1-800-774-5070 toll free
(902) 424-5070 local
(902) 424-0662 fax
e-mail: pensionsinfo@nspension.ca
www.novascotiapension.ca

Privacy Policy

1.0 Policy Statement

Nova Scotia Pension Services Corporation ("Pension Services Corp.") is committed to taking all reasonable steps and precautions to protect the privacy of all members, pensioners, and beneficiaries whose Personal Information is under the administration, possession, and control of Pension Services Corp. Pension Services Corp. will adhere to the privacy protection provisions of applicable legislation as relating to the collection, use, disposal, storage and disclosure of Personal Information. Pension Services Corp. utilizes as a guideline the principles established within the *Canadian Standards Association Model Code for the Protection of Personal Information* supported by the *Personal Information Protection and Electronic Documents Act ("PIPEDA").* In addition to Pension Services Corp.'s dedication to the protection of Personal Information, the corporation recognizes the obligation to protect confidential non-Personal Information of Pension Services Corp. and of the Plans and Funds. These obligations, as well as reference to this policy, are included within Pension Services Corp.'s Code of Business Ethics and Conduct for Employees which is agreed to and signed by all Employees on an annual basis. This policy does not apply to the Personal Information of Employees, in respect of their employee relationships with Pension Services Corp., as such Employees are covered by other policies.

2.0 Definitions

For the purposes of this policy, the following definitions apply:

BOARD
The Board of Directors of Pension Services Corp.

CONFIDENTIALITY AGREEMENT
Appendix C of the Pension Services Corp. Code of Business Ethics and Conduct for Employees, requiring all Employees to read and sign on an annual basis.

EMPLOYEE
An individual in the employ of, seconded to, or under personal service contract with Pension Services Corp. (e.g. temporary workers, and interns who have access to Records).

EXTERNAL PARTIES
Includes any

(i) individual(s) and/or corporation(s) or other entities that are not a member, pensioner, beneficiary of any of the Plans;

(ii) individual(s) and/or corporation(s) or other entities that are not an employer of current or previous members;
(iii) individual(s) and/or corporation(s) or other entities that are not Service Providers currently contracted with Pension Services Corp.

FUND
The Nova Scotia Teachers' Pension Fund and the Public Service Superannuation Fund.

PERSONAL INFORMATION
Includes information about an identifiable individual, for example, date of birth, social insurance number, income, home address, marital status, contributions, salary, eligible pensionable service, and medical information, but does not include
(i) the position name or title, business address, business telephone number, business fax number, or business e-mail address of a member, pensioner, or beneficiary of one of the Plans when such business contact information is used for the purpose of communicating or facilitating communication with a member, pensioner, or beneficiary in relation to their employment;
(ii) information that is publicly accessible.

PLANS
The Nova Scotia Teachers' Pension Plan, the Public Service Superannuation Plan, the three former Sydney Steel plans, and the Members' Retiring Allowance (MLA) plan.

PRIVACY BREACH
Unauthorized collection, access, use, disclosure, alteration or disposal of Personal Information.

PRIVACY OFFICER
Designated as the Director, Enterprise Risk & Compliance, responsible for Pension Services Corp.'s compliance with this policy.

RECORD
As defined in PIPEDA, includes any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microform, sound recording, videotape, machine-readable record, and any other documentary material, regardless of physical form or characteristics, and any copy of any of those things.

SENIOR MANAGEMENT
Includes the Chief Executive Officer and President ("CEO"), Chief Investment Officer ("CIO"), Chief Pensions Officer ("CPO"), Director of Information Management & Technology, Director of Financial Services, and Director of Human Resources.

SERVICE PROVIDERS
Means any individual(s) and/or corporation(s) currently contracted under a service agreement with Pension Services Corp.

TRUSTEES
Nova Scotia Teachers' Pension Plan Trustee Inc. and Public Service Superannuation Plan Trustee Inc.

3.0 Policy Objectives

The policy is designed to ensure that Pension Services Corp. meets its legislated and ethical obligations in its management and protection of Personal Information throughout the information's life cycle. This includes ensuring the protection of Personal Information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposition.

4.0 Application

This policy applies to:

- all Employees
- all Personal Information in the custody and control of Pension Services Corp.

5.0 Principles

1. **Accountability:**
   - ✓ Pension Services Corp. is accountable for all information under the control of Pension Services Corp., including information disclosed to Service Providers for processing.
   - ✓ The Privacy Officer and the CEO are accountable for Pension Services Corp.'s compliance with this policy.
   - ✓ External Parties requesting non-public Plan or Fund information will be directed to the CEO who will evaluate the request, respond directly, or consult with the Board and/or the respective Trustee on an appropriate response.

