CARPENTERS' RESIDENTIAL HEALTH AND WELLNESS PLAN, CARPENTERS RESIDENTIAL PENSION PLAN, CARPENTERS RESIDENTIAL LEGAL SERVICES PLAN, CARPENTERS AND ALLIED WORKERS LOCAL 27 SHINGLING & SIDING DIVISION GROUP RRSP TRUST FUND, CARPENTERS AND ALLIED WORKERS LOCAL 27 SHINGLING & SIDING DIVISION PRODUCTIVITY BONUS PLAN and CARPENTERS LOCAL 1030 VACATION PAY TRUST FUND

(the "Plans")

PRIVACY POLICY AND PRACTICES

Approved by the Board of Trustees: June 21, 2019

Privacy of Personal Information is the cornerstone of the Plans' administration procedures and policies. The Trustees understand the importance of protecting Personal Information. The Trustees are committed to collecting, using and disclosing Personal Information responsibly. The Trustees are committed to being open and transparent about the way the Plans handle Personal Information.

Personal Information is - Personal Information includes any factual or subjective Information, recorded or not, about an identifiable individual. This includes Information, in any form, such as:

- Social Insurance Number
- income
- ethnic origin
- personal address
- opinions, evaluations, comments, medical records

Personal Information is not - Personal Information does not include the title or business address, or business telephone number, of a Plan Member or person on whose behalf a contribution is received by the Plans.

The Trustees are aware of the sensitive nature of the Personal Information that Members have disclosed. The administration staff of the Plans are trained in the appropriate uses, and protection, of Personal Information. Together with the Trustees, those involved in the administration of the Plans ensure that:

- Only necessary Personal Information is collected;
- Personal Information is shared only with consent and as indicated in this Privacy Policy unless written notification from a Member is received allowing other disclosure;
- Storage, retention and destruction of Personal Information complies with applicable legislation;

- The Plans' privacy protocols comply with applicable privacy legislation and standards of the applicable regulatory authorities.

The Plans' practices adhere to the Pension Information Protection and Electronic Documents Act (PIPEDA). Specifically the Plans follow the code in Schedule I of PIPEDA that was developed by business, consumers, academics and governance under the auspices of the Canadian Standards Association (CSA) for the Protection of Personal Information. The hallmarks of our privacy practices are:

1. **Accountability** – The Plans are responsible for the Personal Information under its control. The Trustees have designated individuals who are accountable for the Plans' compliance with the Privacy Policy.

2. **Identifying Purposes** - The purposes for which Personal Information is collected shall be identified at or before the time the Personal Information is collected.

3. **Consent** - The knowledge and consent of the individual are required for the collection, use, or disclosure of their Personal Information, except where inappropriate.

4. **Limiting Collection** - The collection of Personal Information will be limited to that which is necessary for the purposes the Plans have identified. Personal Information will be collected by fair and lawful means.

5. **Limiting Use, Disclosure, and Retention** - Personal Information will not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal Information will be retained only as long as necessary for the fulfilment of those purposes.

6. **Accuracy** - Personal Information will be as accurate, complete, and up-to-date as is necessary for the purposes for which is to be used.

7. **Safeguards** - Personal Information will be protected by security safeguards appropriate to the sensitivity of the Personal Information.

8. **Openness** – The persons responsible for Plan administration will make readily available specific Information about its policies and practices relating to the management of Personal Information.

9. **Individual Access** - Upon request, an individual will be informed of the existence, use, and disclosure of his or her Personal Information and shall be given access to that Personal Information. An individual shall be able to challenge the accuracy and completeness of the Personal Information and have it amended as appropriate.

10. **Challenge Compliance** - An individual will be able to address a challenge concerning our compliance with the above Principles to the designated individual or individuals accountable for the Plans' privacy practices.

