Access & Privacy Essentials Toolkit

For Universities & Colleges

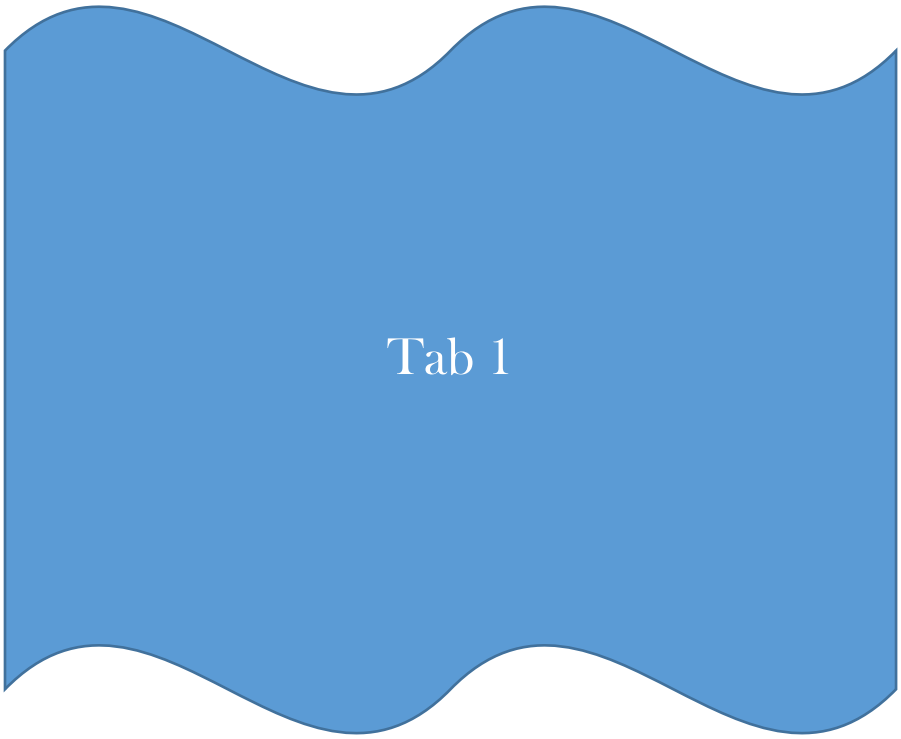
Office of the Information and Privacy Commissioner for Nova Scotia
oipcns@novascotia.ca 902-424-4684 https://oipc.novascotia.ca

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 Information and Privacy Commissioner for Nova Scotia 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 .

Contents

Access to Information Rules & Tools


Tab 1

FOIPOP Access Rules – At a Glance

Access to Information Rules		
Request Processing Essentials		
2	Purpose	• Sets out the purposes of the Act.
4(1)	Records	• Act applies to all records in the custody or under the control of a public body.
4(2)	Exceptions	• Notwithstanding s. 4(1) the Act does not apply to 10 record types including: ○ Published material or material that is available for purchase by the public, ○ A record of a question that is to be used on an examination or test.
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. • *FOIPOP* Regulations set amounts and limit the services for which fees may be charged.
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.

Exemptions		
Certain types of information may be exempted from disclosure. There are two types of exemptions: discretionary and mandatory.		
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: ○ Harm the security of a system ○ The information is a law enforcement record and disclosure is an offence pursuant to an enactment ○ Result in civil liability or harm proper custody ○ Does not apply to a decision not to prosecute

Discretionary Exemptions cont'd		
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 of a governing body 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 • Governing body includes faculties and the senate of a university (Regulations s. 19)
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

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)

Notice

This table is intended 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* at: http://nslegislature.ca/legc/statutes/freedom%20of%20information%20and%20protection%20of%20privacy.pdf

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 and local 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 Information and Privacy Commissioner for Nova Scotia. The access rules in *FOIPOP* are similar and in some places identical to rules found in every other access to information law across Canada.

Universities and the Nova Scotia Community College are local public bodies under *FOIPOP*. Under *FOIPOP* "university" means a person, association or corporation that is authorized by the *Degree Granting Act* to grant any recognition of academic achievement that is called a degree (s. 3(1)(o)). Public bodies include "local public bodies".

FOIPOP requires local public bodies, by by-law or other legal instrument, designate a head for the purposes of *FOIPOP* (s. 49A and s. 3(1)(c)).

