APPROVED DECEMBER 13, 2005
Reviewed and Confirmed by the Board May 10, 2011
Reviewed, amended and adopted by the Board February 2, 2016
Reviewed, amended and adopted by the Board March 2, 2018
Reviewed, amended and adopted by the Board March 10, 2020

Sheet Metal Workers Local 30 Benefit Trust Funds

Privacy Policy

Background

The **Sheet Metal Workers Local 30 Pension Trust Fund and Plan and the Sheet Metal Workers Local 30 Welfare Trust Fund and Plan** (herein after referred to as either the "Funds/funds/Fund/fund" or "Plans/plans/Plan/plan") provide pension and health care benefits to covered members, their families and in some cases to others, including the determination of eligibility for benefits. The Trustees and their agents collect, use, disclose and retain personal information in the management of the Plans. Certain of that personal information is protected under the federal Personal Information Protection and Electronic Documents Act ("PIPEDA"). PIPEDA applies to the Trustees and their agents to the extent that they collect, use or disclose personal information and personal health information in the course of their activities. In addition, certain personal health information, which may be collected in connection with the determination of eligibility for a benefit under a plan, may be protected under Ontario's Personal Health Information Protection Act ("PHIPA").

Privacy Statement

The Trustees are committed to protecting the privacy of the Plans' members, dependants and beneficiaries including the confidentiality of their personal information and personal health information in compliance with all applicable legislation.

Application and Scope of the Privacy Policy

In order to provide benefits, including the determination of eligibility for benefits, the Funds and Plans collect, use, disclose and retain personal information that may be protected under applicable legislation.

The Privacy Policy of the Funds and Plans applies to:

a) The Board of Trustees.

b) Any third party retained by the Boards of Trustees that collects personal information or to whom personal information is given.

Personal information may be collected for the purpose of administration of the Funds and Plans includes the following information about any active, retired, deceased or terminated member and any member's spouse, child, dependant and beneficiary who is, may be, or was eligible for benefits:

- Name
- Date of birth
- Social insurance number
- Marital status
- Income
- Dependant status
- Dental and health prognosis and treatments
- Medical test results
- Nature of a disability and its occurrence.

The protection of personal information will be governed at all times by the federal Personal Information Protection and Electronic Documents Act (PIPEDA) as amended from time to time, the Ontario Personal Health Information Protection Act (PHIPA) and any other applicable legislation.

Privacy Procedures

Recognizing that the Trustees, and other third parties retained by them in the course of operation and administration of the Plans and Funds, will come into possession of personal information (including personal health information) relating to Plan members, dependants and beneficiaries, the Trustees have implemented the following procedures:

1. The Trustees will ensure that they and their agents request only the personal information necessary for the purposes of administering the Plans in accordance with the applicable Plan text, trust documents, legislative requirements, the Trustees' fiduciary and other legal obligations.

2. The Trustees will ensure that the administrative practices established for the Plans provide that members or others providing personal information about themselves or their dependants, give their consent for the collection, use, disclosure, retention and, when such information is no longer needed for the management of the Plans, destruction of personal information.

   Whenever practical, the Trustees will obtain consent and receive personal information in writing, using forms appropriate for such purposes. These forms may include pre-printed enrolment and application forms, claims forms, remittance forms from employers, identification documents (birth or citizenship certificates, passports and drivers' licences), medical reports and death certificates. Consent will not be accepted from third parties, unless the person giving consent is an authorized legal representative or guardian (for example a parent of a dependent child or someone who has a current power of attorney).

3. The Trustees will allow personal information to be collected, used, disclosed and retained without consent, where medical, legal or security reasons make it impossible or impractical to obtain consent, or where the collection, use or collection, use and disclosure is permitted without consent under applicable legislation or by law.

4. The Trustees will use personal information only for the purpose of administering the Plans. Such uses may include, but not limited to:
   - Determining eligibility and enrolling new members in the Plans
   - Preparing benefit statements for Plan members and beneficiaries
   - Calculating and paying benefits
   - Assessing and adjudicating claims and appeals
   - Responding to inquiries from members and beneficiaries and
   - Making decisions relating to the administration of the Plans for which the use of such information is necessary.

