QUFA VOICES
Your Queen's University Faculty Association Newsletter

VOICES IN THIS ISSUE: March 2025

PRESIDENT'S VOICE: QUFA in Solidarity with PSAC 901, by Mary C. (Cella) Olmstead … 1-2
GRIEVANCE CORNER: It's All in the Details, by Karen Sisson … 3
QUFA ALBUM: PSAC 901 Job Action, by Robert G. May … 4
FYI: Endpoint Protection: Consequences and Recommendations, by Christian Muise, Wendy Powley, James Stewart, and Catherine Stinson … 5-6
OPEN LETTER: Endpoint Protection: An Open Letter from the Faculty of Law, by Eric S. Knutsen, Lisa Kelly, and Ashwini Vasanthakumar … 7-8

PRESIDENT'S VOICE

QUFA in Solidarity with PSAC 901

QUFA stands in solidarity with striking PSAC 901 members, who perform crucial work at Queen's

By Mary C. (Cella) Olmstead
President, QUFA

This is an updated version of an open letter of solidarity with PSAC 901 that was made public on Thursday 13 March 2025.

QUFA stands in solidarity with PSAC 901 as they engage in a legal strike to secure fair compensation and safe working conditions for their members.

The work carried out by these Teaching Assistants, Research Assistants, and Teaching Fellows is integral to the research, scholarship, and teaching of all QUFA Members. Their work makes our work possible. Their working conditions are our working conditions. When they are not adequately supported, our work is not adequately supported, and our students suffer.

Nearly 40% of all classes at Queen's are taught by Adjuncts. Adjuncts are highly qualified professionals stuck in precarious contract work. Because of budgetary decisions, both by the Ontario government and by Queens, many of these Adjuncts are losing their jobs. Many of their courses are being cancelled or assigned to already

QUFA IMAGES

A Colourful Show of Solidarity

Robert G. May

Faculty members in full academic regalia gathered in front of Richardson Hall on Friday 21 March 2025 for a Faculty Day of Action, a rally and teach-in in support of striking PSAC 901 workers. The event was organized by a group called Concerned Queen's Faculty (CQF), and represented a range of members from Arts and Science and other faculties across campus.

ANNOUNCEMENT

PSAC 901 Job Action: The Latest

At the end of the third week of the PSAC Unit 1 strike, QUFA continues to stand in solidarity with workers in this union. This past Friday, QUFA provided pizza on the picket line as part of our commitment to help lend support to PSAC's striking members, per our solidarity policy.

This is a difficult time for graduate students who are struggling to meet financial, academic, and research responsibilities. I encourage you to reach out to graduate student colleagues and offer your support in whatever capacity you can.

As a reminder, the QUFA Collective Agreement (CA) secures your right to refuse to carry out the work of a striking union. You can find more details on the QUFA job action Web site:

https://qufa.ca/campus-job-action-news/

If you have concerns that you are being asked to take on duties that are the work of PSAC 901 members, please contact QUFA for advice (qufa@queensu.ca).

Finally, if you receive any communication regarding your labour during the strike that is not authored by Queen's administration, or QUFA staff or leadership, please contact us immediately for advice and support. It is important to understand that QUFA maintains exclusive authority to provide advice to the Membership about the correct interpretation of our CA, and you cannot be compelled to exercise your negotiated rights in a particular way. We remain available if you have any questions about how your work has changed or is being directed while the strike is ongoing.

overworked graduate students in the form of teaching fellowships, because this is a cheaper option. Teaching Fellows should be paid at a rate that does not make them a default cheaper option.

When Bill 124 was declared unconstitutional, QUFA and other campus unions sent an open letter to Queen's administration requesting that contracts be reopened so that workers could negotiate fair wages. They flatly refused. Now, many of our graduate students are living below the poverty line, having their wages unconstitutionally suppressed for three years. We strongly urge Queen's administration to act with integrity by returning to the bargaining table, negotiating in good faith, and providing all PSAC members with fair compensation, resources, and the support they deserve.

We remind our Members that they have the right to refuse work that is assigned to members of a striking union. Our Collective Agreement also provides protection for QUFA Members who decline to cross the picket lines of another union in order to carry out their own work (Article 12.3.c). You are required to inform your head "as early as reasonably possible," and may be required to forfeit pay *for the day* on which you do not undertake your duties, but you cannot be disciplined for this action.

