Access & Privacy Essentials Toolkit

For Small Public Bodies - FOIPOP

Office of the Information and Privacy Commissioner for Nova Scotia
oipcns@novascotia.ca 902-424-4684 https://oipc.novascotia.ca

Contents

Notice to Users

This document is intended to provide general information only. It is important to read the full legislation not just the sections summarized to understand the full extent of the provision. This document is not intended nor can it be relied upon as legal advice. As an independent agency mandated to oversee compliance with *FOIPOP, MGA* and *PHIA* the Office of the Information and Privacy Commissioner for Nova Scotia cannot approve in advance any proposal from a public body, municipality or health custodian. We must maintain our ability to investigate any complaints and to provide recommendations in response to these complaints. The contents of this document do not fetter or bind this office with respect to any matter, including any complaint investigation or other matter respecting which the Commissioner will keep an open mind. It remains the responsibility of each public body, municipality and health custodian to ensure that they comply with their responsibilities under the relevant legislation. Visit us at: https://oipc.novascotia.ca

FOIPOP Access and Privacy Rules – At a Glance

Access to Information Rules		
Discretionary Exemptions		
Exemption		**Summary**
12	Intergovernmental Affairs	• Harm the conduct of relations between Nova Scotia and identified governments or • Reveal information received in confidence from identified governments • Does not apply to records in existence for 15 or more years
13	Deliberations of Executive Council	• Reveals substance of deliberations of the Executive Council or any of its committees including advice, policy considerations or draft legislation • Does not apply to records in existence for 10 or more years • Does not apply to background information if the decision has been made public, implemented or five years have passed since the decision was made
14	Advice to public body or minister	• Advice or recommendations or draft regulations developed by or for a public body • Does not apply to background information or information that has been in existence for five or more years
15	Law enforcement	• Harm to law enforcement including, for example: o Harm the security of a system o The information is a law enforcement record and disclosure is an offence pursuant to an enactment o Result in civil liability or harm proper custody o Does not apply to a decision not to prosecute
16	Solicitor client privilege	• May refuse to disclose information subject to solicitor client privilege
17	Financial or economic interests	• Harm financial or economic interests of a public body or the government of Nova Scotia • Shall not refuse to disclose the results of product or environmental testing
18	Health & Safety	• Threaten anyone else's safety or mental or physical health, interfere with public safety or results in immediate and grave harm to the applicant's safety or mental or physical health
19	Conservation	• Result in damage to heritage sites or endangered or vulnerable species
19A	Local public body - Closed meetings	• Where an enactment authorizes in camera meetings the head may refuse to disclose draft resolutions, bylaws or other legal instruments or substance of deliberations so long as the meeting was held in private and has not been in existence for 15 years or more
19B	Local public body - Academic research	• Details of academic research conducted by an employee of a local public body
19C	University - Certain personal information	• Evaluative or opinion material compiled solely to determine suitability for appointment or for evaluating an applicant's research projects or materials if the information was provided in confidence.
19D	Local public body – hospital records	• Records created for the purpose of education or improvement in medical care or practice (s. 60(2) *Evidence Act*) • Does not apply to medical and hospital records pertaining to a patient
19E	Labour conciliation records	• Any information (report or testimony) obtained by board or officer appointed pursuant to identified statutes

Access to Information Rules		
Mandatory Exemptions		
20	Personal information	• The disclosure would be an unreasonable invasion of a third party's personal privacy
21	Confidential information	• The disclosure would reveal trade secret, financial, labour relations etc. info + supplied in confidence + reasonably expected to harm significantly various identified business interests (all three factors must be true)
Request Processing Essentials		
4	Records	• Act applies to all records in the custody or under the control of a public body
6	Applicant obligations	• Request must be in writing, subject matter specified and fees paid
7(1)	Public body duty	• The public body must make every reasonable effort to assist the applicant and respond without delay openly, accurately and completely
5(2)	Duty to sever	• The right of access to a record does not extend to information exempted from disclosure pursuant to the Act but if that information can reasonably be severed from the record, an applicant has the right of access to the remainder of the record
7(2)	Time	• Public body must respond within 30 days unless a permitted time extension is taken
11	Fees	• Public body may charge fees only as permitted by the Act and regulations • Public body must consider waiving fees when requested
7(2)	Content	• The public body's response must include the information listed
22	Notices	• Where the public body has reason to believe that s. 20 or s. 21 applies, the public body must give notice as set out in this section, within the timelines

Notice

This table is intended only as a quick reference tool. The sections are only summarized. You must read the entire provision to properly understand the full requirements of each section. You can find a copy of the *Freedom of Information and Protection of Privacy Act* and Regulations at: https://oipc.novascotia.ca.

Essential Access to Information Rules

Purpose of Access Law
The purpose of access to information legislation such as the *Freedom of Information and Protection of Privacy Act ("FOIPOP"*) is to ensure that public bodies are fully accountable to the public by giving the public a right of access to records, giving individuals a right of access to their own personal information and specifying limited exceptions to the right of access. Further, *FOIPOP* ensures that there is independent oversight of decisions made by the public body. That oversight is provided by the Office of the Information and Privacy Commissioner. The access rules in the *FOIPOP* are similar and in some places identical to rules found in every other access to information law across Canada.