Is it "FOI able"?
Unless specifically excepted from *FOIPOP*, **all** records in the custody or under the control of universities are subject to the right of access. Generally all of a university's records are "FOI able" including university 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 *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 may be "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 university must withhold the information. A discretionary exemption is one where if all of the requirements are met, the university may or may not withhold the information. The university 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.

Tab 1: *FOIPOP* – Access Rules At a Glance

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

How to Process an Access to Information Request

Universities should have in place a process for managing access to information requests. Review the tools listed below to get a sense of the steps necessary to process an access to information request.

Tab 2: Life Cycle of a Typical Access to Information Request

Tab 3: Request Processing Checklist

In the course of processing the request you will need to consider whether or not to charge fees and whether or not you need to take or request a time extension.

Tab 4: Time Extension Guidelines

How to Sever a Document

1. Read the document carefully, make sure you understand the content. Talk to the business area that produced the record if you need help understanding the document and its purpose.
2. Read all 11 exemptions to disclosure carefully so you have a sense of what information might fall within the exemptions. You may decide none apply. You may decide that one or two stand out as possibly applying to the record.

The exemptions that apply generally to public bodies apply to local public bodies. In addition, *FOIPOP* provides a number of exemptions aimed specifically at local public bodies including:

- s. 19A – closed meetings of local public bodies (see also Regulations s. 19)
- s. 19B – academic research
- s. 19C – certain personal information (appointments, admission, awards & research evaluation)
- s. 19D – certain hospital records (hospitals are also considered to be local public bodies)

3. Do some research on how the exemptions might apply to the type of record you are reviewing. Talk to your colleagues in other universities and colleges, check your files to see if your university has had previous similar requests and read the information available on the Information and Privacy Commissioner's website.
4. Carefully review the record with the exemption in mind. Make sure that any information you sever (redact) satisfies all of the requirements of the exemption.

Tab 5: How to Sever a Document

Best Practices
Some best practices for administering an access to information program are:

- **Copy of *FOIPOP***: Have a copy of *FOIPOP* at your side. Always refer carefully to the sections summarized in the FOIPOP Access Rules – At a Glance document on page 5 of this document.

- **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 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 *FOIPOP* 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.
  Tab 6: Standard Routine Release List for Universities (includes ideas of what to include in your routine release list)

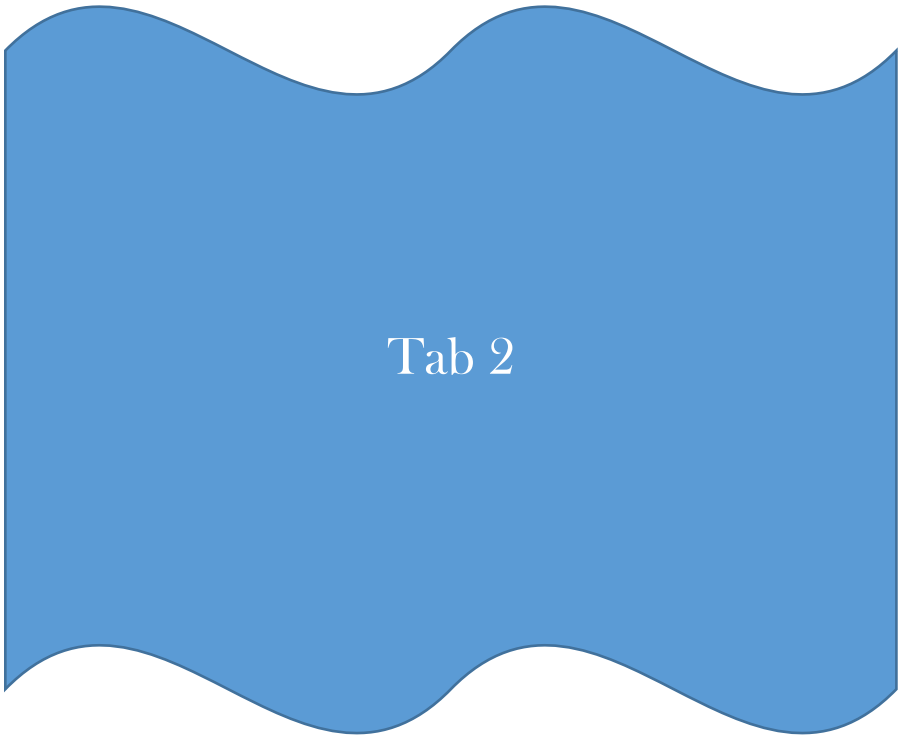
- **Records Retention – Manage Your Records:** Each university should have in place an approved records retention policy. We have created a records retention template with some recommended retention periods for records typically found at universities. The template is based on retention policies of several Canadian universities.
  Tab 7: Records Retention Policy Template

- **Communication – Manage the Applicants:** Always have a conversation with the applicant. Make sure you are clear about what he/she wants and that he/she is clear about your process.