For more details, please refer to previous QUFA communication on campus job action that lays out the rights and responsibilities of our Members during job action by another union.[1] Again, I encourage you to show solidarity with our graduate-student colleagues by joining them on the picket line, writing a letter of support,[2] or donating to the Sustain Striking Workers Fund.[3]

Notes

[1]https://qufa.ca/campus-job-action-news/

[2]https://actionnetwork.org/letters/write-a-letter-to-queens-admin-to-support-psac-901

[3]https://www.paypal.com/ncp/payment/FJ5LWFSTBE9JN

Mary C. (Cella) Olmstead can be reached at olmstead@queensu.ca.

QUFA VOICES March 2025 (Volume 20, Number 7, Issue 125)

QUFA Voices is published by the Queen's University Faculty Association (QUFA), 9 St Lawrence Avenue, Kingston, Ontario, K7L 3N6, Canada (qufa@queensu.ca). It is distributed electronically to all QUFA Members via the QUFA-NEWSLETTER-L listserv. Past issues are archived on the QUFA Web site at https://www.qufa.ca/voices/.

QUFA Voices publishes QUFA-related news and information for QUFA Members and provides QUFA Members with a forum to express their QUFA-related ideas and opinions. We want to hear from you! Please send your QUFA-related story ideas, news items, opinion pieces, letters to the editor, photographs, and other submissions to the editor.

QUFA Voices is edited by Robert G. May. He can be reached at mayr@queensu.ca.

GRIEVANCE CORNER

It's All in the Details

Knowing your QUFA-Queen's Collective Agreement rights during the PSAC 901 job action

By Karen Sisson
Grievance Officer, QUFA

In light of the ongoing PSAC 901 strike, QUFA staff have received several questions from QUFA Members about each Member's right to withdraw their labour when declining to cross a picket line of a legally striking bargaining unit pursuant to Article 12.3.c and 12.3.d.

Some faculty have also expressed interest in coordinating various demonstrations of support for the workers engaged in the strike, and QUFA has also provided some advice about such activities. To that end, it is important to acknowledge that demonstrations of solidarity can take many forms and are certainly not limited to the withdrawal of labour. Nevertheless, in response to such queries, QUFA has very carefully and consistently advised that it is legally prohibited from organizing or otherwise encouraging or condoning any conduct that could be construed as job action during the life of the Collective Agreement (CA) (a.k.a. "wildcatting").

A very important distinguishing feature of the right to refuse to cross a picket line at Article 12.3 is the fact that the right is an individual right and not a collective right. That distinction is important because of the strict statutory prohibition against unlawful strikes or lockouts contained in Ontario's Labour Relations Act (OLRA). The QUFA CA also explicitly prohibits any strikes or lockouts during the life of the CA at Article 12.1.

A "strike" is defined in the OLRA as "a cessation of work, a refusal to work or to continue to work by employees *in combination or in concert or in accordance with a common understanding*, or a slow-down or other concerted activity on the part of employees designed to restrict or limit output" (emphasis added). Such a broad statutory definition is why the right to refuse to cross a picket line at Article 12.3 must be understood strictly as an individual right and not a collective right; otherwise, the article could be deemed unenforceable for being contrary to statute.

Because it is an individual right, the choice to invoke Article 12.3.c or Article 12.3.d must be exercised by a faculty member for their own reasons and not in a manner that amounts to a concerted or coordinated work refusal. QUFA cannot tell a member whether to exercise the right, and any other member of the Queen's community is equally prohibited from seeking to intimidate or otherwise compel any QUFA Member to invoke or decline to invoke that provision of the CA.

Some other misunderstandings may have arisen due to certain communications provided by the Administration to QUFA Members. Some of those communications seem to suggest limitations to the rights provided by Article 12.3 that are simply not present in the CA. As an example, the right is intended to be invoked individually and on a day-by-day basis. There is no reason a QUFA Member should feel compelled to agree to anything other than a single day of leave without pay for each occurrence, and there is no need for a Member to make any broad declarations covering their scheduled duties until the cessation of the strike.

As another example, while it is reasonable for the Administration to request that Members fill out additional paperwork that may not be strictly required per the CA, Members should not be made to fear that their rights will be unenforceable based on a failure to have completed such a form in a timely way.