5. The Trustees will disclose personal information only to the extent necessary for the proper administration of the Plans, including making benefit payments, reporting benefits paid, income tax reporting, and determining and resolving conflicting benefit claims. Entities to whom the Trustees may disclose information include, but are not limited to:
   - Financial institutions, including insurance companies and banks
   - Insurers, re-insurers and insurance brokers
   - Health care providers and facilities, including clinics and hospitals
   - Provincial health insurance plans
   - Federal or Provincial government agencies, including the Canada Revenue Agency
   - Investigative, second opinion and security agencies retained by the Trustees
   - Legal counsel or law enforcement agencies
   - Other trust funds and their administrators and
   - Other unions.

6. The Trustees will protect personal information by employing security safeguards which are appropriate to the sensitivity of the information in their possession, and personal information that is in transit by way of mail, email, fax or other mode of delivery

7. The Trustees will ensure that any third party retained by the Trustees to provide services to the Plans is bound, in writing, to comply with applicable legislation protecting personal information. For greater certainty, this procedure applies to the following suppliers to the Funds and Plans:

   - The actuary
   - The administration services provider
   - The auditor

- Legal counsel
- Consultants
- Financial Institutions including the custodian, banks or payroll processing firms
- Insurers and re-insurers
- Parties to reciprocal agreements
- Sheet Metal Workers Union Local 30 and any of its staff or programs managed by it
- Contributing employers and their organizations
- Any other organization retained by the Trustees and which will or may have access to the personal information of the Plans' members and/or dependants.

8. The Trustees are committed to transparency. Plan members will be given access to the Privacy Policy via the Plans' website. In addition, Plan members will be allowed to review the personal information on file for them. Plan members will be allowed to advise the Trustees, or anyone holding the applicable personal information, if the information is not accurate. When inaccurate information is found, the Trustees will ensure that it is corrected.

9. Applicable Fund and Plan documents will contain a summary of the Privacy Policy.

10. Plan members will be informed about the Plans' Privacy Officer and how to contact the Privacy Officer.

11. Appeals will normally be considered without any information that would identify the member. The Trustees however note that Plan members may make themselves known to the Trustees or a Trustee and if this is the case the Trustee will make a disclosure to the other Trustees that he/she is aware of the member's identity and will not share that identity with the Trustees full consent from the member is obtained. The Trustees are of the opinion that knowledge of the member's name is not relevant to an appeal.

    In the case of Plan member appeals to the Trustees for re-consideration of a decision made by or on behalf of the Plan and the member wishes that his/her identity be given, the Trustees will require that the affected Plan member give consent for the Trustees to review personal information necessary for them to effectively consider an appeal.

12. The Trustees have appointed a Privacy Officer who is accountable to the Trustees for compliance with applicable privacy legislation and for the handling of Plan member inquiries. The Privacy Officer is Kimberly Houston, Managing Director for the Administration Services Provider.

13. A breach of the Privacy Policy will be handled by the Privacy Officer in compliance with the applicable legislation.

14. Schedule 1 is attached to and party of the Privacy Policy.

15. The Privacy Policy will be reviewed every two years or more frequently if necessary.

16. The Privacy Policy will be available to Plan members via the Plan's website.

Sheet Metal Workers Local 30 Benefit Trust Funds

PRIVACY POLICY SCHEDULE 1
Mandatory Notification Requirements of PIPEDA
Effective November 1, 2018

Organizations subject to the federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA") must notify affected individuals of a breach to the confidentiality of their personal information that results in real **risk of significant harm** to them.

PIPEDA regulations define **significant harm** as including "bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property."

The regulations require organizations to report all applicable breaches to the Privacy Commissioner of Canada ("the Commissioner") and to maintain records of all breaches involving personal information including those that do not meet the **real risk of significant harm** threshold.

Background

The factors that are relevant in determining whether there is a **real risk of significant harm** to an individual include:

a. the sensitivity of the personal information involved,
b. the probability that the personal information has been, is being or will be misused,
c. and any other prescribed factor. There are currently no other prescribed factors.

