PRS MATTERS

Revised: June 2025

Privacy in the Workplace: Understanding Your Rights and Responsibilities

In recent years, advances in information and surveillance technology have raised legitimate concerns about the ever-shrinking sphere of privacy in society. In Ontario's public schools, increasingly sophisticated methods of storing, recording, and exchanging information have made it much easier for school boards to gather information of a quality and quantity that would not have been possible only a few years ago. In this context, to what degree do ETFO members have an expectation of privacy in the workplace and at what point does the employer's access to data (for example, email correspondence) become a violation of the right to privacy?

Rights and Responsibilities

As outlined in PRS Matters bulletin Documentation and Personal Information Concerning Students, the two primary statutes that govern privacy and access to information in Ontario's public schools are the Freedom of Information and Protection of Privacy Act (FIPPA) and the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA). The Education Act also has provisions for the protection of student privacy, as well as search-and-seizure rights of school boards under certain circumstances. There are, however, well-established principles in statutes and case law, including a recent ruling from the Supreme Court of Canada, which underscore teachers' rights to be secure from unreasonable search and seizure pursuant to the Canadian Charter of Rights and Freedoms.

As with all statutory rights, there are limitations and corresponding responsibilities that seek to balance an employee's right to privacy (and the responsibility of the employer to safeguard it) with the right of a school board to access information that is necessary for the safe and effective operation of schools. Employers are also bound by collective agreement language that may contain provisions that address protection of personal data and access to information.

While the balance of these rights and responsibilities is case-specific, there are some general principles that members should be aware of to safeguard their privacy in the workplace.

- Members should follow school board policies pertaining to workplace privacy (e.g., IT usage, data protection).
- Communication using school board hardware should remain professional at all times. Members should refrain from conducting personal business on school devices and during working hours.
- Personal data to which members do not wish the employer to have access should not be stored on work devices or other school board property. Members are encouraged to ensure data is stored securely on personal devices or at home.
- Members should maintain clear boundaries between their personal and professional lives and are advised against sharing personal information – both in person and online – with parents, students, and community members.

Social Media

While ETFO members have a right to privacy in the workplace, a school board may have the right to investigate conduct – either by the member or others – that is captured on social media.

Educators are held to a high standard of conduct in both their work and personal lives, and our current digital world means members should expect that anything could be recorded and posted online. When a member's "offline" or even "off-duty" conduct ends up online, there may be legitimate grounds for discipline if that conduct undermines public confidence in the school board. Even if a member takes care to enable privacy settings on a social media post, if the post is easily traceable to the school board and could cause reputational damage to the board, the member is not immune to discipline.

School boards also have a duty to ensure that members of the school community are not misusing social media to intimidate, demean, or threaten employees. Under the Occupational Health and Safety Act, employers must protect their employees from harassment and bullying that occurs on social media. Although online harassment may take place outside of school, the school board still has a duty to investigate if the harassment arises from or negatively impacts the school environment. Whether the source of the harassment is a student, parent, or another employee, the school board must intervene, up to and including reporting such incidents to the police. School boards have a greater obligation to protect members if the harassment occurs on social media operated by school administrators or the board itself (e.g., school-run Facebook groups for parents).

Members should also be conscious of Policy/Program Memorandum 128 (PPM 128), which establishes that members of school communities – including parents, students, administrators, and other school board employees – are not permitted to record, take, or share non-consensual recordings or photos of other school community members. If recordings or photos are required as part of a member's professional duties, the purpose should be made clear, they should be used only when parents explicitly provide consent and only for the purpose for which consent was provided, and they should not be captured or stored on personal devices. Instead, they should be securely stored on employer-provided devices and deleted as soon as they have served their purpose.

Surveillance

The Education Act affords principals the right to engage in search and seizure if there is reason to believe the safe operation of a school may be at risk. While there are limits to the employer's ability to engage in surveillance without good reason, ETFO members should always be mindful of the greater potential for surveillance when communicating in a forum or using a tool owned or operated by the school board (e.g., school board laptops, cellphones, email, and digital platforms).

While employees have a greater expectation of privacy when using personal devices during work hours, particularly on platforms not owned or operated by the school board, members should always ensure they are conforming with applicable school board policies as well as the Ontario College of Teachers' professional standards and standards of practice.

Tips and Best Practices to Maintain Privacy

Even outside of the workplace, members should be aware of the potential for surveillance. Even if an account is private, advertisers and scammers can still secure access to sensitive data. To protect yourself online, it is important to limit the amount of information shared and to adjust privacy settings accordingly. In addition, the following steps are recommended to safeguard privacy both within and outside of the workplace.

Artificial Intelligence

Be sure you understand how your information is being used by platforms. To prevent your data being acquired by Artificial intelligence, each social media platform has opt-out settings that can be activated for this purpose.

Content

Don't overshare. Avoid providing more details than necessary. Users shouldn't have to share an address or date of birth to be on most platforms. In addition, keep your work and personal activity separate. Don't use personal accounts for school-based activity and don't use school board accounts for personal social media activity.

Devices

When using a shared device, remember to log out and delete your browsing history when you are finished.

Links

Don't click on suspicious links. Even if the link appears to be from someone you know, avoid clicking on links unless it is from a trusted source.

Passwords and Security

Use strong passwords and don't reuse passwords across multiple programs or websites. Using multi-factor authentication, such as passcode and biometric recognition, is also recommended to add an additional layer of security to the application being used.

Privacy Policy

Become familiar with the privacy policies of the social media platforms you want to join. In reading a social media policy, be sure to understand what information the organization is collecting, how they are using it, and to what other organizations it is being disclosed.

Understand and Manage your Privacy Settings

Find out how to adjust your privacy settings and customize them so that information is shared only in ways you want it to be.

While this document provides an overview, it is not a comprehensive guide. Please contact your ETFO local or provincial staff in Professional Relations Services (PRS) for support with specific concerns.

JT:MMC

Elementary Teachers' Federation of Ontario
Fédération des enseignantes et des enseignants de l'élémentaire de l'Ontario
136 Isabella St, Toronto ON M4Y 0B5
Tel: 416-962-3836 / Toll Free: 1-888-838-3836 / Website: etfo.ca

ETFO FEEO