2. **Identifying Purposes of Collection:**
   - ✓ Pension Services Corp. will identify, where reasonable, the purposes for which Personal Information is collected at or before the time the information is collected.
   - ✓ The purposes for which Pension Services Corp. collects Personal Information will be those that would be considered reasonable given the responsibilities of Pension Services Corp. Such purposes include, but are not limited to, the administration of the Plans, Funds, pensions and benefits of members, pensioners, and their beneficiaries, and communication of information to said parties.

3. **Obtaining Consent:**
   - ✓ Pension Services Corp. will obtain consent of the respective member, pensioner, or beneficiary as required or permitted by law for the collection, use, or disclosure of Personal Information related to that individual, except where inappropriate and in the best interests of the individual (eg. individual is seriously ill or

incapacitated), prohibited by law, or as set out in section five (5), Limiting Use, Disclosure, and Retention, below.

- ✓ The form of the consent may vary depending on the circumstances and the type of Personal Information.
- ✓ Consent is only valid if it is reasonable to expect that the member, pensioner, or beneficiary, to whom Pension Services Corp.'s activities are directed, understands the nature, purpose, and consequences of the collection, use, or disclosure of the individual's Personal Information. For example, a member, pensioner, or beneficiary's consent is implied in situations where reasonable expectations are applicable such as enrolment in one of the Plans.

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

5. **Limiting Use, Disclosure, and Retention:**
   - ✓ Personal Information of members, pensioners, and beneficiaries is confidential and will not be used or disclosed (electronically, verbally, etc.) for purposes other than those for which it was collected, except when:
     - the consent of the same member, pensioner, or beneficiary is received;
     - required or permitted by law;
     - required by a government institution or the member, pensioner, or beneficiary's next of kin or authorized representative if there are reasonable grounds to believe that the member, pensioner, or beneficiary is suspected of, has been the victim of, or is suspected of having been the victim of financial abuse or fraud and where it is reasonable to expect that obtaining the consent from the member, pensioner, or beneficiary for the disclosure would compromise the ability to prevent or investigate the abuse or fraud.
     - required by a Service Provider while acting under a duty of confidentiality (e.g. Auditors); or
     - requested by the member or pensioner's current and/or previous employer and under any of the following circumstances:
       - the employer would reasonably have or have had such information on file for the member as part of the employer/employee relationship;
       - the requested information was originally provided to Pension Services Corp. by the requesting employer as part of Pension Services Corp.'s regular administration of such employer's pension plan;
       - the requested information does not contain pension-specific information (eg. selected survivor option) provided by the member or pensioner directly to Pension Services Corp. in confidence that can be connected directly to an individual member or pensioner; or
       - the requested information does not contain Personal Information of pensioners.

- ✓ Personal Information will be retained only as long as necessary for the fulfillment of the purposes for which it was collected, and as Pension Services Corp. requires in order to satisfy potential legal obligations.

6. **Accuracy of Personal Information:**
   - ✓ Pension Services Corp. will keep Personal Information as accurate, complete, and up-to-date as is reasonably possible for the purposes for which it is to be used and for which the Personal Information is under the control of Pension Services Corp.
   - ✓ It is expected that members, employers, pensioners and beneficiaries will make all reasonable efforts to provide accurate, complete, and up-to-date Personal Information.

7. **Safeguards:**
   - ✓ Senior Management will ensure there are current policies and procedures in place concerning the administration of Personal Information and other confidential information that is collected, stored, accessed, processed or disposed of within its custody and control. The safeguarding measures include physical and technological controls as well as audit and educational measures.

8. **Openness:**
   - ✓ Pension Services Corp. will be open about its Personal Information policies, process and practices.
   - ✓ This policy will be made readily available and will be posted on Pension Services Corp.'s internet website.

9. **Providing Access to Personal Information:**
   - ✓ Upon request and with appropriate verification of identity, Pension Services Corp. will provide a member, pensioner, or beneficiary access to their own Personal Information, except where Pension Services Corp. is required or permitted by law not to do so, and in conjunction with section five (5), Limiting Use, Disclosure, and Retention, above.
   - ✓ Requests for access to a member, pensioner, or beneficiary's own Personal Information will be managed by the respective Pension Services Corp. manager and/or their designated representative. Pension Services Corp. staff may require a reasonable amount of time to process requests for access as staff are required to perform a diligent review prior to providing access to Personal Information.

10. **Questions of Corporate Compliance:**
    - ✓ Individuals may contact Pension Services Corp.'s Privacy Officer with questions or concerns surrounding Pension Services Corp.'s compliance with this policy at the following address: PensionsInfo@nspension.ca
    - ✓ Pension Services Corp. will adopt a Privacy Breach Protocol (appendix) intended to assist Employees in their response to the discovery of a Privacy Breach and/or a complaint from an individual about a perceived Privacy Breach.