Is it "FOI able"?
Unless specifically excepted from *FOIPOP*, **all** records in the custody or under the control of the public body are subject to the right of access. Generally all of a public body's records are "FOI able" including public body records on personal laptops and in password protected email accounts. However, some examples of records to which the *FOIPOP* right of access does not apply include:

- Material that is a matter of public record;
- A note, communication or draft decision of a person in a judicial or quasi-judicial capacity;
- A record of a question that is to be used on an examination or test.

See section 4 of *FOIPOP* for a complete list of exceptions.

Note about exceptions and exemptions:

FOIPOP refers to "exceptions" meaning those types of records that *FOIPOP* does not apply to. "Exemptions" are the sections of the *FOIPOP* that describe types of information that can be withheld (severed) from a responsive record. For example, information that is subject to solicitor client privilege is "exempted" from disclosure.

Request Basics
A person makes a request by submitting a request in writing. Applicants do not have to use any specific form but there is a standard form available. It costs $5 to make a general access to information request and there is no fee to make a request for your own personal information. Requests must receive a response within 30 days (or longer if a time extension is warranted).

The only information that can be withheld (severed) from a record is information that meets the requirements for exemptions to disclosure. There are mandatory exemptions and discretionary exemptions. A mandatory exemption is one that if all of the requirements are met, the public body must withhold the information. A discretionary exemption is one where if all of the requirements are met, the public body may or may not withhold the information. The public body should consider such things as the age of the record, the public interest in disclosure, the benefits of disclosure generally and past practice to decide whether a discretionary exemption should be applied.

Rule: *Freedom of Information and Protection of Privacy Act* – Access Rules At a Glance

When processing an access request it is essential to protect the identity of the requester/applicant because this is their personal information and so subject to the rules regarding protection of privacy.

How to Process an Access to Information Request

Public bodies should have in place a process for managing access to information requests. The access to information coordinator for your public body will manage the request process which will include evaluating whether or not a fee can be charged, whether the fee should be waived, whether time extensions can be taken and what information can or cannot be released.

Tool: Life Cycle of a Typical Access to Information Request

Best Practices

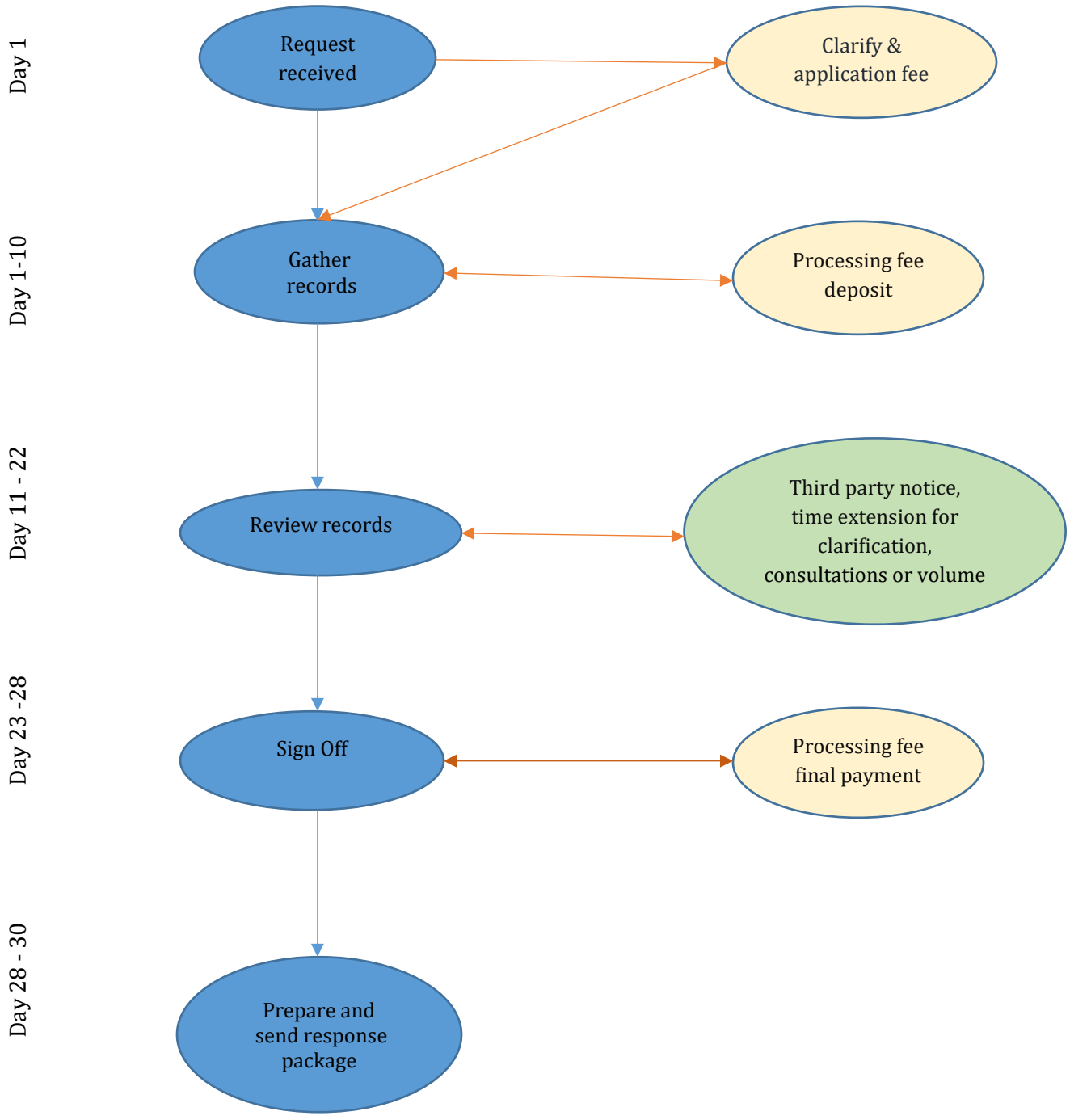
Some best practices for ensuring an effective access to information program are:

- **Don't process the whole request:** Think of access requests as a method of last resort. Try to publish information that you know citizens are interested in. Use a routine release list, open data and open information websites to make the information easily accessible. Think about the types of access requests you've had most frequently in the past and publish that type of information. Remember, when you routinely release information, you do not have to disclose the entire document – you can produce a public version. (Remember though that the original version can still be requested using the formal FOI process.) If you do these things, when you receive an access to information request, hopefully you will have information publicly available that is responsive to the request, leaving you just a bit of the request to process formally.

  Tool: Sample Routine Release List

- **Buy-In from the Top –**Executives should be well informed about the public body's access to information (and protection of privacy) program and should understand and support the requirement for accountability and transparency as set out in FOIPOP.

Life Cycle of a Typical Access to Information Request



Sample Routine Release List

The following is a list of records typically created at the municipal level that could be made publicly available without a formal access request. The list is intended to assist both municipalities and public bodies in identifying record types that could potentially be routinely released. Ideally they would be posted on a website or otherwise made easily and immediately available upon request with no charge to the requester.

Business Area	Record Types
Access	• List of all formal access to information requests (personal information redacted) • Copy of all previously released general records
Boards & committees	• External board membership and appointment procedures • Municipal and school board elections background, procedure, voter and candidate information, results
Business units	• General overview of the business unit responsibilities • Contact information of business unit staff • Links to relevant legislation and historical versions of relevant legislation • Standards and regulations • Copies of bylaws • Statistics • Program evaluations
Council and mayor	• Councilor name by district and district maps • Councilor compensation records • Councilor discretionary and district capital spending records • Municipal elections campaign contribution records • Elected officials' mileage reimbursement claims and travel expenses • Record of conflict of interest declarations for council and committees
Employees	• Contact information for business unit staff • Generic information about current benefits and hours of work • Current job descriptions, salary ranges or hourly rate, classification of positions • Employee expense reports • Organizational charts • Overtime expenditures
Financial	• Audited financial statements • Costs of specific or special events • Expenditure reports by cost elements (salaries, office supplies, travel etc.) • Standard & Poor's annual rating • Budgets including capital budget • Project overviews • Business plans • Procurement information • Taxation information • Tender results • General real estate acquisitions and disposals • Real estate record of closed transactions • Community Grants Program • Tax exemption plans

Business Area	Record Types
Fire & Emergency	• Emergency management plans and kits • Fleet vehicles • Fire investigation summaries • Fire inspection reports • Fire prevention information, template, inspection sheets, permit applications • Fire hall rental information • Fire station location and coverage areas • Fire incident statistics • Volunteer firefighter recruitment information
Meetings	• Membership, schedule, minutes, agendas and reports for all meetings (except in camera), including archived minutes, agendas and reports • Meeting logs for in camera meetings held by council, standing committees and advisory committees • Meeting procedures
Parks & Recreation	• Guides and guidelines • Application forms • Toolkits • Strategy documents • Field conditions
Planning & Development	• Guides and guidelines and toolkits • Application forms • Strategy documents • Official street list • Water quality information • Climate change information • Information on invasive species that the municipality is managing • Lot file information (with personal information redacted) including occupancy permits, encroachment permits, development permits, streets and services permits, lot grading permits, blasting permits • Blasting reports • Building permits (with personal information redacted) • Building standard statistics • Vending license statistics • Parking permit statistics • Bylaw standards • Parking enforcement statistics • Animal control statistics • Number of licensed taxi cabs • Approved concept, tentative and final subdivision plans • Plans and maps prepared by planning
Policies, Procedures & Plans	• Access and privacy obligations • Annual service plans • Human resources business plan • Human resources policies and procedures • Municipal archive access information and procedures • Policies • District boundary review information and procedures • Economic strategy summary description and approved plan
Business Area	**Record Types**
Policing	• Media releases

	• External crime mapping • Crime and related statistics
Polls & Surveys	• Results of polls or surveys
Transit	• Service descriptions • Schedule and route information • Fare information • Terminal information • Parking information • Security information • Snow plan information • Statistical information in relation to accidents/collisions, ridership, complaints • Fleet and fleet maintenance
Transportation & Public Works	• Curbside collection schedules • Permit applications for parades • Reports and policies including on street parking policy, neighbourhood shortcutting, etc. • Road construction projects • Traffic control manual • Summary of solid waste satisfaction surveys

Note: This document is based on a survey of publicly available records on a variety of Nova Scotia municipal websites, particularly the Halifax Regional Municipality

