IATSE Local 873 Privacy Code

Effective: June 2025

Introduction

Protecting personal information is a core principle in negotiating contracts, managing membership, and administering our organization. IATSE Local 873 recognizes the importance of safeguarding personal information and is committed to collecting, using, and disclosing such information responsibly. We strive to be transparent in how we handle personal data.

Although it is not definitively established that organizations like ours fall under the Personal Information Protection and Electronic Documents Act (PIPEDA), we believe privacy is critical and have adopted this Privacy Code to comply with PIPEDA's ten foundational principles.

PIPEDA governs the collection, use, and disclosure of personal information. The term "personal information" is broadly defined under the Act as "information about an identifiable individual," but excludes an employee's name, title, business address, or business telephone number.

This policy outlines how we protect sensitive personal data, including financial and health-related information.

---

1. Accountability

IATSE Local 873 is accountable for the protection of personal information relating to both members and staff. While overall responsibility rests with the officers of the Local, day-to-day compliance is managed by staff, committee members, and the Executive Board.

The designated Privacy Officer is responsible for ensuring compliance with this policy. We use appropriate safeguards—including contractual agreements with third parties—to ensure personal information shared externally is handled in accordance with this Privacy Code.

While we employ security measures to protect sensitive information during electronic communications, members are advised that confidentiality cannot be fully guaranteed when using email or wireless technologies.

We continue to develop and implement procedures to:

- Protect personal information
- Handle complaints and inquiries

- Train staff, Executive Board, and Committee Members
- Communicate our policies to members, employers, and staff

---

2. Purpose of Collecting Personal Information

We collect personal information to:

- Communicate with members
- Provide employers with a means to contact members
- Administer and enforce the terms of our collective agreements
- Deliver member benefits
- Support workplace health and safety
- Promote the membership
- Manage the collection of dues and other payments

Should any new purpose for collecting personal information arise, members will be notified.

Much of this data is collected, used, and disclosed electronically. Our website uses cookies to deliver services to members, staff, and employers. (See the Supporting Documentation for a full explanation of cookies.)

A detailed list of personal information collected, the purposes for its use, and information retention and disposal practices is available upon request to the Privacy Officer.

---

3. Consent

Consent may be expressed, implied, or given through an authorized representative (such as a lawyer or agent), and may be provided orally, in writing, or electronically.

We will obtain consent before collecting, using, or disclosing personal information, except in the circumstances outlined below or where permitted by law.

Given the established relationship between the Union and its members, we consider consent to be implied for purposes outlined in this policy.

If our purposes for collection, use, or disclosure change, we will inform you in writing and seek new consent.

Withdrawal or Refusal of Consent

You may withdraw or refuse consent at any time, subject to legal or contractual limitations, by providing reasonable notice. Doing so may affect our ability to provide certain services to you or to employers.

If you disable cookies or set your browser to high privacy settings, you may be unable to access some website features. Alternatives include:

- Adding the IATSE Local 873 website to your browser's exception list
- Using cookie management software

If you prefer not to access services online, you may contact the office directly for printed materials.

We may collect, use, or disclose personal information without consent in limited cases outlined in Section 7 of PIPEDA, available upon request.

---

4. Limiting Collection of Personal Information

We only collect personal information necessary for the identified purposes using lawful and appropriate methods.

---

5. Limiting Use, Disclosure, and Retention

Personal information is used or disclosed solely for the purpose it was collected unless otherwise authorized by consent or required by law.

Information is retained only as long as necessary to fulfill its purpose or to meet legal requirements. Redundant data is deleted, shredded, or securely destroyed.

---

6. Accuracy

We take reasonable steps to ensure that personal information is accurate, complete, and current. Members and staff are expected to keep their own information (e.g., contact details) up to date.

---

7. Safeguards

We use appropriate safeguards based on the sensitivity of the information to prevent unauthorized access, use, or disclosure. These safeguards may include:

- Physical measures: locked cabinets and restricted office access

- Organizational measures: access granted on a need-to-know basis
- Technological measures: password protection and encryption
- Contractual measures: privacy agreements with third-party service providers

---

8. Openness

We are transparent about our privacy policies and procedures. Upon request, we will provide:

- The name and contact details of the Privacy Officer
- A description of the personal information we collect and its uses
- A copy of our Privacy Code or other relevant documentation
- Information about disclosures to affiliated or related organizations

---

9. Social Media – Guidelines for Professional Use

When using social media in a professional context:

- Do not share, collect, or disclose personal or confidential information
- Avoid discussing work-related details that are not publicly available
- Use unique passwords for social media accounts and refrain from downloading unsafe content
- Maintain professionalism in tone and conduct
- Avoid commenting on IATSE policy or political matters
- Do not use the IATSE logo, word mark, visual identity, or other branding that implies you represent the Local

Members should familiarize themselves with acceptable social media practices. Please note: unless formally designated, you are not authorized to represent the Local publicly.

---

10. Individual Access

Members and staff may request access to their personal information by submitting a written request to the Privacy Officer.

Upon verification of identity, individuals will be informed of the existence, use, and disclosure of their data and may request corrections if needed. Access will be provided within 30 days and at minimal or no cost, unless an extension is necessary for consultation or processing.

Access may be limited in some cases, such as where:

- Information pertains to other individuals
- Disclosure poses legal or security concerns
- Information is protected by solicitor-client or litigation privilege
- Requests are unreasonably costly

---

11. Challenging Compliance

Members and staff have the right to challenge our compliance with this Privacy Code.

Complaints or inquiries should be submitted in writing to:

Privacy Officer
IATSE Local 873
82 Carnforth Rd.
Toronto, ON M4A 2K7
humanresources@iatse873.com

We will review and respond to all concerns within a reasonable timeframe.