Any action taken by a QUFA Member in relation to Article 12 (or any other portion of the CA) must be taken based on informed advice and a clear understanding of the right. In recent weeks, QUFA has provided several written communications to the Membership about Article 12 and other matters pertinent to demonstrating solidarity with other bargaining units at Queen's. Those articles may be found on the QUFA Web site. QUFA has also hosted several information sessions, and details about any further sessions will be made available to the Membership. If you have any additional questions after reviewing QUFA's materials, please do not hesitate to reach out to request a consultation call.

Karen Sisson can be reached at ks233@queensu.ca.

ANNOUNCEMENT

Spring General Meeting

The annual QUFA Spring General Meeting is scheduled for

Thursday 24 April 2025
1.00 p.m.
via Zoom

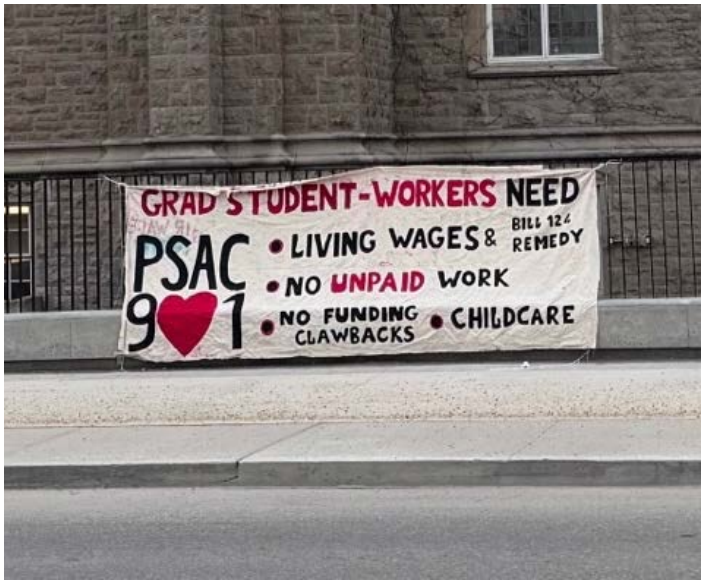
In accordance with the QUFA Constitution, Members will receive an official notice on 10 April 2025 and the Agenda on 17 April 2025.

This meeting will include elections for Executive Committee positions, and nominations are still open (please see the Nominations announcement on p. 4 of this issue of *QUFA Voices* for more information).

QUFA ALBUM

PSAC 901 Job Action

Members of PSAC 901, representing graduate Teaching Assistants, Teaching Fellows, and Postdoctoral Scholars at Queen's, have been on strike since 10 March 2025. On 21 March, a group called Concerned Queen's Faculty (CQF) held a rally and teach-in to support these striking workers (photos middle left and bottom). Striking PSAC 901 workers have been picketing outside the JDUC near Stauffer Library to make their presence known and to put pressure on Queen's Administration to negotiate a fair renewal Collective Agreement as soon as possible (photos right and middle right). QUFA stands in solidarity with PSAC 901 and hopes for a fair settlement very soon. Photos courtesy Robert G. May.



FYI

Endpoint Protection: Consequences and Recommendations

What QUFA Members need to know before enrolling their devices in Endpoint Protection

By Christian Muise
School of Computing

Wendy Powley
School of Computing

James Stewart
School of Computing

and Catherine Stinson
School of Computing

Devices used by Queen's faculty to access Queen's protected resources must soon be enrolled in the Endpoint Protection Program (EPP), requiring software installation that allows Queen's Information and Technology Services (ITS) to ensure compliance with security standards.

While this program is intended to enhance security, the software raises significant user privacy concerns, as well as concerns about how it will affect the way we work. We urge all QUFA Members to understand the potential risks before installing this software on any device that is for personal use, or on which you are storing highly confidential information.

Levels of Protection

There are two different levels of protection depending on which Queen's resources you need to access on your device:

- **Microsoft (MS) Intune**: Required for accessing MS 365 (e-mail, calendar, MS Office, etc.).
- **MS Defender for Endpoint (MDE)**: Required for finance, HR, PeopleSoft, and other protected Queen's resources.

Both levels require installation of software on any device used to access Queen's tools, including personal devices.

