

Nova Scotia Department of Finance Privacy Policy

Approval Date: May 13, 2009

Approved By: Vicki Harnish, Deputy Minister

Effective Date: September 9, 2009



1. Policy Statement

The Department of Finance will ensure adherence to the privacy protection provisions of the *Freedom of Information and Protection of Privacy (FOIPOP) Act*, the *Personal Information International Disclosure Protection Act (PIIDPA)*, the Government Privacy Policy and other applicable legislation. The Department of Finance will uphold the principles of transparency, custodianship and shared responsibility established in the Government Privacy Policy, as it relates to the collection, use and disclosure of personal information.

2. Definitions

Employee

An individual in the employ of, seconded to, or under personal service contract to the Government entity and their volunteers, students, and interns who have access to records.

FOIPOP

NS Freedom of Information and Protection of Privacy Act.

Office of Primary Responsibility (OPR)

The position within the Department with the responsibility for specific functions or operations and for the records that support those functions or operations.

Personal information

As defined in clause 3(1)(l) of the *FOIPOP Act*, "recorded information about an identifiable individual, including:

- (i) the individual's name, address or telephone number,
- (ii) the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations,
- (iii) the individual's age, sex, sexual orientation, marital status or family status,
- (iv) an identifying number, symbol or other particular assigned to the individual,
- (v) the individual's fingerprints, blood type or inheritable characteristics,
- (vi) information about the individual's health-care history, including a physical or mental disability,
- (vii) information about the individual's educational, financial, criminal or employment history,
- (viii) anyone else's opinions about the individual, and
- (ix) the individual's personal views or opinions, except if they are about someone else."

Personal Information Bank (as defined by the *Treasury Board of Canada Secretariat*)

A *personal information bank* (PIB) is a summary of the types of information about individuals that is held by a department and it includes all personal information that is organized and retrievable by a person's name or by an identifying number, symbol or other particular assigned only to that person, such as a vendor master number or employee identification number. A PIB includes personal information that has been or is being used, or is available for use for an administrative purpose. Examples include employee and pensioner deductions and benefits information used for payroll processing, and testing and licensing information about insurance agents.

A *standard information bank* describes information contained in common administrative records that many government institutions maintain about their employees or the general public. Examples include pay and benefits, training and development, performance, health and safety, names, addresses, phone numbers, and other contact information and opinions of the general public received through correspondence, applications, public opinion polls and surveys, and work and education histories collected and used in accordance with hiring practices.

Privacy Breach	The event of unauthorized collection, access, use, disclosure, storage or alteration of personal information.
Privacy Impact Assessment (PIA)	Is the due diligence exercise which identifies and addresses potential privacy risks that may occur in the course of the operations of a public body.
PIIDPA	<i>NS Personal Information International Disclosure Protection Act, SNS 2007</i>
Record	<p>As defined in clause 3(1)(k) of the <i>FOIPOP Act</i>, “records” includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records.”</p> <p>Records document transactions, rights or obligations of the Department and includes e-mails and other electronic documents, databases, as well as Web 2.0 technologies such as blogs, wikis, and instant messages.</p>
Records Life Cycle	The stages of activity from creation/receipt of a record up to and including its final disposition. The phases of the records life cycle are active, semi-active, and inactive and are set out in the records schedule, such as STAR/STOR. Activities in the records life cycle include creating, receiving, classifying, indexing, registering, maintaining, accessing, retrieving, using, distributing, storing, migrating to another medium, destroying, and preserving.
Records Schedule	A comprehensive description and classification of all records of a public body, with a plan governing the life cycle of the records from creation or receipt to disposition or permanent preservation. (<i>Government Records Act</i>)

Third Party

In relation to a request for access to a record or for the correction of personal information, means any person, group of persons, or organizations other than

- the person who made the request, or
- a public body.

Vital Records

Master records of significant legal, operational, historical, and/or fiscal value which cannot be recreated from other sources; necessary to establish the department's legal and financial position, includes indexes of asset holdings.

The records of government that contain information essential to:

- conduct emergency operations during and immediately following a disaster;
- resume/continue government services or operations;
- re-establish the legal, financial and functional responsibilities of government; and
- re-establish the rights and obligations of individuals, corporate bodies and other governments with respect to the Government of Nova Scotia.