Privacy Rules		
24	Collection	• Public bodies shall not collect personal information unless: o The collection is expressly authorized by an enactment o The information is collected for the purpose of law enforcement o The information relates directly to an dis necessary for an operating program or activity of the public body
24(2)	Accuracy	• If personal information will be used to make a decision that directly affects the individual the public body must ensure the information is accurate and complete
24(3)	Security	• The public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure and disposal
24(4)	Retention	• Where a public body uses an individual's personal information to make a decision that directly affects the individual, the public body must retain the information for at least one year
25	Correction	• Applicant may request a correction • Where no correction is made, the public body must annotate
26	Use	• A public body may use personal information only o For the purpose for which that information was obtained or compiled or o For a use compatible with that purpose o If the individual has consented to the use o For a purpose for which the information may be disclosed to the public body under s. 27- 30
27	Disclosure (c) (b) (a) (d) (e) (f)	• A public body may disclose personal information only: **Compatible use & consent** o For the purpose the information was obtained or compiled or a use compatible with that purpose o If the individual has consented in writing to the disclosure **Law, subpoena, court orders** o As provided pursuant to an enactment o For the purpose of complying with an enactment or with a treaty or agreement made pursuant to an enactment o To comply with a subpoena, warrant, summons or order issued by a court or person with jurisdiction to compel production of information **Public bodies** o To an officer or employee of a public body if the information is necessary for the performance of the duties of, or for the protection of the health or safety of, the officer or employee

Privacy Rules Cont'd		
27	Disclosure	**Public bodies cont'd**
	(g)	○ To a public body to meet the necessary requirements of government operations
	(h)	○ For the purpose of collecting a debt or fine owing to the Province or public body of to make a payment owed by the Province or public body
		Law enforcement
	(m)	○ To a public body or a law-enforcement agency in Canada to assist in an investigation undertaken with a view to a law-enforcement proceeding or from which a law enforcement proceeding is likely to result
	(n)	○ If the information is disclosed by a law-enforcement agency to another law enforcement agency in Canada or in a foreign country under a written agreement, treaty or legislative authority
		Auditor, bargaining agent, public archives & research
	(i)	○ To the Auditor General for audit purposes
	(j)	○ To a member of the House of Assembly who has been requested by the individual, whom the information is about , to assist in resolving a problem
	(k)	○ To a representative or bargaining agent who has been authorized in writing by the employee whom the information is about to make an inquiry
	(l)	○ To the Public Archives of Nova Scotia, or the archives of a public body for archival purposes
	(q)	○ For the purpose of research or to archives as set out in s. 29 & 30
		Safety
	(o)	○ If the head of the public body determines that compelling circumstances exist that affect anyone's health or safety
		Next of kin
	(p)	○ So next of kin or a friend of an injured, ill or deceased individual may be contacted

Notice

This table is intended only as a quick reference tool. The sections are only summarized. You must read the entire provision to properly understand the full requirements of each section. You can find a copy of the *Municipal Government Act* at: http://nslegislature.ca/legc/statutes/municipal%20government.pdf

Essential Privacy Protection Rules

There are two types of privacy rules in the *FOIPOP:* rules that apply to formal access to information requests ("FOI" requests) and rules that apply during your day-to-day work. The tests are not the same in the two situations.

Privacy and "FOI" requests
As noted earlier, all of the records in the custody or control of a public body are subject to the access requirements of *FOIPOP.* This includes the personal information of employees and citizens. But just because they are subject to the *FOIPOP* does not mean that they will be disclosed. When someone asks for records that include the personal information of a third party, the records must be carefully reviewed to first identify the portion of the records that contains third party personal information. Once the information is identified, then the FOIPOP administrator must apply a four part test to determine whether or not disclosure of the third party personal information would be an "unreasonable invasion of third party personal privacy". Applying this test takes some training and a solid familiarity of the test set out in 20(1) of *FOIPOP*. It is typically done by the person with delegated authority to apply the access provisions of *FOIPOP*.

Privacy and day-to-day work in a municipality
The privacy rules that apply to your day-to-day work in a public body are set out in sections 24-31 of *FOIPOP*. These rules say that public bodies can only collect, use or disclose personal information as an employee of a public body in very limited circumstances. In fact, if challenged, you must be able to establish that you are authorized to collect, use or disclose personal information as set out in one of the provisions of *FOIPOP*.

As a practical matter, sharing of personal information between employees of a public body is limited to information necessary for the performance of the duties of the employee or for the protection of health or safety.
Rules: *Freedom of Information and Protection of Privacy Act:* Privacy Rules at a Glance

How do you know if it's allowed?
In order to find out if the public body's collection, use or disclosure of personal information is permitted you should complete a privacy impact assessment. This assessment walks you through the privacy requirements of *FOIPOP*. Using the form supplied you can evaluate whether or not you can or should collect, use of disclose personal information, helps you identify privacy risks and privacy mitigation strategies.
Tool: Privacy Impact Assessment Template

Building privacy into your programs and processes

In order to ensure that your public body is taking privacy rules into account throughout all of its business processes, programs, IT projects etc., you should implement what is known as a "Privacy Management Framework". A privacy management framework is just a collection of tools, policies and practices which together will ensure that you catch privacy problems before they happen and that you design your processes and programs in such a way that you minimize risks of a privacy breach. The essential elements of a privacy management program are set out in the Privacy Management Program At a Glance document. It takes time to build a privacy management framework. To do so, you should conduct a gap analysis of your public body to see where your privacy program needs the most work. From the gap analysis you can build a work plan that will, over time, significantly improve the quality and reach of your privacy management program.