Key Concerns

Please note that the information contained in this article comes from Microsoft documentation. We are not privy to the actual details of Queen's installation or configuration of MS software. There are also important differences in how the software works on different types of devices and with different operating systems.

- **Full Device Access:** MDE allows authorized administrators to execute scripts remotely, enabling them full access to the device, including downloading files, changing configurations, installing software, and more.[1] Access can be made without device owner permission, and by anyone who has been granted permission. Paul Muir, Queen's Information Security Officer, has noted that the capability exists to access private user data, but simply assures us that ITS employees are professional and would not violate our rights.[2]

- **Software and App Exposure:** MS Intune and MDE provide administrators with a list of installed applications,[3] potentially revealing personal information, such as dating or gambling habits, or identifying communities with whom a person identifies.

- **Microsoft's Access to Data:** As a cloud-based solution, data collected is accessible not only to Queen's ITS, but also to Microsoft. The country in which the data is stored remains unclear.

GET INVOLVED

QUFA Executive Nominations Are Open!

This year's Nominations Committee comprises:

- **Diane Beauchemin** (Chair)
- **Lorena Jessop** (Executive Committee Member and Continuing Adjunct)
- **Dan Cohen** (Council Member)
- **Trisha Lawson** (Council Member)
- **Diane Beauchemin** (General Member)
- **Susan Lord** (General Member)

The Executive positions up for nomination or election this year, per the cycle outlined in the QUFA Constitution (Article 9.2.vi) are:

- Vice President
- President
- Chair of the Political Action and Communications Committee (PACC)
- Term Adjunct Representative
- Member at Large (one of two positions)
- Health and Safety Representative
- Chair of Council (to be elected by Council in March or April)
- The Past President is appointed in this round

In addition, there is an off-cycle vacancy for a Continuing Adjunct Representative.

If you are interested in standing for election or you know of people interested to serve, please get in touch with Diane Beauchemin (diane.beauchemin@queensu.ca) or Leslie Jermyn (qufaed@queensu.ca).

- **Control Over Device Permissions:** MS Intune can modify permissions for location, camera, microphone, Bluetooth, Wi-Fi settings, software updates, and more without user consent,[4] thus increasing the possibility of remote monitoring without the user's knowledge or permission.

- **Personal Device Requirements:** With office phones removed and mobile phones being exempt from personal expense reimbursement (PER), most faculty will need to enrol personal devices to at least access their e-mail. You will be required to update your operating system when dictated by EPP, app permissions may be restricted, and your device will be deemed outdated and in need of replacement when it no longer meets system requirements. Certain devices, such as Chromebooks, have already been denied access.

- **Potential Attack Risks:** By linking all devices through the EPP to Queen's and Microsoft, vulnerabilities in MS Intune and MDE could expose all enrolled machines to potential cyberattacks.

Consequences

Mandatory Endpoint Protection undermines academic freedom, potentially granting Queen's (and Microsoft) access to research, intellectual property, and personal data. Privacy laws advocate for minimal data collection, yet the EPP does the opposite.

Queen's ITS has not detailed safeguards against employee misuse of access, including student workers who may potentially oversee faculty devices. Moreover, as surveillance expands in workplaces globally, this policy sets a concerning precedent for increasing administrative control over faculty digital activity.

While security is essential, requiring faculty to surrender personal device control is excessive. The same security goals could be met with less invasive solutions, such as mandatory antivirus software, without compromising academic freedom and personal privacy.

Recommendations

If the Endpoint Protection Program is enforced, faculty may need to adapt. We suggest the following:

- Use separate devices exclusively for Queen's applications. Do not enrol personal devices. This will mean moving between devices and potentially carrying two phones.
- Access Queen's tools via Windows Virtual Desktop (WVD) to avoid local enrolment. WVD allows access to Queen's protected resources by logging into a virtual machine. You will need to save files created or downloaded on WVD to OneDrive.
- Avoid storing personal data on enrolled devices, and limit personal tasks on these machines.
- Use alternative communication tools, such as Zoom, Slack, or Signal.

