendments would help encourage engagements with workplace information technology that are modern, efficient and digitally literate.

I. Adopting a more permissive approach to the personal use of IT resources

During previous consultations regarding the IT policy, AMAPCEO has emphasized the view that the Employer has taken an overly prohibitive position in respect of employee's personal use of employer IT resources. Currently, as per Article 6.2 of the policy, *any* use of government IT resources for a non-work related purpose, unless explicitly approved by a manager, would be in violation of the policy. Even with explicit managerial approval, the only acceptable uses for IT resources, as per the policy guidelines, are "minimal" amounts of personal business, such as a single personal banking transaction[1].

It is unrealistic to expect this highly restrictive approach to use of IT resources to be applied with any consistency. To be clear, AMAPCEO is not aware and does not suggest that the policy is being enforced in such a manner. In our experience, many managers in the OPS are more likely to take a common sense approach to the use of IT resources, rather than adhere to the policy to the point of inefficiency and absurdity.

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

[1] Government of Ontario. "Acceptable Use of Information and Information Technology (I&IT) Resources Guidelines" (March 2011), p. 7.

> "The problem, of course, is that a literal application and enforcement of [the I&IT 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."[1]

The fact that the current policy seems to encourage widespread technical breaches raises the question of whether a broadly unenforceable policy is one that is appropriate to the workplace. We would suggest it is not, and that it gives rise to concerns regarding selective enforcement of the policy. Specifically, we are concerned that individual employees who find themselves in conflict with the employer, even if that conflict is originally extraneous to any IT usage concern, might become subject to monitoring and discipline in accordance with the policy. This would be unfair and unacceptable.

We suggest the incorporation of language that would allow for the reasonable personal use of IT resources, while safeguarding the legitimate interests of the employer. This would be in keeping with the approach taken in several comparable Canadian jurisdictions. For example, the analogous Government of Canada IT policy has been recently updated to incorporate a more tolerant approach to personal use of IT resource. It defines "Acceptable use" as the following:

- To perform activities as part of their official duties;
- For career development and other professional activities;
- **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.**[2] (emphasis added)

The Government of British Columbia also permits the personal use of IT resources, without the necessity of managerial authorization, in its Appropriate Use policy:

> **Reasonable personal use of government IT Resources by Employees is permitted.** Personal use is reasonable provided that it: a) is limited during core business hours and does not interfere with the Employee's duties and responsibilities; b) is lawful; c) does not compromise the security of government IT Resources or Government Information; and d) is not used for personal financial gain.[3] (emphasis added)

[1] AMAPCEO v. Ontario 2013 CanLii 87767 (ON GSB) (Herlich) at para 103.
[2] Government of Canada. "Policy on Acceptable Network and Device Use" Accessed at: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=27122
[3] Government of British Columbia. "Appropriate Use Policy" Accessed at: http://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/appropriate-use-policy

Similarly, the Government of Alberta IT policy provides for personal use of the internet and email as a "guiding principle":

> "Users may use the Internet and E-mail for personal use, provided that such use does not interfere, in any manner, with the performance of their regular duties and complies with the policy below."[4]

What is common to each of the examples above is that they take as their starting point that reasonable personal use – without explicit managerial authorization - is permitted, insofar as this does not infringe on specific employer interests as further detailed in the policy. Given the concerns listed above, we would urge you to move towards a similar structure for personal use in the next iteration of the OPS IT policy.

II. Remove Restrictions to Web 2.0 Platforms and Social Media

We are requesting that the employer revise the current approach taken in the policy to the use of social media and "web 2.0" platforms in the workplace. In 2007, as social media platforms experienced a significant increase in popularity, the government moved reflexively to restrict the use of specific websites. At the time, the concerns cited included possible spikes in bandwidth usage, privacy matters, and network security issues. In addition, the employer, and even the Premier, questioned whether social networks "added value to the workplace".[5] These concerns were reflected in the current iteration of the IT policy. For example, in enumerating unacceptable uses of IT resources the current guidelines note that a primary rationale for forbidding use of social networking and "Web 2.0" is that it may "distract users from job duties"[6].

It is now apparent that many of the concerns which animated the OPS' initial restrictions on social media have diminished. The changing landscape was acknowledged Ontario's former head of Corporate Security as far back as 2011:

> "We blocked [Facebook] fairly early on. There were concerns about our networks at the time – bandwidth utilization. We were not comfortable with the security of Facebook and there were an awful lot of privacy concerns. **Now, if we had to do it today, it would be 50/50**".[7]

To the extent that bandwidth concerns are still driving any parameters of the IT policy, AMAPCEO would encourage the employer to make the necessary investments to ensure that those working in the OPS can participate in a comprehensive range of mainstream digital practices.