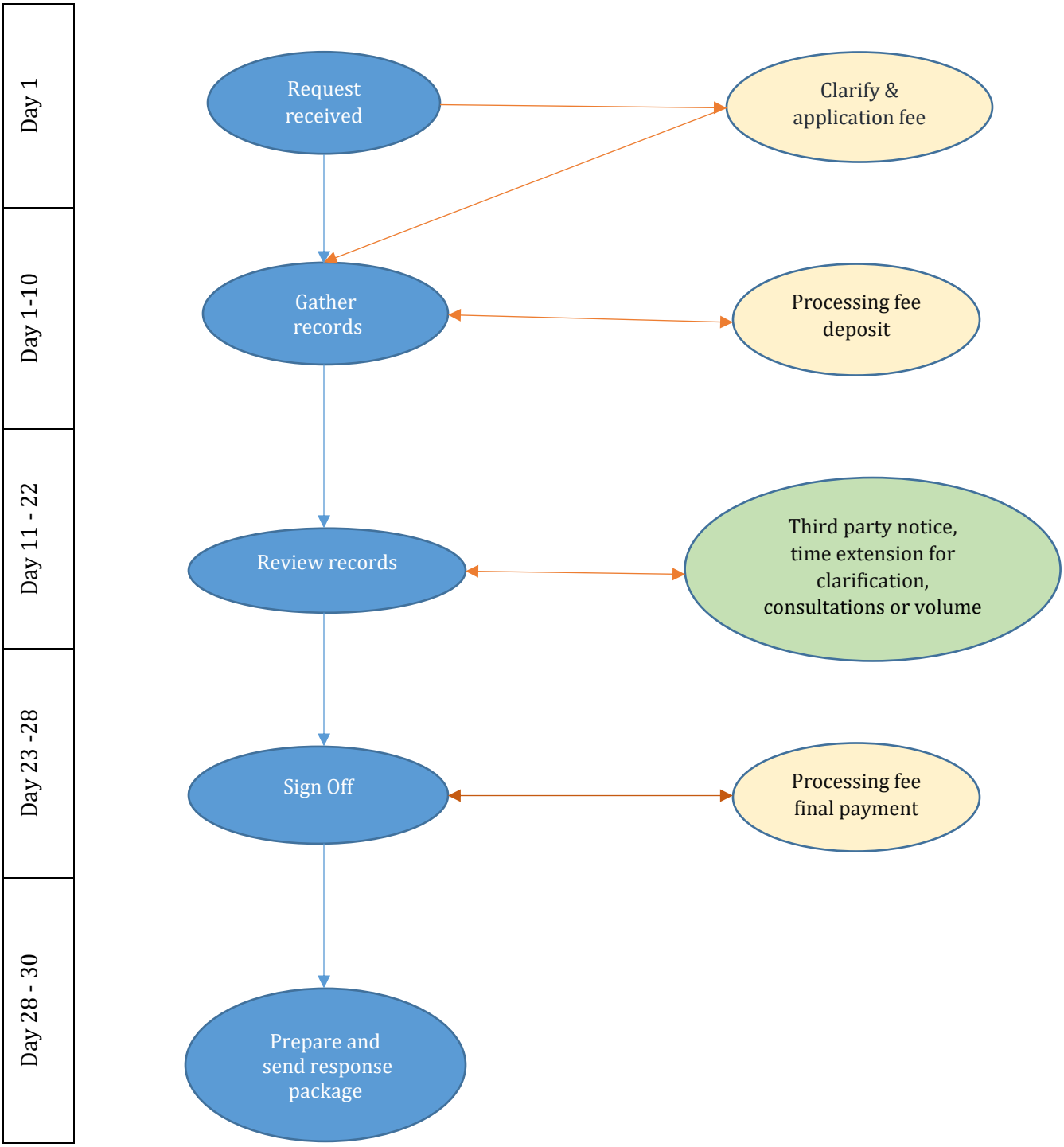
- **Communication – Manage Your Business Areas:** You cannot be effective in your role if you are not trusted and seen as an expert. You need business areas to cooperate by providing all of the responsive records in a timely fashion. You need them to trust that you know how to apply the *FOIPOP* rules.