Tool: Privacy Management Program at a Glance.
Tool: Privacy Management Program – Gap Analysis Worksheet
Tool: How to Manage a Privacy Breach
Tool: Privacy Breach Checklist
Tool: Reasonable Security Checklist

Best practices

Privacy is a fundamental right of citizens and so any limitation on the privacy of citizens should be carefully analyzed to ensure such limitation is warranted. If your project involves sensitive personal information, a broad collection of personal information or a serious impingement on privacy, answer the following four questions before proceeding:

Is the measure demonstrably necessary to meet a specific need? At a minimum, the objective must relate to societal concerns which are pressing and substantial in a free and democratic society. To be "demonstrably necessary" the municipality should explain the rational connection between the specific need and the project.

Is it likely to be effective in meeting that need? Provide empirical evidence to support the initiative.

Is the loss of privacy proportional to the need? Explain how the collection, use and/or disclosure of personal information will be undertaken in the least privacy invasive manner possible. Minimizing the number of data elements collected, limiting access to the data and short retention periods are all examples of reducing the privacy invasive impact.

Is there a less privacy invasive way of achieving the same end? Explain what other less privacy invasive methods have already been tried to meet the identified need.

Privacy Impact Assessment

Freedom of Information and Protection of Privacy Act

What is a Privacy Impact Assessment?

The *Freedom of Information and Protection of Privacy Act* ("FOIPOP") sets out mandatory requirements relating to personal information held by public bodies. FOIPOP also requires that public bodies protect the confidentiality of personal information, and the privacy of the individual who is the subject of that information. This includes protecting the information from theft, loss and unauthorized access to, use of, disclosure, copying or disposal of the information.

A privacy impact assessment is a tool to identify risks and mitigation strategies associated with the use of personal information. It is an essential tool for ensuring compliance with the privacy requirements set out in FOIPOP and is a building block of a good privacy management program.[1]

When Should I Complete a Privacy Impact Assessment?

You should complete a privacy impact assessment ("PIA") for all new systems, projects, programs or activities. PIAs should also be completed when any significant changes are being contemplated to projects, programs or systems. There are a variety of PIA templates available online[2]. This PIA template was created by the Office of the Information and Privacy Commissioner for Nova Scotia and it incorporates elements of a number of existing templates.

[1] For more information about Privacy Management Programs visit the website of the Office of the Information and Privacy Commissioner at: https://oipc.novascotia.ca.

[2] See for example the Capital District Health Authority's PIA form at http://www.cdha.nshealth.ca/privacy-confidentiality/documents , the Government of Nova Scotia template at: https://novascotia.ca/just/IAP/_docs/Appendix%20B%20PIA%20Template.pdf , the Government of British Columbia templates and guidance documents at: http://www.cio.gov.bc.ca/cio/priv_leg/foippa/pia/pia_index.page?#DoINeedCompPIA

Privacy Impact Assessment

Project Name: _____

Document Version, Review and Approval History

Version	Author	Nature of Change	Date

Notice to Users

This document is intended to provide general information only. It is not intended nor can it be relied upon as legal advice. As an independent agency mandated to oversee compliance with *FOIPOP, MGA* and *PHIA* the Office of the Information and Privacy Commissioner (OIPC) cannot approve in advance any proposal from a public body. We must maintain our ability to investigate any complaints and to provide recommendations in response to these complaints. The contents of this document do not fetter or bind this office with respect to any matter, including any complaint investigation or other matter respecting which the Commissioner will keep an open mind. It remains the responsibility of each public body to ensure that they comply with their responsibilities under the relevant legislation. Visit us at: https://oipc.novascotia.ca.

A. General Information

1. **Name of Program or Service**

2. **Name of Department, Branch and Program Area**

3. **Name of Program or Service Representative**

4. **Contact Information**

B. Description

1. **Description of the Initiative:** Provide a summary of the program, project activity or system, describe its purposes, goals and objectives. Explain the need for the new program, project or system and its benefits.

2. **Scope of this PIA:** Explain what part or phase of the initiative the PIA covers and what it does not cover.

3. **Elements of Information or Data**: List the personal information data elements involved in the initiative. This could include citizen's name, age, address, educational history, work status, health information, financial information, photos, comments on a blog, license numbers or hiring data.

4. **Description of Information Flow (include text and diagram)**: Attach an information flow diagram showing how information will be collected and disclosed as a result of the initiative. See **Appendix A** for a sample information flow diagram.

If your initiative will not involve the collection, use or disclosure of personal information, you can stop here and submit this document to your privacy officer.

C. Collection, Use and Disclosure of Personal Information

1. **Limiting Collection, Use and Disclosure:** Privacy is a fundamental right of citizens and so any limitation on the privacy of citizens should be carefully analyzed to ensure such limitation is warranted. If your project involves highly sensitive personal information, a broad collection of personal information or a serious impingement on privacy[3] answer the following four questions before proceeding:

a. Is the measure demonstrably necessary to meet a specific need? At a minimum, the objective must relate to societal concerns which are pressing and substantial in a free and democratic society. To be "demonstrably necessary" the public body should explain the rational connection between the specific need and the project.

b. Is it likely to be effective in meeting that need? Provide empirical evidence to support the initiative.

c. Is the loss of privacy proportional to the need? Explain how the collection, use and/or disclosure of personal information will be undertaken in the least privacy invasive manner possible. Minimizing the number of data elements collected, limiting access to the data and short retention periods are all examples of reducing the privacy invasive impact.

d. Is there a less privacy invasive way of achieving the same end? Explain what other less privacy invasive methods have already been tried to meet the identified need.