[4]"Use of Government of Alberta Internet and E-mail" Government of Alberta. Accessed at: http://www.chr.alberta.ca/Practitioners/?file=directives/relations/use-of-information&cf=5
[5]See the comments of Premier McGuinty in the Toronto Star, May 4, 2007: https://www.thestar.com/business/2007/05/04/worries_follow_rise_of_facebook.html
[6]Government of Ontario. "Acceptable Use of I&IT Resources Guidelines", pp. 6, 7.
[7] McCauley, Peter, quoted in Sutton, Neil. "Ontario Government Debates Future on Twitter, Facebook" *Canadian Security* March 7, 2011. http://www.canadiansecuritymag.com/Top-Stories/Ontario-government-debates-future-on-Twitter-Facebook.html

In regards to the idea that social media use would present an unacceptable distraction to job duties, we would suggest that the IT policy is not the appropriate place to prescribe what is and it not a threat to employee performance. There is little to credibly distinguish situations where an employee spends an inappropriate amount of time on social media from one where an employee is engaged in any other non work-related activity. Given this, we maintain that supervision of whether an employee is appropriately engaged in their duties would be more reasonably be left to typical performance management channels, rather than prohibitions in the IT policy.

Beyond the diminishing rationale for preventing access to social networks, it seems clear that the relative value of allowing these platforms in the workplace has increased. AMAPCEO's membership is routinely expected to use digitally-literate applications in order to engage the public, and using social media is often an important component of that. We note that many other large employers, including the federal government, have revised their approach to Web 2.0 and social media. For example, in its most recent iteration of its Acceptable Use policy, the federal government included the following statement regarding the importance of embracing new forms of communication technology:

> The Government of Canada recognizes that open access to Government of Canada electronic networks and devices, including the Internet, is essential to transforming the way public servants work and serve Canadians. Open access to the Internet including Government of Canada and external Web 2.0 tools and services will enhance productivity, communication and collaboration, and encourage the sharing of knowledge and expertise to support innovation. [8]

The federal policy goes further to specifically list social media interaction as an appropriate use of IT resources, when conducted on personal time and not overlapping with unacceptable forms of IT use. We would urge the OPS to adopt a similar policy direction.

III. Clarifying the Applicability of the Policy to Personal Devices in the Workplace

One area that requires increased attention in the policy surrounds the use of personally-owned IT resources in the workplace. Specifically, we suggest that the policy needs to specifically contend with what employee devices might be covered under the policy, when, and under what circumstances.

It is without question that employee-owned IT devices are more prevalent in the workplace than ever before. Correspondingly, these devices occasionally interface with employer-owned or work related resources in various (and sometimes unpredictable) ways. Examples of this are numerous, but could include situations where an employee owned storage device is used to transport electronic files, or when an employee owned smartphone uses the employer's Wi-Fi network to conduct personal business.

The policy is silent as to whether these kinds of devices, when they have some form of interaction with employer-owned or work-related resources, might be treated as falling under the

[8] Government of Canada "Canada Policy on Acceptable Network and Device Use", p. 11.

policy. A recent Grievance Settlement Board decision is illustrative of why this may be problematic[9]. In a hearing to determine the admissibility of certain pieces of evidence, the employer argued that an AMAPCEO member's privacy expectations regarding a personal electronic storage device were diminished given the presence of several generic work documents on it, alongside many other personal files. The employer argument hinged on the idea that the presence of work files "transformed" the key into an employer resource for the purposes of the IT policy[10]. The argument was ultimately unsuccessful. However, the fact that it was raised points to a need for more clarity regarding in what circumstances an employee owned device might fall under the policy.

Increased clarity regarding employee-owned IT devices is especially important as other large employers in the province begin to move towards "bring your own device" policies aimed at finding efficiencies by encouraging employees to merge personal and work IT resources. However, to be clear, whether or not the OPS intends to move towards such a policy we are strongly of the view that the current IT rules needs to provide our members with clear expectations regarding how their personal devices may be treated while at work.

IV. Strengthening Employee Digital Privacy

A final policy area that requires attention relates to the workplace privacy interests of our membership. Generally, employees in Ontario (and especially Crown employees) suffer from a lack of regulation regarding their privacy vis a vis their employer. There is little statutory guidance regarding how provincial employers are to behave with the personal employee information that may result from, for example, their use of employer-owned I&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.

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 information has the potential to reveal intimate biographical information that would typically attract reasonable expectations of privacy. However, Section 6.4 of 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.

Looking again to the analogous Government of Canada policy, we note an appendix is devoted to dealing exclusively with privacy concerns[11]. Perhaps given the different statutory privacy regime in place in the federal jurisdiction, this policy makes clear that individuals must be informed of departmental monitoring practices via a "privacy notice", prior to their implementation. We see no reason why a similar standard could not be set in the OPS, even absent any regulatory necessity.

[9] See AMAPCEO v. Ontario (Government and Consumer Services) 2016 CanLII 17002 (ON GSB) (Anderson).
[10] *Ibid* at para 100.
[11] "Policy on Acceptable Network and Device Use, Appendix D", p. 14. Government of Canada.

We would therefore recommend the following rules be incorporated into the policy:

1. Employees should be provided with a statement explaining the employer's standard network monitoring practices and what purposes network monitoring will be used for;
2. Any collection and/or monitoring of personal employee information must be subject to informed employee consent;
3. Any employee 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;
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.

While we encourage the employer to adopt these rules as a starting point, we would also be welcome to engaging further should the employer seek to address workplace privacy concerns more generally.

Again, we appreciate the opportunity to provide input into the policy review process. Please do not hesitate to contact us with any questions or concerns regarding the suggestions noted above, or to arrange for a meeting with myself and our staff.

Sincerely,

Dave Bulmer
President