PIPEDA defines a "**breach of security safeguards**" as the loss or disclosure of personal information or the unauthorized access to personal information resulting from a breach of the organization's security safeguards or from its failure to establish such safeguards.

Impact on the Plan/Plans

In the event of an applicable breach, the Plan must:

- report the breach to the Commissioner (see Plan Notice to Commissioner below);

- notify the affected individuals; and
- notify government institutions, or other organizations if the Plan believes that the other organizations may be able to reduce the risk of harm to the affected individuals

Penalties

If the Plan fails to report privacy breaches to the Commissioner, fails to notify affected individuals of breaches affecting their personal information or fails to maintain records of such breaches it could be subject to fines of up to $100,000.

Plan Notice to Commissioner

PIPEDA requires that a report to the Commissioner be made as soon as feasible after the Plan determines that a privacy breach that resulted in a **real risk of significant harm** has occurred. The regulations require the report must be in writing, and be submitted via a secure means of communication, such as an encrypted email.

The Plan communication must contain at least the following:

- a description of the breach and its cause, if known;
- the date, or the period or approximate period, of the breach;
- a description of the personal information involved to the extent that it is known;
- the number, or approximate number, of individuals affected by the breach;
- a description of the steps taken by the Plan to reduce the risk of harm to those individuals;
- a description of the steps taken by the Plan, or intended to be taken, to notify the affected individuals; and,
- the contact information of the Plan's Privacy Officer who can answer the Commissioner's questions about the breach.

The regulations recognize that the full extent of a breach may not be known immediately. They permit, but do not require, the Plan to provide new information to the Commissioner following the initial reporting of a breach.

Notice to Individuals

PIPEDA requires that notice of a breach must normally be provided to affected individuals directly and as soon as feasible after the Plan determines that a breach has occurred. Notices must contain sufficient information to allow an individual to understand the significance to them of the breach and to take steps, where possible, to reduce the risk of harm or mitigate such harm.

The regulations require that at least the following information be included in such notices:

- a description of the breach;
- the date, or the period or approximate period, of the breach;
- a description of the personal information which was compromised to the extent that it is known;
- a description of the steps taken by the Plan to reduce the risk of harm to affected individuals;
- a description of the steps that affected individuals could take to reduce the risk of harm to them or mitigate such harm; and,
- the contact information of the Privacy Officer who will answer questions about the breach.

The regulations provide that notice may be given in person, by telephone, mail, email or any other form of communication that a reasonable person would consider appropriate in the circumstances. The form of notice should be documented so the Plan can address any future claim that no notice, or insufficient notice, was provided.

The regulations also provide that affected individuals can be notified indirectly if direct notice would likely cause further harm to the individual, cause undue hardship for the Plan/Plans, or if the Plan does not have contact information for the affected individual. Indirect notice must be given by public communication or by a similar measure that could reasonably be expected to reach the affected individuals such as a newspaper advertisement, posting in the workplace or on a relevant website.

The method of notice will be determined by the Privacy Officer and the Plan via the Recording Secretary with the Board of Trustees.

Breach Record Keeping

PIPEDA requires that the Plan maintain records of all breaches of its security safeguards, including those that do not meet the **real risk of significant harm** threshold, for 24 months from the date the Plan/Plans determined that a breach had occurred. These records must be available to the Commissioner upon request and must contain sufficient information for the Commissioner to determine whether the Plan complied with its notification and reporting obligations.

The records of breaches which did not satisfy the **real risk of significant harm** threshold should indicate how that determination was made.

Breach records are destroyed after 24 months unless the matter is the subject of

known litigation.

Depending on the information breach the Plan may pay the cost of cost of credit monitoring for affected individuals if the confidentiality of their financial information is breached. Different steps may be required if the confidentiality of personal medical information is breached. The determination will be made on a case by case basis by the Board of Trustees.

Encrypted Data

It is the policy of the Plan administrator to send confidential data in an encrypted format. However, many members /union officers and other stakeholders may not. Breaches involving encrypted data are not exempted from the notification and reporting requirements of PIPEDA.

The use of high-quality encryption may reduce the risk of harm to below the **real risk of significant harm** threshold so no notification or reporting would be required. In such circumstances, the Plan must maintain a record of the breach for 24 months.