45 McIntosh Drive, Markham, ON L3R 8C7 1-888-278-9003 questions@ndtbenefits.org www.ndtbenefits.org

NDT INDUSTRY HEALTH BENEFIT FUND

Privacy Policy

Approved by the Board of Trustees: November 27, 2025

The Board of Trustees of the NDT Industry Health Benefit Fund (the "Fund) and the NDT Industry Health Benefit Plan (the "Plan") is responsible for the good governance of the Plan and Fund.

Privacy of Personal Information is the cornerstone of the Plan's 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 and in compliance with all applicable legislation. The Trustees are committed to being open and transparent about the way the Plan handles Personal Information.

Personal Information - 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 Plan.

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

- Only necessary Personal Information is collected;
- Personal Information is obtained and shared only with consent when applicable 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 all applicable legislation;
- The Plan's privacy protocols comply with all applicable privacy legislation and standards of the applicable regulatory authorities, in particular, all applicable legislation dealing with privacy and health care records.

The Plan's practices adhere to the Personal Information Protection and Electronic Documents Act (PIPEDA) or other applicable law. Specifically, the Plan follows 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 the Plan's privacy practices are:

1. **Accountability** – The Plan is responsible for the Personal Information under its control. The Trustees have designated individuals who are accountable for the Plan's 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 Plan has 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 in accordance with prudent record retention practices.

6. **Accuracy** - Personal Information will be as accurate, complete, and up-to-date as is necessary for the purposes for which it 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 the Plan's administration will make readily available specific Information about the 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 their 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 Plan's privacy practices.

The Plan's Practices for Protection of Personal Information

The Plan 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 including evidence of ongoing disability where applicable;
- 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 Plan 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 Plan's administration staff who need the Personal Information for the performance of their duties to determine the benefit entitlements payable under the terms of the Plan. The Plan's administration office may communicate with service providers approved by the Board for carrying out certain duties such as the payment of Plan claims, review of disability, etc.;
- The Board of Trustees governing the Plan, 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 Plan;

- The participating Unions or an agent of the Union, only to the extent that the Plan member has authorized a response if required, including having copied one or more of the foregoing in relation to a benefit entitlement. The Union(s) may request information regarding a Plan member for the administration of a collective or other agreement impacting on the Plan or for ensuring compliance with a Plan policy;
- Insurance carriers, adjudication advisors, or persons or firms in related businesses (such as electronic payment providers) in order to maintain Plan policies, coverage, authorize and make payments;
- Plan auditor as necessary and data will be made anonymous wherever possible;
- Plan actuaries in order to determine benefit costs and entitlements;
- Legal counsel for the purpose of resolving benefit entitlements or disputes;
- Regulatory authorities in order to comply with applicable legislation;
- Investigative or related 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 Plan in a form satisfactory to the Plan; and
- Anyone who is otherwise authorized by law.

The Plan will protect and store Personal Information by:

- Being compliant at all times with prudent record retention practices;
- 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 a secure building, storage rooms, and locked filing cabinets;
- Ensuring electronic systems are secure and require passwords;
- Ensuring only authorized Plan's administration staff have access to hard copy or electronic records;
- Encouraging members and others to send Personal Information to the Plan in an encrypted format or marked "private";
- Sending Personal Information electronically to other parties using encryption;
- Sending Personal Information to other parties by mail by marking documents "private" or encrypted; and
- Maintaining and administration protocol that includes a system of file backup.

The Plan will not, under any conditions, supply medical history without specific written consent from the Plan member unless required by law or when provided to an authorized provider to the Plan for the purpose of determining eligibility for benefits.

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

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

REPORTING OF PRIVACY BREACHES

The Plan will follow the protocol in the attached Schedule 1 - Mandatory Notice Requirements of PIPEDA.

PRIVACY STATEMENT

The Plan will include a Privacy Statement on appropriate Plan documents. The Privacy Statement was prepared in collaboration with legal counsel. The Plan's Privacy Statement is:

> By signing below, I hereby certify that the Information provided is true to the best of my knowledge and consent to the collection, maintenance, use, and disclosure of my personal Information as described in the Privacy Statement below. I acknowledge that providing my consent will allow access to the Information required to assess my benefit eligibility and entitlement, and that refusing to consent may result in delay or denial of my request and/or benefit. This consent may be revoked by me at any time by sending written instructions to the Plan's Administration Office.
>
> I consent to the collection, use, and disclosure of my personal Information
>
> ___YES ___NO
>
> _____
>
> Signature and Consent Date
>
> Privacy Statement: I authorize the NDT Industry Health Benefit Plan ("the Plan"), its administrator McAteer-Employee Benefit Plan Services Limited, and providers working with the Plan or administrator to collect, maintain, use and disclose my personal Information that is necessary for the administration of the Plan. Personal Information will be protected pursuant to the applicable legislation. The Plan may collect, maintain, use and disclose my personal Information with relevant persons or organizations (employer, health benefit managers, health

professionals, institutions, insurers, investigative agencies, legal counsel, the union, pharmacies, regulators, re-insurers) in order to manage the Plan and entitlement to the benefits of the Plan, and may include Information such as financial, health or benefits related Information. Questions related to the Privacy Statement should be directed to the Privacy Officer.

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 Plan's Privacy Officer. If you have any questions or concerns about the Plan's Privacy Policy, please contact the Plan's Privacy Officer:

North America:
Ryan Laird, Communications Consultant
NDT Industry Health Benefit Plan
Administration Office
45 McIntosh Drive
Markham, Ontario
L3R 8C7

Tel: 905-946-9700 x 232
Toll Free: 1-800-263-3564

Fax: 905-946-2535
Email: rlaird@mcateer.ca

Review:

This Policy is reviewed every two years or more frequently if necessary.

Transparency:

This Policy is available to members via the Plan's website www.ndtbenfits.org.

PRIVACY POLICY SCHEDULE 1

Mandatory Notification Requirements of PIPEDA Effective January 1, 2026

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 to the Privacy Commissioner of Canada ("the Commissioner") all applicable breaches that result in real risk of significant harm, 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; and
c. 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

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

- report the breach to the Commissioner if applicable (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 applicable 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 to 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 resulting in a real risk of significant harm 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, or if the Plan does not have contact information for the affected individual. Indirect notice shall 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.

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 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.

Notwithstanding that a breach is not reportable, it will be reported to the Privacy Officer as part of the breach record-keeping protocol.

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 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.