If the Endpoint Protection Program moves forward, we request the following of Queen's ITS:

- Faculty should have the same access as students to commonly used applications, such as e-mail, calendar, MS Teams, and MS Word, without mandatory device enrolment.
- If device enrolment is required for access to these applications, Queen's must provide faculty members with phones and compliant computer equipment. At a minimum, phones should be eligible for reimbursement through PER.
- HR access should be removed from the list of restricted applications. Faculty should have access their pay-stubs and T4 slips without being required to comply with policies they do not support.
- There should be a requirement that the device owner be notified of any access made to a device through Live Monitoring (which is the tool that provides full access to the device).
- There should be full transparency regarding the configuration and policies for access, not just a blanket request to trust without transparency.

Notes

[1]https://learn.microsoft.com/en-us/defender-endpoint/live-response

[2]https://www.queensjournal.ca/it-security-update-raises-red-flags-for-faculty-privacy/

[3]https://learn.microsoft.com/en-us/intune/intune-service/protect/privacy-data-collect

[4]https://learn.microsoft.com/en-us/intune/intune-service/user-help/what-info-can-your-company-see-when-you-enroll-your-device-in-intune

Christian Muise can be reached at christian.muise@queensu.ca.

Wendy Powley can be reached at wendy.powley@queensu.ca.

James Stewart can be reached at stewartj@queensu.ca.

Catherine Stinson can be reached at c.stinson@queensu.ca.

OPEN LETTER

Endpoint Protection: An Open Letter from the Faculty of Law

Queen's Law Faculty raise a host of important concerns about the Endpoint Protection Program in this open letter

By Erik S. Knutsen
Faculty of Law

Lisa Kelly
Faculty of Law

and Ashwini Vasanthakumar
Faculty of Law

The majority of the Law faculty at Queen's raised a series of concerns with the Endpoint Protection Program (EPP). EPP, as communicated in e-mails and Web information, appears to conflict seriously with our professional and regulatory duties as lawyers, our professional and legal duties as researchers, and our rights to privacy under the Canadian Charter of Rights and Freedoms.

The Conflict with the Professional Duty of a Lawyer

A key professional duty of a lawyer is to keep client information privileged and confidential. This duty is centred in our rules of professional conduct from the Law Society of Ontario, to which we must adhere. This includes adequate protection from unauthorized access to that information, or to the capability of its erasure.

As you can imagine, many of us offer legal advice to a variety of national and international figures and entities. This work enhances the public profile and impact of Queen's Law. Indeed, lawyers are expected to provide services *pro bono*, as part of our commitment to access to justice within the legal profession. Many of us work on and litigate highly controversial and politically sensitive matters, including but not limited to reproductive rights, war crimes and international criminal liability, immigration and refugee protection, corporate malfeasance, and political dissent. Many of the issues we deal with involve access to extremely confidential information involving national security, international security, trade secrets, protected data, proprietary data, private health information, privileged legal and litigation information and strategy, and information about the guilt or innocence of parties. Most of us are contacted because of our connection with Queen's and our Queen's profiles online, and as marketed by the university.

Additionally, to protect sensitive information, many faculty members use encrypted tools such as Proton Mail and Signal for more secure communications. As faculty at the School of Computing have stressed, "Endpoint protection would put that information not only in the hands of [Queen's] ITS workers, but also Microsoft, a US-based tech company."[1] Given the heightened state of surveillance today in the United States and globally, we are unable to surrender basic and fundamental privacy in our devices and with confidential sensitive information in such a fashion.

The current EPP plan, as it stands, is untenable with maintaining adherence to the Law Society of Ontario's Rules of Professional Conduct if such work at all is carried out on the same device (which of course it should be and would be, as these are the devices we are using for Queen's work). While some of these concerns are specific to the legal profession, we expect that many Queen's faculty and researchers may face similar conflicts with professional ethics.

QUFA VOICES

Voice Your Views!

If you have an opinion about anything you read in *QUFA Voices*, send us a letter to the editor!

mayr@queensu.ca

The Conflict with Research Obligations for Privacy

We are expected to do research as part of our jobs. Concomitant with that expectation is the ethical and legal agreement we make to hold research data confidential. We are stewards of that information, and we must agree to protect it through various research ethics processes at the university, with granting agencies and funders, as well as with international research programs and partners at other institutions with strict data compliance protocols. A majority of us perform and store our research results on devices that are "Queen's funded" (as that term has been defined under EPP).

To date, we have been given no guidance as to how EPP is to operate within the research context. It appears to be a breach of the very things we must ensure, as researchers, in terms of data privacy and control. We find it especially confounding that a research institution like Queen's would not have squarely addressed this issue with faculty up front, well before program rollout.