6.0 Policy Guidelines

1. The Director of Human Resources will ensure that all new Employees receive a copy of this policy in an orientation package, and duly execute the Confidentiality Agreement.
2. Pension Services Corp. managers will be responsible for incorporating the objectives of this policy during the training of new Employees as well as delivering on-going reminders and examples to staff, supporting the principles and guidelines of this policy.
3. Access to Pension Services Corp.'s premises must be controlled at all times to prevent unauthorized access to Personal Information and other confidential information.
4. Computers must be locked while Employees are temporarily away from their office or work station.
5. All files must be secured after business hours. As a minimum, offices should be locked if confidential files have to 'stay out' overnight. All files containing Personal Information or other confidential information of members, pensioners, and beneficiaries, should be located within the central filing room; otherwise, the exact location of such files should be accounted for and such files 'locked away' overnight.
6. Files containing Personal Information must not be removed from the premises of Pension Services Corp., and disposal of both transitory and master Records will only be carried out by an authorized records management professional in accordance with the established disposition policy and procedures.
7. Pension Services Corp. will perform a diligent review when providing information to an individual so as not to include Personal Information belonging to another member, pensioner, and/or beneficiary. .
8. Any uncertainty regarding a response to an employer's request for member information will be brought to the attention of the Manager of Employer Services, Manager of Client Services, or the Chief Pensions Officer for further review.
9. Pension Services Corp. will impose the same standards and controls with any of its Service Providers that are or may be in possession of Personal Information and any other confidential information, through the execution of a non-disclosure agreement and within any executed contracts or service agreements undertaken with said Service Provider. Specifically, such contracts and/or agreements will include details on how Personal Information, and any other confidential information, under the administration of Pension Services Corp., is delivered, stored, and destroyed by the applicable Service Provider, with the ability of such controls to be inspected by Pension Services Corp. and/or its Trustees, upon request, or will include such other measures or representations as are satisfactory to Pension Services Corp. in its discretion.
10. An internal system security audit will be undertaken quarterly and then verified by the Director, Enterprise Risk & Compliance as per the Pension Services Corp. Compliance Monitoring & Internal Audit Manual.
11. Any suspected or actual breach(es) of this policy must be timely reported to the CEO and/or the Director, Enterprise Risk & Compliance.

7.0 Monitoring

The Privacy Officer is responsible for monitoring the implementation of and adherence to this policy.

8.0 References

- Canadian Standards Association Model Code 10 Principles
- CPPIB Privacy Policy
- Digital Privacy Act
- NS Public Service Superannuation Act and Regulations, and Collective Agreements
- NS Teachers' Pension Act and Regulations, including the 2005 Joint Trust Agreement
- OMERS Corporate Privacy Policy
- Pension Services Corp. Code of Business Ethics and Conduct
- Pension Services Corp. Communications and Disclosure Policy
- Pension Services Corp. Compliance Monitoring & Internal Audit Manual
- Personal Information Protection and Electronic Documents Act

9.0 Enquiries

Any questions of uncertainty pertaining to the meaning or application of this policy should be referred to the CEO, the Director, Enterprise Risk & Compliance, or their respective delegates.

Approved By:	Doug Moodie Chief Executive Officer and President
Document Owner:	Director, Enterprise Risk & Compliance
Effective Date:	01 November, 2018
Next Review Date:	31 October, 2019

APPENDIX - PRIVACY BREACH PROCEDURE

I. OBJECTIVES

This procedure is divided into two parts, and is intended to assist Employees and Pension Services Corp. in their responses to:

- the discovery of a Privacy Breach
- a complaint from an individual about a Privacy Breach

II. DIRECTIVES – SECURITY ARRANGEMENTS

Pension Services Corp. is responsible for protecting Personal Information by making reasonable security arrangements against risks such as unauthorized access, collection, use, disclosure or disposal.

III. ACCOUNTABILITY

- The Privacy Officer and the CEO will be accountable for Pension Services Corp.'s compliance with this procedure.
- Each Employee is responsible for complying with this procedure.

IV. PROCEDURES FOR MANAGING AND REPORTING A PRIVACY BREACH

Step 1 - Identify the Privacy Breach and take immediate action
Step 2 - Notify the appropriate party(ies)
Step 3 - Manage the Privacy Breach
Step 4 - Investigate and document the Privacy Breach
Step 5 - Follow-up and long term action plan

Step 1 – Identify the Privacy Breach and take immediate action

The Employee responsible for the Privacy Breach or the Employee who discovers the Privacy Breach must do his or her best to both identify what happened and to contain, minimize and remedy the damage from the Privacy Breach.