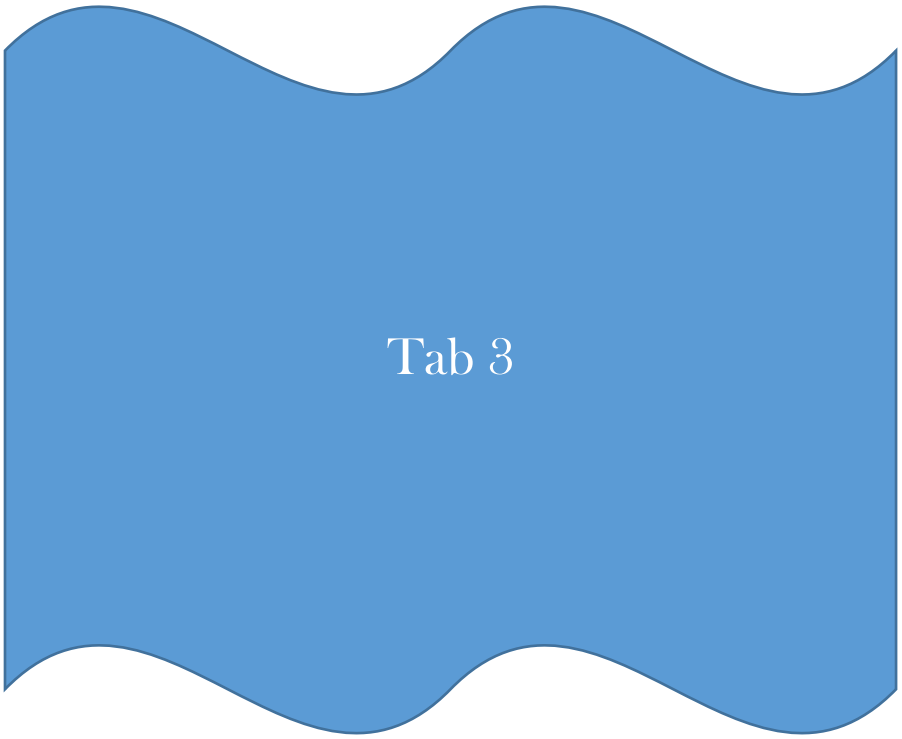
- **Communication – Manage Third Parties:** Often applicants are interested in business-related information such as contracts and proposals that third parties have an interest in. It is very important to take the time to understand when the third party business exception applies and to provide good information to the third party including: a copy of the document at issue, suggestions for what may be withheld and what cannot be withheld under this exception (such as public information or information taken straight from the university's public request for proposal document).

- **Buy-In from the Top –** Keep your executive well informed about your access to information (and protection of privacy) program. Make sure they know the basic rules so that you have their support when you make decisions.