3. Application

This policy applies to:

1. All employees, contractors, and agents of the Nova Scotia Department of Finance who have access to and/or share with the Department the custody and/or control of personal information.
2. All personal information, regardless of media or format, in the custody and control of the Department of Finance.

4. Objectives

This policy is designed to ensure that government meets its legislated obligations to manage personal information throughout its 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 disposal.

5. Directives

The Department of Finance shall:

- Only collect, access, store, use, and disclose personal information where authorized by law.
- Maintain a directory of personal information banks that are currently in its custody or under its control, as required by section 48 of the *FOIPOP Act*.
- Classify, retain and dispose of personal information in its custody or under its control in accordance with approved records retention schedules, such as STAR/STOR. Personal information will be disposed of once the authorized uses for which it is retained have concluded.
- Ensure personal information is authentic, reliable as evidence of transactions, rights or obligations, and is accessible to authorized users.
- Make reasonable security arrangements to protect personal information in its custody and under its control, throughout its records life cycle by establishing and documenting procedures and controls regarding the collection, use, disclosure, retention, and disposal of personal information.
- Consider the *FOIPOP Act* and *PIIDPA* obligations and other legislation, regulations and operational procedures that have specific reference to the collection, use, disclosure, and disposal of personal information, with respect to the protection of personal information, as part of maintaining this policy.
- Identify those individuals with designated or delegated responsibilities for making reasonable security arrangements for personal information in keeping with the provisions of applicable legislation, policies, procedures and agreements.
- Establish a privacy breach protocol.
- Identify potential risks to personal information by completing a privacy impact assessment for any new program or service or for any significant

change to a program or service.

- Advise all employees of this policy coming into force.
- This policy shall be made readily available and will be posted on the Department of Finance's Internet Website.
- Ensure employees receive the appropriate orientation regarding the collection, use, disclosure, storage, and disposal of personal information.
- Ensure employees who handle personal information receive training specific to their role in order to protect the personal information that they access.
- Requests for the correction of personal information and concerns about compliance with this policy shall be directed to the IAP Administrator.
- Ensure best security practices, as established by each division, are followed in the handling and storage of personal information.
- Establish decentralized records repositories in divisions, as required, to store records containing personal information until these records can be boxed and sent offsite for storage, transferred to a central agency, or sent for disposal.
- Ensure the appropriate protection of personal information in its custody.
- Ensure the identity of individuals is not readily identified when publicly displaying aggregate data about individuals.
- Make this policy available to the public through the Department's Website.
- Ensure all existing privacy policies of the department are consistent with this and the corporate privacy policy.
- The Privacy Program established under this Policy shall be evaluated on an annual basis.

6. Policy Guidelines

The Department of Finance shall:

- Prevent the unauthorized collection, use, and disclosure of personal information.
- Develop a Privacy Impact Assessment (PIA) template that is in

accordance with the PIA template maintained by the Information Access and Privacy (IAP) Office, Justice.

- Develop and publicize a process for requests to correct personal information as per section 25 of the *FOIPOP Act*.
- Provide a process for expressing concerns about compliance with this policy.
- Establish procedures for the security and protection of personal information as required to support this policy.
- Provide reasonable security arrangements to secure and control access to personal information. Security arrangements may include such things as the use of locked filing cabinets; access to records is limited to only those individuals who need access for the purpose of carrying out a program or service; databases containing personal information will be password protected; passwords will only be issued to staff that require access to deliver the program or service; files containing personal information will not be removed from offices or left unattended; and the disposal of records containing personal information will be carried out using secure methods, such as shredding.
- Provide training and awareness on the privacy protection of personal information to all staff. All new employees will receive a copy of this policy in an orientation package and they will receive the appropriate training regarding the privacy of personal information, as required by their position.
- Governance and accountability structures will be established and implemented to ensure the appropriate management of personal information, including during collaborative service delivery arrangements and when information is shared with other provincial government departments, other governments, or external entities.
- Identify those individuals with designated or delegated responsibilities for making reasonable security arrangements for personal information in keeping with the provisions of applicable legislation and policies.

7. Accountability and Security

Deputy Minister

Is accountable for compliance with the corporate policy and is responsible for the approval, compliance, administration, and monitoring of this policy. These responsibilities include designating an individual responsible for administering and monitoring compliance with DOF's privacy obligations, supplementing the requirements of the corporate policy to meet any additional, unique, or special

responsibilities a government entity may have to protect personal information.