Based on this analysis you may decide you do not need to collect, use or disclose personal information for your project. You may decide to reduce the data elements (you need to go back and redo part B before proceeding) or you may determine that you can justify the scope of your collection, use and/or disclosure and so proceed to question 2.

2. **Legal Authority for the Collection, Use and Disclosure of Personal Information:** For each of the collection, use and disclosures identified, evaluate your public body's legal authority and complete the following table. Refer to **Appendix B** for an example of an authorities summary table. Refer to **Appendix C** for a summary of the authorities to collect, use and disclose personal information under FOIPOP.

[3] Typically projects such as video surveillance, collection or use of GPS data, any covert surveillance, use of bio metrics etc. should be considered highly sensitive and will require this preliminary analysis.

Personal Information Authorities Summary			
	Personal Information Description/Purpose	**Type**	**FOIPOP Authority**
1.			
2.			
3.			
4.			
5.			

3. **Compliance with *Personal Information International Disclosure Protection Act*:**
PIIDPA requires that personal information in the custody or control of a public body shall not be stored or accessed outside of Canada, subject to limited exceptions (s.5(1)). Set out here whether or not there will be any proposed storage or access outside of Canada and if so, describe what *PIIDPA* exceptions apply. See **Appendix D** for a summary of the *PIIDPA* exceptions.

***Personal Information International Disclosure Protection Act* Authorities**			
	Personal Information Description/Purpose	**Type**	**PIIDPA Authority**
1.			
2.			
3.			

D. Correction, Accuracy and Retention of Personal Information

1. **Correction and Accuracy:**

a. How is an individual's information updated or corrected?
b. If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated?
c. If personal information will be disclosed to others, how will the public body notify them of the update, correction or annotation? (See s. 25 of FOIPOP for further information on correction and accuracy obligations).

2. **Retention:**

a. Does your initiative use personal information to make decisions that directly affect an individual? If yes, please explain.

b. Do you have a records retention and/or disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

E. Security of Personal Information

1. **Reasonable security:** FOIPOP requires that public bodies protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure and disposal of personal information (s. 24(3) FOIPOP).

a. **Administrative safeguards** – Describe administrative safeguards (such as policies, training, contract provisions, consent forms etc.).

b. **Technical Safeguards** – Describe technical safeguards (such as passwords and user ID, authentication, encryption, firewalls & intrusion detection, secure transmission, disaster recovery).

c. **Physical Safeguards** – Describe physical safeguards (such as secure access, laptops secured to desk, alarm systems).

d. **Auditing** – Describe auditing capability and strategies (audit logs, records of user activity, proactive and focused audit capacity).

If your initiative involves the creation of a new system, consider completing a security threat and risk assessment.

2. **Access Matrix:** Personal information should only be used and disclosed as permitted under FOIPOP. Access to personal information must be limited to those employees whose job responsibilities require that they access the personal information. Attach a copy of the user access matrix. A user access matrix will list all of the position types (eg. clerical, manager of investigations, finance director) across one axis and all of the personal information types (or file types or data modules) across the other. The matrix will identify by position which individuals will have access to the identified data. See **Appendix E** for an example of an access matrix.

F. Risk Mitigation

Assess the impact on privacy, confidentiality and security of personal information as a result of the new program or service or change & make recommendations for mitigation of privacy risks. See **Appendix F** for examples of risks and mitigation strategies.

Risk Mitigation Table

	Risk	Mitigation Strategy	Likelihood	Impact

G. Action Plan

The purpose of this section is to provide an action plan to implement the recommendations listed in section F to reduce the privacy risks that have been identified. This section will provide a mechanism to track the recommendations, as well as describe responses to the recommendations of the PIA. Ensuring the recommended mitigations are implemented according to the action plan is the program area's responsibility, and may be followed-up by the privacy officer at any point.

Privacy Risk Action Plan		
Mitigation Strategy	Steps Required & Responsible Officer	Date to be Achieved

PIA Review Date: _____

PIAs require regular review to ensure that the system, project or program has not substantially changed and to ensure that mitigation strategies have been properly implemented. In addition changes in other areas (such as technology or the implementation of other related programs) may create new risks that should be identified and mitigated. Typically the review date is selected based on the action plan – within six months of the final required completion dates is a good standard to use.

H. Approvals

Completed by:

[Insert position]

Date

Reviewed by:

Privacy Officer

Date

[Insert position]