Tab 2

Life Cycle of a Typical Access to Information Request



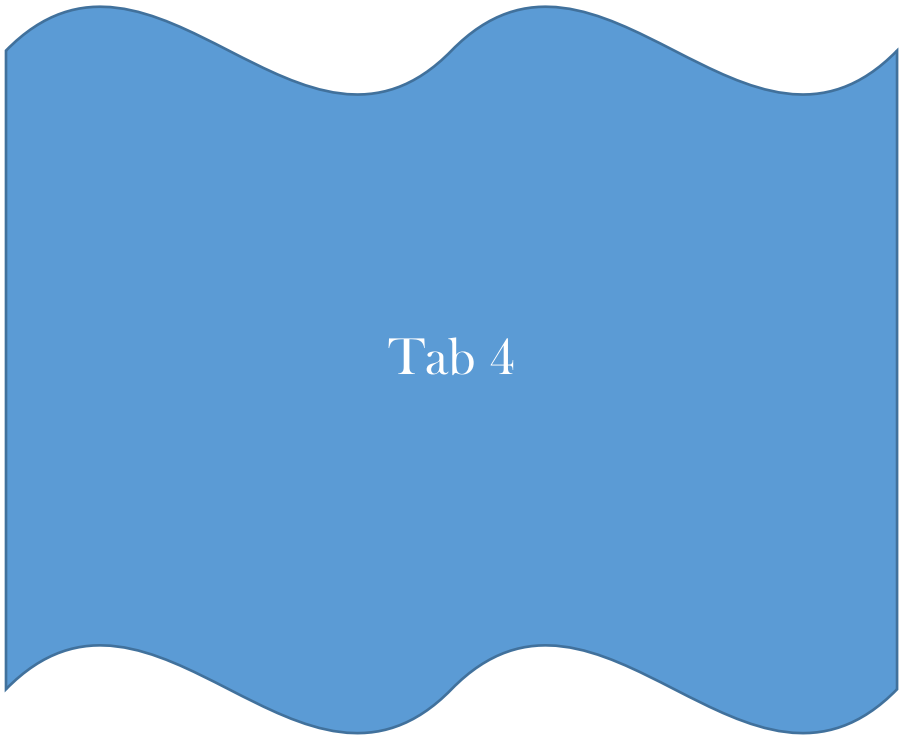

Tab 3

Request Processing Checklist			
Task	**Description**	**Timeline**	**Done**
Review request	• Clarify if necessary. • Check if material is already public and released. (s. 4(1) and(2))	Day 1 - 3	
Application fee	• Ensure fee received for general requests only. (s. 11(4))	Day 1	
30 day clock	• Start the clock. (s. 7(2))	Day 1	
Acknowledgement letter	• Send the applicant an acknowledgment letter confirming record requested, explaining where, when and how access will be given. (s. 7(2)(a)(i)) • Best practice is to call the applicant to ensure you're communicating well in terms of scope of request, anticipated fees and timelines. (s. 7(1)))	Day 1-2	
Call for records	• Email copy of record request to all relevant business areas – do not disclose identity of applicant. • Within 5 days, follow up with business area to ensure search is progressing.	Day 1-10	

Processing fee required	• Determine if more than two hours of searching is required, if so consider whether fee is required. (s. 11(3))
	• Calculate fee if necessary – ensure it is evidence-based.
	• Send the applicant a fee deposit request:
	  ○ advise him/her of the right to request a fee waiver (s. 11(5) and 11(7)),
	  ○ advise him/her of due date for payment (close file if payment not received),
	  ○ advise him/her of the right to request a review of the fee.
	• Stop the clock pending payment of the fee deposit if applicable. (s. 7(2))
		Day 1-5	

Review records	**Step 1** – Read briefly to ensure that the package is complete, if not, go back to the business areas to ensure response is accurate and complete. **Step 2** –Remove exact duplicates. **Step 3** – Number the pages of the records and make a clean copy. **Step 4** – On your working copy read the package carefully, highlight any portion where an exemption may apply. Note the exemption beside the severing (not at the top of the page.) **Step 5** – Determine if any third party consultations are required and if so, send a letter to the third party with a copy of the relevant records to obtain their comment. (s. 22(1)) **Step 6** – For each exemption considered, review the meaning of the exemption to determine if all requirements of the exemption have been met.	Day 11 - 22	

Request Processing Checklist Cont'd			
Task	**Description**	**Timeline**	**Done**
Review records cont'd	**Step 7** – for any discretionary exemption applied, determine whether discretion should be exercised in favour of disclosure. Note on file the factors you considered in exercising discretion.	Day 11-22	
Time extension	• If the package contains a high volume, requires third party consultations, or requires further clarification you may take a time extension of up to 30 days. (s. 9(1)). • If more than 30 days are required, you may request a further time extension from the Information and Privacy Commissioner. • Write to the applicant to advise him/her of any time extension, the reason for the extension, and that he/she may complain to the Information and Privacy Commissioner.	Day 1- 30	
Sign off	• Prepare sign off memo explaining exemptions and any recommended exercise of discretion. • Prepare a copy of the records for review by the sign off authority (always keep a copy in your file). • Give due date and follow up.	Day 23 - 28	
Processing fees	• If fees were charged, go back to the program area to confirm the actual search time. • Recalculate the fee to determine the actual fee, compare it with the fee estimate and determine if any further fee payment or refund is required. • If a final payment is required, contact the applicant in writing to request final payment. Put the request on hold pending payment.	Day 23	
Response package	• Prepare a response letter to the applicant that satisfies all of the requirements of s. 7(2). • Send the response package to the applicant – keep an exact copy of everything you sent to the applicant.	Day 28 - 30	
Close file	• Close your file once the package has been sent. • Always keep a copy of the original record, the record showing your redactions (if any) and a copy of the actual version released to the applicant.	Day 30	