The Conflict with Charter Privacy Rights

Additionally, the EPP is in tension with the kinds of privacy rights and values

embodied in section 8 of the Charter of Rights and Freedoms. The Supreme Court of Canada has repeatedly held that digital devices reflect the core of our biographical privacy. Privacy must therefore be protected. Legal ramifications may flow from impinging privacy when there are other, less intrusive and equally (or more) effective ways of achieving the same objective.

In view of the fact that Queen's does not provide employees with office phones, it is safe to assume that most faculty members must use a "personal device" (as that term has been defined under EPP) to access some Queen's software, making these devices subject to at least stage-one Microsoft Intune installation requirements.

In the case of "Queen's-funded devices," the realities of modern life dictate that the vast majority of faculty members will use such devices for professional and personal uses, including storage of personal files and documents, sending of personal communications, and browsing of internet sites unrelated to work. In reference to this type of personal information stored or accessed on a "Queen's-funded device," Queen's ITS has issued the rather ambiguous statement, "As such, information that is considered personal may be created and stored on our endpoints, and thus protected by MDE."[2]

The legitimate purpose of the EPP is ostensibly to protect against unauthorized access, hacking, and malware. However, the level of invasive access that is made possible by EPP actually compromises security.

As faculty at the School of Computing have noted, EPP's "reach extends far beyond these legitimate [security] purposes. It allows access into your computer or phone's files and apps by both [Queen's] ITS staff and by Microsoft, as well as the ability to erase your data, and run scripts on your device, which effectively allows unlimited access." In an interview with the *Queen's Journal*, Queen's ITS information security officer Paul Muir admitted that "it's possible, in some cases, for, as with any system that is centrally managed, those with that privileged access to the system, such as the folks in IT Services, do have the capability of accessing information that may be for the end user."[3]

The degree of surveillance and access to the digital devices of Queen's faculty members under the current EPP policy is not provided for in our Collective Agreement. As such, this new program would violate the contractual and privacy rights of employees.

The Conflict with Indigenous Data Sovereignty

Several Faculty of Law members have engaged or are engaged in work with Indigenous people and communities on matters such as the revitalization of Indigenous laws, land claims, searching for the missing and disappeared Indigenous children from Indian Residential Schools and other colonial institutions, assisting families of missing and murdered Indigenous women and girls, and helping the wrongfully convicted.

Colonial institutions, including universities, have a long history of denying Indigenous peoples access to justice by controlling their data. This long history of disrespect and unauthorized use of Indigenous knowledge and data has created challenges for Indigenous people to access, reclaim, and control data collected and kept by institutions. It has also led to the misrepresentation and attempted erasure of Indigenous knowledge, laws, and data governance systems.

The current EPP, as it has been communicated, appears to conflict with Indigenous data sovereignty which refers to the right of Indigenous peoples to exercise ownership, control, access, and protection over their data that has been shared with faculty members in confidence and with restrictions on use, access, and dissemination. It would also conflict with the United Nations Declaration on the Rights of Indigenous Peoples and Queen's University's own Truth and Reconciliation Task Force's Final Report and recommendation to develop and strengthen relationships with Indigenous communities.

Practical Matters

As a practical matter, we question how it makes sense to mandate MS Intune or MS Defender for Endpoint for faculty, and yet the more than 40,000 students at Queen's are not enrolled but access the same system in the same ways. A quick glance at the protocols of other large Canadian institutions shows that the method of choice for protection of this nature appears to be forming internal safeguards (i.e., on the Queen's side, instead of on the "access" side), thus avoiding the quagmire of privacy and user issues, and frankly doing a better job for security as a result.

Notes

[1]https://qcaa.ca/wp-content/uploads/2025/02/endpoint-protection-.pdf

[2]https://queensu.service-now.com/esm?id=kb_article&sysparm_article=KB0012801

[3]https://www.queensjournal.ca/it-security-update-raises-red-flags-for-faculty-privacy/

Erik S. Knutsen can be reached at knutsen@queensu.ca.

Lisa Kelly can be reached at lisa.kelly@queensu.ca.

Ashwini Vasanthakumar can be reached at ashwini.vasanthakumar@queensu.ca.