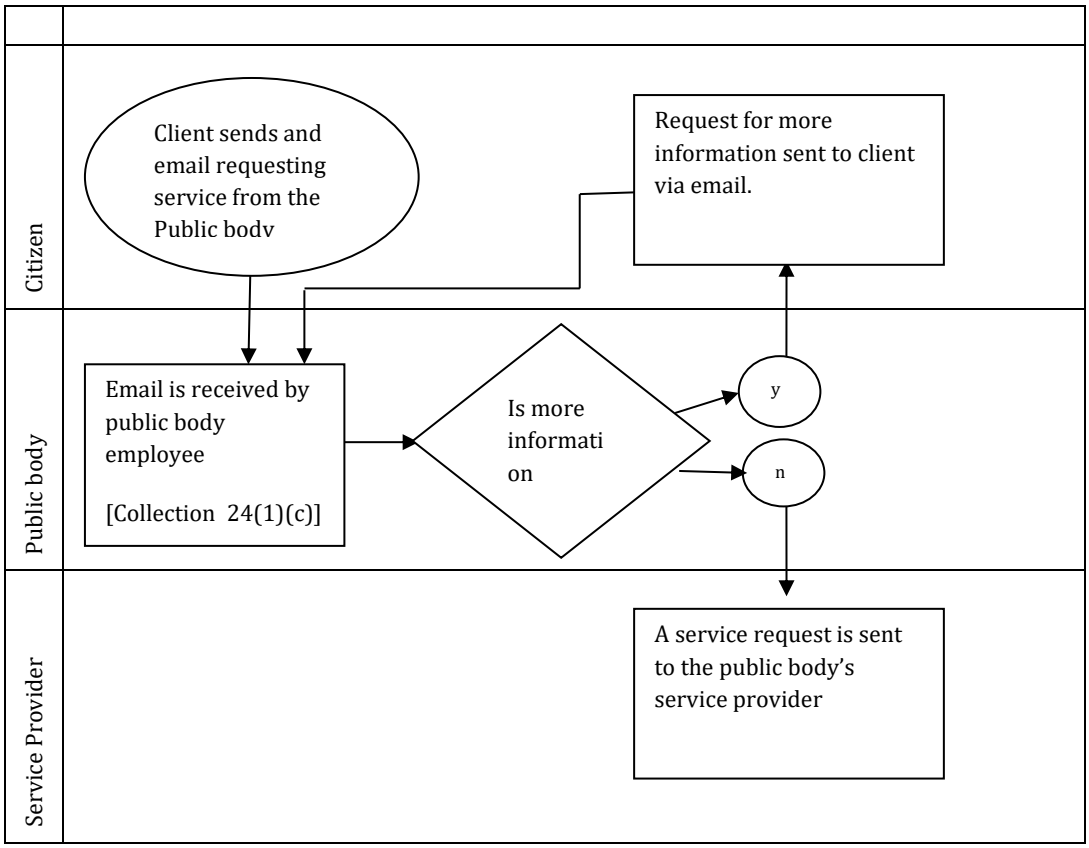
Date

Approved by:

[Insert Executive Sponsor]

Date

Appendix A: Sample Information Flow Diagram



Appendix B: Sample Authorities Summary Table

Using the example given in appendix A, the table below lists the authorities.

Personal Information Authorities Summary			
	Description/Purpose	**Type**	**FOIPOP Authority**
1.	*Email received from client requesting service*	*Collection*	*24(1)(c)*
2.	*Service request transferred to service provider contracted by public body*	*Disclosure*	*27(c)*

Appendix C: Summary of Authorities Under FOIPOP

Collection	
24(1)(a)	The collection of the information is expressly authorized by or pursuant to an enactment (identify the enactment and section)
24(1)(b)	The information is collected for the purpose of law enforcement (review the definition of law enforcement in s.3(1)(e) to ensure it applies)
24(1)(c)	The information relates directly to, and is necessary for, an operating program or activity of the public body
Use	
26(a)	Use is for the purpose for which the information was obtained or compiled, or for a use compatible with that purpose (to determine if a use if compatible review the requirements set out in s. 28)
26(b)	The individual the information is about has identified the information and has consented to the use (such consent should generally be in writing, dated and identifying the information)
26(c)	The use is for a purpose for which the information may be disclosed to the public body pursuant so s. 27 (check the disclosure list below)
Disclosure	
27(a)	In accordance with this Act or as provided pursuant to another enactment (identify the enactment and section)
27(b)	The individual the information is about has identified the information and consented in writing to its disclosure
27(c)	For the purpose for which it was obtained or compiled, or a use compatible with that purpose (to determine if a disclosure is for a compatible purpose review the requirements set out in s.28)
27(d)	For the purpose of complying with an enactment or with a treaty, arrangement or agreement made pursuant to an enactment (identify the enactment and section and attached the agreement if applicable)
27(e)	For the purpose of complying with a subpoena, warrant, summons or order issued or made by a court, person or body with jurisdiction to compel the production of information
27(f)	To an officer or employee of a public body if the information is necessary for the performance of the duties of, or for the protection of the health or safety of, the officer or employee
27(g)	To a public body to meet the necessary requirements of municipal operation

27(h)	For the purpose of collecting a debt or fine owing by an individual to the public body or making a payment owing by the public body to an individual
27(i)	To the Auditor General or other prescribed person for audit purposes
27(j)	To a member of the House of Assembly who has been requested by the individual, whom the information is about, to assist in resolving a problem
27(k)	To a representative of the bargaining agent who has been authorized in writing by the employee, whom the information is about, to make an inquiry
27(l)	To the Public Archives of Nova Scotia, or the archives of a public body for archival purposes
27(m)	To a public body or law-enforcement agency in Canada to assist in an investigation undertaken with a view to law enforcement or from which a law-enforcement proceeding is likely to result
27(n)	If the public body is a law-enforcement agency and the information is disclosed to another law-enforcement agency
27(o)	If the head of the public body determines that compelling circumstances exist that affect anyone's health or safety
27(p)	So that the next of kin or a friend of an injured, ill or deceased individual may be contacted
27(q)	For research, archival or historical purposes as provided in sections 29 and 30