Tab 4

Time Extension Guidelines

INTRODUCTION

Under section 9 of the *Freedom of Information and Protection of Privacy Act* (*FOIPOP*) public bodies may take a thirty day time extension in prescribed circumstances. A further time extension may be granted with the permission of the Information and Privacy Commissioner.[1] These guidelines are intended to assist public bodies with establishing whether the conditions apply for requesting time extensions under section 9(1). By submitting the requested information to the Information and Privacy Commissioner when a further time extension is sought the Information and Privacy Commissioner will have the information required to determine whether a further time extension is authorized.[2]

LEGISLATION

Extension of time for response

9(1) The head of a public body may extend the time provided for in sections 7 or 23 for responding to a request for up to thirty days or, with the Information and Privacy Commissioner's permission, for a longer period if

(a) the applicant does not give enough detail to enable the public body to identify a requested record;
(b) a large number of records is requested or must be searched and meeting the time limit would unreasonably interfere with the operations of the public body; or
(c) more time is needed to consult with a third party or other public body before the head of the public body can decide whether or not to give the applicant access to a requested record.

(2) Where the time is extended pursuant to subsection (1), the head of the public body shall tell the applicant

(a) the reason;
(b) when a response can be expected; and
(c) that the applicant may complain about the extension to the Review Officer.

[1] 1 The Information and Privacy Commissioner for Nova Scotia is also known as the Review Officer and is appointed as the independent oversight authority under the Freedom of Information and Protection of Privacy Act, the Municipal Government Act, the Personal Health Information Act, and the Privacy Review Officer Act

[2] These guidelines were adapted from similar guidelines prepared by the Offices of the Information and Privacy Commissioners in Alberta, Ontario, Newfoundland and British Columbia.

A NOTE ABOUT STATUTORY TIMELINE

Sections 6, 7, 9 and 22(3) of *FOIPOP* are crucial to understanding and applying the statutory timelines for responding to access requests. A public body may only suspend a statutory timeline if it is authorized under s. 7(2). If an application has been received and an applicant has met the requirements of s. 6(1)(b) and (c), the public body has 30 days to respond to the access request. A public body's decision to put a request "on hold" (i.e. stop the clock) does not suspend the statutory timeline if there is no authority to do so under s. 7(2).

If the statutory deadline for responding has passed, a public body is not authorized by s. 9(1) to extend the time for responding. Similarly, if the deadline for responding has passed the Information and Privacy Commissioner cannot grant a time extension under s. 9(1).

Clarify or Narrow?

It is important to understand the difference between a clarified request and a narrowed request. To "clarify" is to make clear what the requester is seeking – so that you are able to identify the record sought. To "narrow" is to reduce the scope of the request, i.e. decreasing the number of records requested. Time extensions for clarification are contemplated under s. 9(1)(a) discussed below.

APPLICATION

Under s. 9(1) of *FOIPOP* there are three circumstances in which the Information and Privacy Commissioner may give a public body permission to extend the time for responding to an access request. Permission may be granted if one or more of ss. 9(1)(a), (b) or (c) apply.

(1) SECTION 9(1)(a) – FAILURE TO PROVIDE SUFFICIENT DETAIL

This provision applies when an applicant does not give enough detail to enable the public body to identify a requested record. If the public body can identify the requested record but is seeking to narrow the scope of the request s. 9(1)(a) would not apply.

Test: When applying for a time extension, the public body must explain why more detail is required to identify a record.

Other Relevant Information:

- Dates of request and follow up with applicant, including efforts made by the public body to contact the applicant and clarify the request.
- If the public body has already requested further details, what is the expected response date?

(2) SECTION 9(1)(b) – VOLUME & UNREASONABLE INTERFERENCE

This provision applies when a large number of records have been requested or must be searched ***and*** meeting the time limit would unreasonably interfere with the operations of the public body.

Test: The public body must demonstrate that:

1) a large number of records have been requested or must be searched, **and**
2) meeting the time limit would unreasonably interfere with the operations of the public body.