The Plans' Practices for Protection of Personal Information

The Plans will collect, use and disclose Personal Information for the following purposes:

- to confirm identity, and protect against errors, fraud or other misrepresentations;
- to determine eligibility for benefits;
- to ensure employer contributions are properly allocated;
- to administer and or confirm compliance with the applicable collective agreement and/or reciprocal agreement;
- to enable the Plans to contact necessary persons;
- to establish and maintain communication with Plan Members and other stakeholders;
- to comply with a variety of legal requirements, including any tax reporting obligations under the Income Tax Act;

Access to Personal Information will only be provided to:

- The Plans' administration staff who need the Personal Information for the performance of their duties to determine the benefit entitlements payable under the terms of the Plans;
- The Board of Trustees governing the Plans, if such Personal Information is required to permit them to carry out their fiduciary duties, including managing any appeal made in respect of a benefit determination of the Plans;
- The Local Union Offices or an agent of the Local Union, only to the extent that the Plan Member has authorized a response to one of the foregoing in relation to a benefit entitlement;
- The Local Union, or an agent of the Local Union, in respect of managing outward communication to Plan Members such as promotional material issued by the Local Union or Local Union newsletters or other general communication to Plan Members;
- The Local Union for the purpose of recognizing the Plan Member's service or retirement status, the latter when the retired Plan Member has provided authorization;
- The Local Union for the maintenance of employment records (dispatch) of Plan Members so that the Plans can, in turn, be informed by the Local Union when a Plan Member has been employed and so the Plans can anticipate contributions payable under a collective agreement;
- Insurance carriers or persons or firms in related businesses (such as electronic payment providers) in order to maintain Plan policies, coverage, authorize and make payments;
- Plan actuaries in order to determine benefit costs and entitlements;
- Legal counsel for the purpose of resolving benefit entitlements;
- Regulatory authorities in order to comply with applicable legislation, including field or site audits/reviews or other inquiries;
- Investigative agencies, particularly for the location of Plan Members, their dependants, actual or potential beneficiaries;
- Any other person or organization who has been given the necessary consent provided the consent has been communicated to the Plans in a form satisfactory to the Plans; and

- Anyone who is otherwise authorized by law.

The Plans will protect and store Personal Information by:

- Using Personal Information only for the purpose for which it is collected and keeping this Personal Information in the strictest of confidence;
- Maintaining electronic files and hard copies of Personal Information;
- Keeping hard copies of Personal Information locked in storage rooms and locked filing cabinets;
- Ensuring electronic systems are secure and require passwords;
- Ensuring only authorized Plans administration staff have access to hard copy or electronic records;
- Sending Personal Information electronically to other parties using encryption;
- Sending Personal Information to other parties by mail by marking documents "private"; and
- Maintaining and administration protocol which includes a system of file backup.

The Plans will not, under any conditions, supply medical history without specific written consent from the Plan Member unless required by law.

When requests are received for disclosure of Personal Information, if not covered under the foregoing rules, the Plans will contact the relevant person for permission to release such Personal Information.

Plan Members and others may withdraw consent for use or disclosure of Personal Information. The Plans will explain the ramifications of that decision.

PRIVACY STATEMENT

The Plans will include a Privacy Statement on appropriate Plan documents. The Plans' Privacy Statement is:

Privacy Statement: The Plans will collect, maintain and communicate only the Personal Information considered necessary for the administration of the Plans. Personal Information will be protected pursuant to the relevant legislation. The Plans may use and exchange information with relevant persons and organizations including the Trustees, institutions, investigative agencies, unions, insurers, re-insurers, auditors, legal counsel, actuaries, payroll/payment providers and regulatory authorities in order to manage the Plans and entitlement to the benefits of the Plans. Questions related to the Privacy Policy should be directed to the Benefit Administration Office.

Please be assured that the Trustees and all Plan administration staff are committed to providing excellent service. Plan Members, dependants and beneficiaries are invited to discuss the Privacy Policy with the Plans' Privacy Officer. If you have any questions or concerns about the Plans' Privacy Policy, please contact the Plans' Privacy Officer:

Kimberly Houston
Privacy Officer
Employee Benefit Plan Services Limited
45 McIntosh Drive
Markham, Ontario
L3R 8C7

Tel: 905-946-9700
Toll Free: 1-800-263-3564

Fax: 905-946-2535
Email: khouston@mcateer.ca
www.carpentersresidential.ca

CARPENTERS' RESIDENTIAL HEALTH AND WELLNESS PLAN,
CARPENTERS RESIDENTIAL PENSION PLAN,
CARPENTERS RESIDENTIAL LEGAL SERVICES PLAN,
CARPENTERS AND ALLIED WORKERS LOCAL 27 SHINGLING & SIDING DIVISION GROUP RRSP TRUST FUND,
CARPENTERS AND ALLIED WORKERS LOCAL 27 SHINGLING & SIDING DIVISION PRODUCTIVITY BONUS PLAN
and
CARPENTERS LOCAL 1030 VACATION PAY TRUST FUND

(the "Plans")

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 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.