Appendix D: Authority to Disclose Personal Information Outside of Canada

Personal Information International Disclosure Protection Act

Application of the Act		
4	PIIDPA does not apply to records listed in s. 4 which include: • Published material or material that is available for purchase by the public • Material that is a matter of public record	
Access and Storage Outside Canada - Authorities		
5(1)(a)	**Consent**	The individual the information is about has identified the information and has consented, in the manner prescribed by regulation, to it being stored in or access from outside Canada.
5(1)(b)	**PIIDPA Disclosure**	The information is stored or accessed outside of Canada for the purpose of disclosure allowed under PIIDPA (see list below)
5(1)(c)	**Permission**	The head of the public body has allowed storage outside of Canada pursuant to s. 5(2): • If the head considers the storage or access is to meet the necessary requirements of the public body's operation, (subject to any restrictions or conditions the head considers advisable) • The head must report the access or storage decision to the Minister within the timeline set out in the Act (s. 5(3))
Disclosure Outside Canada - Authorities		
9(2)(b)	**Consent**	The individual the information is about has identified the information and consented, in writing, to its disclosure inside or outside Canada
9(2)(c)	**Enactment**	In accordance with an enactment of the Province, the Government of Canada or the Parliament of Canada that authorizes or requires its disclosure
9(2)(d)	**Agreement**	In accordance with a provision of a treaty, arrangement or agreement that authorizes or requires its disclosure and is made under an enactment of the Province, the Government of Canada or the Parliament of Canada
9(2)(e)	**To head**	To the head of the public body, if the information is immediately necessary for the performance of the duties of the head
9(2)(f)	**To employee**	To an employee of the public body and the information is immediately necessary for the protection of the health or safety of the employee
9(2)(g)	**To legal counsel**	To legal counsel for the public body, for use in civil proceedings involving the Government of the Province or the public body

9(2)(h)	**Debts**	To collect moneys owing by an individual to the Province or public body or for making a payment owing by the Province of public body
9(2)(i)	**Motor vehicle**	For the purpose of licensing or registration of motor vehicles or drivers or verification of motor vehicle insurance, registration or drivers' licences
9(2)(i)	**Compelling circumstances**	Where the head of the public body determines that compelling circumstances exist that affect anyone's health or safety
9(2)(k)	**Next of kin**	So that next of kin or a friend of an injured, ill or deceased individual may be contacted
9(2)(l)	**Research** **Public Archives**	For a research purposes in accordance with s. 10 To a provincial or public body archive in accordance with s. 11
9(3)	**Law enforcement**	A public body that is a law enforcement agency may disclose to another law enforcement agency in Canada or in a foreign country under an agreement or enactment of Canada or the province
9(4)	**Temporary**	The head of a public body may allow an employee to transport personal information outside Canada temporarily if the head considers it is necessary for the performance of the duties of the employee to transport the information in a computer, cell phone or other mobile device.

Appendix E: Sample Access Matrix

The following example is for a database intended to manage landlord and tenant complaint information. Access to personal information must be strictly limited to those needing the information to carry out their job duties. Depending on how duties are assigned, it may be the clerk's responsibility to input the initial information identifying the landlord, tenant and the complaint summary. If this is not true, then limit the clerk's access to those data elements required.

The Deputy Minister would not typically have access to a database of this nature and so has not been assigned any access rights in the matrix below. The matrix assumes that the landlord and tenant identity information is not contained in the complaint summary nor in the enforcement outcome. The investigation notes could, of course, contain a variety of information including personally identifiable information of the landlord and tenant.

	Landlord Information[4]	**Tenant Information**	**Complaint summary**	**Investigation Notes**	**Enforcement Outcome**
Clerical	✓	✓	✓		✓
Program Director	✓	✓	✓		✓
Manager of investigations	✓	✓	✓	✓	✓
Investigator	✓	✓	✓	✓	✓
Deputy Minister					

[4] Identification information would include name, address and other contact information. This module may be common across a variety of databases.

Appendix F: Sample Risks and Mitigation Strategies

You will need to adopt a scale to measure likelihood and impact. High, medium and low will do or you can choose a numerical scale for greater subtlety in choice.

	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1	Authorized user views record for personal reasons	• Log all read only and change activity • Monitor logs regularly, conduct spot audits and ensure audit capacity in response to complaints • Oath of employment and confidentiality agreements • Training	Likelihood increases with more users	• More sensitive data results in higher impact • More data exposed by incident results in higher impact
2	Service provider fails to report privacy breach to public body.	Contractual terms: • require reporting within 24 hours • impose penalties for failure to report and late reporting • require the service provider to log all read only and change activity and to monitor the logs regularly • permit the public body to conduct audits and to review service provider audit logs	• Experience with the service provider may help determine this • Severity of consequences for service provider may lower the likelihood	Same considerations as above
3	Client's personal information is compromised when transferred to the service provider	Transmission is encrypted and over a secure line	Low – depending on the quality of the encryption	Same as above

This document was prepared by the Office of the Information and Privacy Commissioner for Nova Scotia. We can be reached at:

PO Box 181 Halifax NS B3J 2M4
5670 Spring Garden Road, Suite 509, Halifax
Telephone: 902-424-4684
Toll-free: 1-866-243-1564
TDD/TTY: 1-800-855-0511
https://oipc.novascotia.ca