Some examples are as follows:

- If an electronic data device is stolen the Employee must notify building security staff immediately.
- If a fax is sent to the wrong number, the Employee must call the recipient and ask them to destroy the document and any copies that were made.
- If an email is sent to the wrong person, including to external recipients, the Employee must contact the recipient immediately and ask them to securely destroy any email printouts that were made and delete the email.
- If an unauthorized person has or may have access to a database or computer system, the Employee must immediately notify (in writing) the Director of Information Management & Technology who can instruct Technology staff to disable accounts or change passwords and identification numbers.

Step 2 – Notify the appropriate party

The Employee should report the incident as follows:

- To the Employee's manager
- To the CEO
- To the Director of Information Management & Technology to have passwords reset or to have a lost or stolen device wiped
- To the police if a theft or other crime has occurred (e.g. office break-in, laptop stolen from car)
- To legal counsel if it is a theft or other crime or if legal counsel have an interest in the documents or information at issue (court papers, confidential documents)
- To the Privacy Officer who is responsible for monitoring the implementation of responses to the Privacy Breach

Step 3 – Manage the breach

The CEO is responsible for coordinating a corporate response to the incident, if necessary, and for making a decision, with the option of seeking appropriate consultation (for example, legal counsel), whether to notify the Trustee of the Plan involved, and/or the member, pensioner, or beneficiary whose Personal Information was the subject of the Privacy Breach.

Step 4 – Investigate and document the Privacy Breach

The Employee's manager must:

- Document the Privacy Breach (see the suggested form at the end of this appendix)
- Follow-up on the Privacy Breach, which may include documenting: recovery of the Record or data device, identification of any additional loss of information.

Step 5 – Follow-up and long-term action plan

The Privacy Officer will review the circumstances of the Privacy Breach to determine if policies, procedures or work practices are adequate to protect Personal Information. Together with applicable Senior Management, the Privacy Officer will determine what, if any, follow-up and long-term remedial action is necessary to prevent the Privacy Breach from reoccurring. This includes considering whether the Privacy Breach procedure was followed and whether any new or amended policies or procedures are required, or if any training is required to prevent reoccurrence of the Privacy Breach.

V. PRIVACY COMPLAINT PROCEDURE

Employees may receive a call, email or letter from a citizen or another Employee complaining of an alleged Privacy Breach to a member, pensioner, or beneficiary's Personal Information. The key to handling this type of communication is obtaining as much detail as possible and notifying the appropriate parties.

Step 1 - Receive and document the complaint

- When a complaint is received by telephone or in person, discuss the details with the complainant and document what the complainant believes has happened. This is a critical step and should be completed in writing so that it can form part of Pension Services Corp.'s response to the complaint. (For a suggestion of information to gather, see the form at the end of this appendix.)
- When a complaint is received by email or letter, or once you have captured in writing the details given to you by phone or in person, forward the complaint to your manager.

Step 2 – Notify the appropriate party

The manager should report the complaint to the CEO and/or Privacy Officer. The CEO will coordinate a corporate response, if necessary, and will make a decision, with the option of, after appropriate consultation, whether to notify the impacted Trustee or other appropriate parties.

Step 3 – Complainant Communication

Communication with the complainant should be done in consultation with the CEO, Privacy Officer and/or the applicable Senior Management. The manager responsible for responding to the complaint should incorporate the following into the complaint procedure:

- Send written acknowledgement to the complainant, restating the details presented by the complainant and indicating who will be performing an investigation.
- If necessary, send a written update of progress of the investigation (stage of investigation, follow-up activities, expected or updated time frames). Do this after no more than two months has elapsed since the initial acknowledgement.
- Generate a report of the results of the investigation. At a minimum, the report should include: verification of the breach, mitigating activities and other follow-up activities.

Step 4 – Continue to keep the Privacy Officer informed of any further correspondence from the complainant, and any progress on promised or anticipated changes to policies or procedures.

Information Breach Reporting Form

Please complete this document and provide the completed and signed document to the Privacy Officer. Treat the information you collect about a Privacy Breach as highly confidential. You do not want to further the Privacy Breach by sharing the information more broadly than absolutely required.

1. **Privacy Breach reported by:**

2. **Person responsible for Privacy Breach:**

3. **Details of Privacy Breach (incl. date, time, location etc):**

4. **Notifications to individuals: (incl. name and date):**

5. **Notes of discussions & follow-up:**

Completed by: Date:

Manager (if different from above): Date:

TO BE COMPLETED BY THE PRIVACY OFFICER	
Outcome:	
Date Closed:	
Signature of Privacy Officer	Date