Information Access and Privacy (IAP) Administrator

Is responsible for receiving and prompt disposition of concerns expressed by individuals, groups of individuals or organizations about compliance with this policy and requests for the correction of their personal information, received in writing or on Form 2 http://www.gov.ns.ca/just/IAP/forms/FOIPOP_Form_2.pdf , as provided for in the *FOIPOP Act*. Will coordinate the Department's response to reviews received from the Privacy Review Office; participate in the completion of privacy impact assessments and the resolution of privacy breaches; and coordinate the yearly review of this policy.

Managers/Supervisors

Are responsible for establishing security controls, procedures, standards and guidelines, and breach protocols; that their area of responsibility is in compliance with this policy; that risk mitigation strategies are in place for their operations to protect personal information and are monitored to ensure they continue to be effective; and breach protocols are used. Also responsible to ensure staff in their charge are provided with privacy orientation and training specific to their position. This may include general privacy awareness, using the privacy breach protocol, specific security arrangements, privacy impact assessments, and other training as required.

Employees

Are responsible for sharing responsibility for protecting personal privacy in accordance with privacy laws and the department's policies and practices, including this policy. Employees are responsible for the security and protection of personal information in their care, whether they collect, store, manage, distribute, use, or dispose of it during the conduct of their operations. Employees working within signed confidential agreements will abide by those agreements.

Manager of Information Management

Is responsible for the development and integration of the information access and protection of privacy program within the Information Management group in order to maximize delivery. Provides recommendations to senior management and advises and assists Department staff about privacy issues that arise.

Information Management Staff

Provides guidance, orientation, and advice on departmental information management standards, priorities, procedures, policies and guidelines which includes instruction on the use of applications and systems and indexes to locate information and understand the classification schemes and retention schedules approved for the department's use to manage records and information, such as STAR/STOR. This involves influencing

staff to appreciate the importance of effective information management and improving compliance and understanding of policies and procedures.

Offices of Primary Responsibility (OPRs)

Are responsible for ensuring records are created, registered in the records management system, are an accurate and complete records of government activity throughout their records life cycle (see definition, page 1), and for ensuring records in their custody or under their control are secured against unauthorized access. The OPR will provide records and information in response to requests for information under FOIPOP, routine access, legal proceedings, and general requests for information.

8. Policy Approval

The Executive Management Committee, consisting of the Deputy Minister, Assistant Deputy Minister and Executive level management are responsible for the approval of this policy.

9. Monitoring

The Manager of Information Management will monitor the implementation of this policy and report to the Executive Management Committee on the status of concerns and issues of non-compliance with this policy received.

Managers and supervisors will monitor their staff to ensure compliance with this policy.

Nova Scotia Department of Justice, Information Access and Privacy (IAP) Office is responsible for monitoring the implementation of the corporate Privacy policy.

10. References

- Citizen On-line Identity Authentication Policy, August 1, 2007
- Code of Conduct for Civil Servants, September 1, 2000
- Freedom of Information & Protection of Privacy (FOIPOP) Act and Regulations
- Freedom of Information & Protection of Privacy (FOIPOP) Act Policy (corporate)
- Personal Information International Disclosure Protection (PIIDPA) Act and Regulations
- Government Records Act

- Records Management Policy, Finance January 22, 2008
- Public Archives Act
- Information Management Policy (corporate), October 1, 2008
- Website Privacy Policy (corporate), June 1, 2004
- Web 2.0 Technologies Guidelines (corporate), draft 2008
- Guidelines for Managing Emails of Exiting Employees (corporate), draft 2008
- Privacy Policy (corporate), April 1, 2008
- Statistics Canada Act
- NS Statistics Act
- Occupational Health and Safety Act
- *Report of the Auditor General, "Electronic Information Security and Privacy Protection"*, section 4, pages 31-41, December 2005
- National Standards of Canada "*Model Code for the Protection of Personal Information*"
- Treasury Board of Canada Secretariat, Glossary, url: www.tbs-sct.gc.ca/atip-aiprp/glossary-eng.asp

11. Enquiries

Enquiries concerning this policy will be answered by the IAP Administrator, Angela Smith (902) 424-7932 AJSMITH@gov.ns.ca.