Both a large volume of records and unreasonable interference with operations must be present in order to meet the test for s. 9(1)(b). Consider the following factors in evaluating whether or not s. 9(1)(b) applies:

Volume:

- How many pages?
- Do the records require special handling?
- Does the type of record require different methods of searching or handling?
- How does volume compare with average request volume?
- Existence of previous requests for the same or similar records

Circumstances that may contribute to unreasonable interference:

- Significant increase in access requests (e.g., sharp rise over 1-4 months)
- Significant increase in administrator caseloads (sharp rise in average caseload)
- Computer systems or technical problems
- Unexpected leave
- Unusual number (high percentage) of new administrators-in-training
- Program area discovers a significant amount of additional records
- Type of records (e.g. maps, photographs, etc.)
- Multiple formats of records (e.g. database, email and hard copy records are all responsive to the access request)
- Number of program areas searched
- Location of records (e.g. records held in multiple locations, records stored off-site or regionally)
- Degree to which the subject matter expertise of the department holding the records will be diverted to the department's detriment

Invalid Circumstances:

- The operation has not been allocated sufficient resources
- Long term or systemic problems
- Vacations
- Office processes (e.g., sign-off)
- Personal commitments
- Pre-planned events (e.g., retirements)
- Previous s. 9(1) extension taken and no work done on file
- Type of applicant (media, political, etc.)

Other Relevant Information:

- The public body made attempts to correct a mistake in processing the request
- The public body communicated with the applicant
- The public body made a phased release
- The public body provided reasonable release dates
- The public body waived fees

(3) SECTION 9(1)(c) – CONSULTATION REQUIRED

Section 9(1)(c) applies when more time is needed to consult with a third party or other public body before the public body can decide whether or not to give the applicant access to a requested record. Note that "third party" and "other public body" do not include programs or branches within the same public body. The implication is that consultation is done for the purpose of deciding whether or not to give access. Because of s. 22(3) the time limit set out in s. 7(2) continues to apply even when third party notice is required but that time may be extended pursuant to s. 9.

Test: The public body needs to explain why it is necessary to consult with a third party or other public body in order to make a decision about access, including how the third party or other public body is expected to assist. Also, the public body needs to explain why it needs more time to do this.

Some valid reasons for consulting:

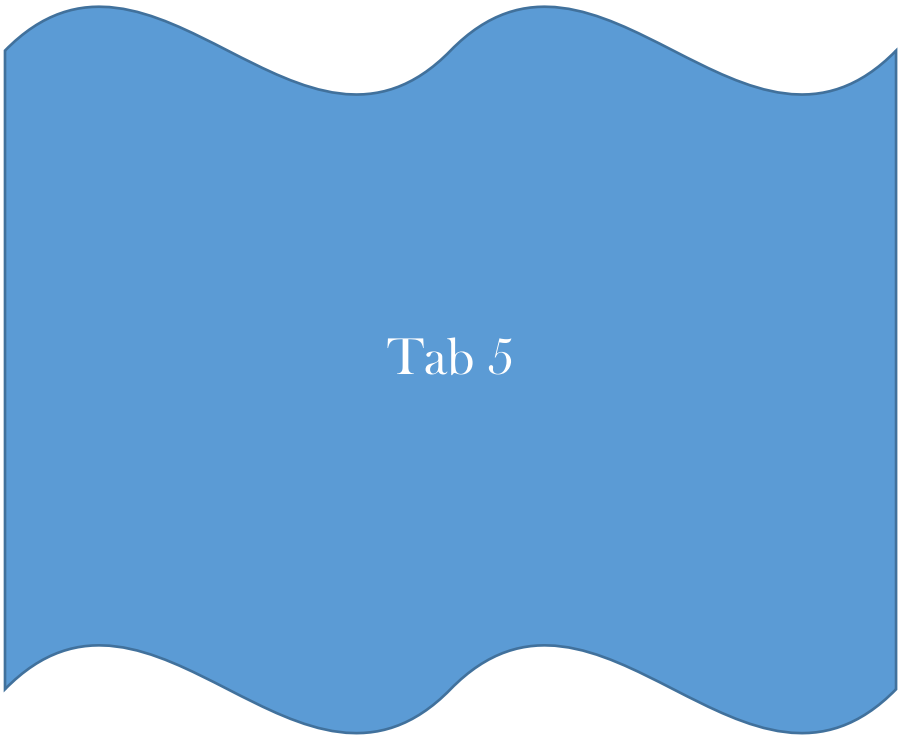
- Third party or other public body has an interest in the records
- Records created or controlled jointly
- The public body must give third party notice pursuant to s. 22.

