PSAC 901

Public Service Alliance of Canada Local 901

May 21, 2026

FOR IMMEDIATE RELEASE:
New Cybersecurity Requirements for Graduate Workers

To all Graduate Teaching Assistants (TAs), Teaching Fellows (TFs), affiliated Research Assistants (RAs) and Postdoctoral Scholars at Queen's University:

We have been made aware that on May 19, 2026 graduate workers received communications regarding Queen's University's new cybersecurity protection requirements for personal devices. The deadline for adopting either Endpoint Assessment or Protected Access is currently **July 7, 2026.**

PSAC 901 encourages members not to enroll in the Protected Access model early. We also encourage members to avoid downloading Microsoft Intune onto personal devices altogether unless absolutely necessary. According to Microsoft, using Intune would provide Queen's administrators access to personal information including: device owner, device name, serial number, model, manufacturer and operating system details.

Our members have raised legitimate concerns regarding privacy, institutional oversight on privately owned devices, and the broader implications of expanding institutionally managed digital environments into personal spaces.

At present, there remains limited publicly available information outlining the full implications of these systems, including what data may be collected and how session controls would function in practice. While Queen's has presented Protected Access as an alternative to full device enrollment through Intune, many underlying concerns regarding worker autonomy, privacy, and institutional control over personal devices remain unresolved.

These concerns are not without precedent. The Queen's University Faculty Association (QUFA) previously grieved the mandatory downloading of Microsoft Intune onto personal devices. This process, we believe, contributed to Queen's University's adoption of the current Protected Access model as an alternative to full device enrollment.

Although Protected Access differs from Intune's more invasive mandate, broader concerns surrounding privacy, consent and the expectation that workers use personal

devices for institutional labour continue to affect graduate workers. For example, Microsoft states that Conditional Access App Control systems, such as the one newly required by Queen's, continue to "monitor and control user app access and sessions in real time," including blocking downloads, requiring reauthentication, preventing cut/copy/print functions and logging user actions within sessions.

This issue further highlights the increasingly blurred lines between student and employee status for graduate workers at Queen's. Graduate workers routinely occupy overlapping roles as students, instructors, researchers, employees, and tenants while simultaneously being expected to provide and maintain the personal devices necessary to carry out institutional work. As cybersecurity requirements expand, so too do concerns regarding who bears the costs, responsibilities and risks associated with these systems.

We are currently discussing these developments with members and in connection with the SGPS and have reached out to our friends at the Ontario Federation of Labour (OFL) and the Ontario Privacy Commissioner for guidance.

Collecting member concerns is a top priority. Please submit any questions, concerns, and thoughts you have in this Google Form. In the coming weeks, we will also be hosting a town hall to provide space for members to discuss concerns collectively, share information, and explore possible avenues for response and advocacy. Additional details will be shared soon.

In solidarity,

PSAC Local 901 Executive Committee