Department of Justice

Privacy Policy

Approval Date: April 2, 2009

Effective Date: April 3, 2009

Approved By:

Marian Tyson, Q.C.
Deputy Minister

I POLICY STATEMENT

It is the policy of the Department of Justice (DOJ) that it will ensure adherence to the privacy protection provisions of the *Freedom of Information and Protection of Privacy Act*, the *Personal Information International Disclosure Protection Act*, the Government Privacy Policy and other applicable legislation. DOJ 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.

II DEFINITIONS

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

employee	an individual in the employ of, seconded to, or under personal service contract to the public body and their volunteers, students, and interns who have access to records.
FOIPOP	*Nova Scotia Freedom of Information and Protection of Privacy Act*
personal information	as defined in clause 3(1)(I) 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"
privacy breach	the event of unauthorized collection, access, use, disclosure, storage, or alteration of personal information

PIA	a Privacy Impact Assessment is a due diligence exercise which identifies and addresses potential privacy risks that may occur in the course of the operations of a public body
record	as defined in clause 3(1)(k) of the *FOIPOP Act*, 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
Information Life Cycle	All stages through which information passes between its creation and final disposition, including creation, collection, receipt, maintenance, use, dissemination, and disposition. Functions and activities performed during the life cycle include such things as storage, access/retrieval, and modification.

III POLICY OBJECTIVES

The policy is designed to ensure that the DOJ meets its legislated obligations in the management of 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, storage or disposal.

IV APPLICATION

This policy applies to:

all DOJ employees
all personal information in the custody and control of DOJ

V POLICY DIRECTIVES

- the privacy policy will be posted on the DOJ web site, at http://www.gov.ns.ca/just/ all employees will be advised of the policy coming into force
- DOJ must collect, access, store, use, disclose and dispose of Personal Information only where authorized by law or agreement with other public body that is authorized by law

each divisional head is responsible for making reasonable security arrangements for personal information in keeping with the provisions of applicable legislation

- DOJ must have a privacy breach/complaint protocol, per the template maintained by the NS Information Access and Privacy Office (see Appendix A)
- DOJ must complete PIAs for all new and significantly amended programs or services that collect, use or disclose personal information (see Appendix B for the PIA Template)
- program areas are responsible for ensuring that contracts with service providers are compliant with this policy and the *Personal Information International Disclosure Protection Act*
- personal information in the custody of DOJ may be subject to other legislation See the procedures manual for specific processes on managing this information. For example:
    - *Youth Criminal Justice Act (YCJA)* - access, use and disclosure of information of Youths convicted under the *YCJA* will be compliant with the provisions of the *YCJA*
    - *Fatality Investigation Act* - restricts disclosure of certain records. Requests for these records can be made under the *FOIPOP Act.* (However, the privacy interests related to a deceased person and their family will be considered, as well as the Chief Medical Examiner's legislated authority)
    - *Private Investigators and Private Guards Act* - access and disclosure of personal information about private investigators and security guards will be compliant with the provisions of the *Private Investigators and Private Guards Act*

Correction & Concerns

Individuals should contact the DOJ Information Access and Privacy (IAP) Administrator at 424-6572 if they:

- have concerns about compliance with the DOJ Privacy Policy
- require correction of personal information

VI POLICY GUIDELINES

- DOJ has created a separate Privacy & Security Procedures Manual that addresses the specific privacy needs of the various divisions, as well as security procedures
- the DOJ IAP Administrator is responsible for delivering privacy awareness training
- personal information must only be collected, used and disclosed in compliance with the *FOIPOP Act* (see Appendix C for a summary)

VII ACCOUNTABILITY & SECURITY

General Statement

DOJ is accountable for the privacy of the personal information it holds, and for the associated business processes and procedures for the collection, use, disclosure, retention and disposal of that information.

1. Accountability

the Deputy Minister of Justice is accountable for compliance with this policy

- employees are accountable for complying with the DOJ privacy policy, and the Government of Nova Scotia's privacy policy

2. Security

- employees will make reasonable efforts to ensure protection of personal information. For example:
    - keeping filing cabinets containing personal information locked
    - not removing files containing personal information from offices or left unattended unless operationally required
    - disposing of both transitory or master records containing personal information using secure methods, such as cross-shredding
    - ensuring their Blackberries are password-protected and e-mails sent/received through GroupWise are encrypted via a designated Blackberry server
- access will be limited to individuals who need access only for the purpose of carrying out a program or service, *i.e.*, a need to know basis
- databases containing personal information will be password protected and passwords will only be issued to staff that require access to deliver the program or service.
- To be compliant with PIIDPA ss 9(4), Deputy Minister approval is required to take Blackberries and other electronic devices containing personal information outside the country

VIII MONITORING

The DOJ IAP Administrator will be responsible for monitoring compliance with this policy.

IX REFERENCES

Freedom of Information and Protection of Privacy Act and Regulations
Personal Information International Disclosure Protection Act and Regulations
Government Records Act
Privacy Review Officer Act
Management Manual 300: Common Services, Chapter 4, Policy 4.7, Website Privacy Policy
Management Manual 300: Common Services, Chapter 4, Policy 4.11, Privacy Policy
Management Manual 100: Management Guide, Chapter 1, Policy 1.2, Management Manuals Policy
Department of Justice Privacy Breach/Complaint Protocol (Appendix A)
Department of Justice Privacy Impact Assessment Template (Appendix B)
Department of Justice Privacy & Security Procedures Manual

X ENQUIRIES

Enquiries should be directed to the DOJ IAP Administrator at 424-6572/424-6836.