Other Relevant Information:

- When did public body initiate consultation?
- Explanation for any delay in initiating consultations
- Number of consultations required
- Number of pages sent for consultation
- Availability of third party or public body contacts
- Did public body set deadline expectations for third party or other public body?
- Is time required for consultation reasonable?
- Has the public body followed up on consultation request?
- Has the public body proceeded with a phased release?

Invalid Circumstances:

- Consultations with staff in same public body, e.g., legal counsel or program area
- Consultations for a purpose other than deciding whether to give access


Tab 5

How to Sever A Document

1. Read the document carefully and thoroughly. Make sure you understand the content. Talk to the business area that produced the record if you need help understanding the document and its purpose.

2. Read all 11 exemptions to disclosure carefully so you have a sense of what information might fall within the exemptions. You may decide none apply. You may decide that one or two stand out as possibly applying to the record.

3. Do some research on how the exemptions might apply to the type of record you are reviewing. Talk to your colleagues in other universities and colleges, check your files to see if your university has had previous requests, read the information available on the Information and Privacy Commissioner's website.

4. Carefully review the record with the exemption in mind. Make sure that any information you sever (redact) satisfies all of the requirements of the exemption.

There are several exemptions that are the most commonly applied exemptions. Below are disclosure exemption fact sheets for the following exemptions:

- Section 20 (personal information)
- Section 21 (third party business information)
- Section 16 (solicitor-client privilege)
- Section 18 (threat to safety)

Disclosure Exemption Fact Sheet #1
s. 20 FOIPOP - Personal Information of a Third Party

Is it an "unreasonable invasion of personal privacy"?

When you receive an access to information request which includes a request for the personal information of a third party, you must determine whether or not disclosing the personal information of a third party would be an "unreasonable invasion" of the third party's personal privacy. This is the test set out in s. 20 of *FOIPOP*:

20 (1) The head of the public body shall refuse to disclose personal information to an applicant, if the disclosure would be an unreasonable invasion of a third party's personal privacy.

Applying the test involves a four step process.

Step 1: Is it personal information?

Section 3
(i) "personal information" means 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;

For an example of how to evaluate whether information is "personal information", see recent review reports on this issue listed below.

Tip #1: Just because the record contains third party personal information, such as a name, it does not necessarily mean that you must withhold that information. You must complete all four steps of this process to decide if disclosing the information would be an unreasonable invasion of the third party's personal privacy.

Tip #2: Just because there are no names in a record does not necessarily mean that it does not contain personal information. If the information is about an identifiable individual it is "personal information". For example, if the record includes a photograph, an identity number, or a description of a person, each of these pieces of information may be considered to be personal information.

Step 2: Is the disclosure listed as "<u>not</u> an unreasonable invasion of personal privacy" in s. 20(4)?

Next, evaluate if the proposed disclosure falls into one of the categories set out in s. 20(4). If it does, the disclosure is not an unreasonable invasion of a third party's personal privacy – s. 20 does not apply.

20(4) A disclosure of personal information is not an unreasonable invasion of a third party's personal privacy if

(a) the third party has, in writing, consented to or requested the disclosure;
(b) there are compelling circumstances affecting anyone's health or safety;
(c) an enactment authorizes the disclosure;
(d) the disclosure is for a research or statistical purpose and is in accordance with Section 29 or 30;
(e) the information is about the third party's position, functions or remuneration as an officer, employee or member of a public body or as a member of a minister's staff;
(f) the disclosure reveals financial and other similar details of a contract to supply goods or services to a public body;
(g) the information is about expenses incurred by the third party while travelling at the expense of a public body;
(h) the disclosure reveals details of a licence, permit or other similar discretionary benefit granted to the third party by a public body, not including personal information supplied in support of the request for the benefit; or
(i) the disclosure reveals details of a discretionary benefit of a financial nature granted to the third party by a public body, not including personal information that is supplied in support of the request for the benefit or is referred to in clause (c) of subsection (3).

If the information falls into s. 20(4) stop here. The proposed disclosure is not an unreasonable invasion of personal privacy and s. 20 does not apply. Other exemptions might apply, but not s. 20.

Information in university records that may fall under s. 20(4) are the identity, title and remuneration of employees (s.20(4)(e)), the details of a contract to supply goods or services to the university (s. 20(4)(f)), and information about expenses incurred by an employee and reimbursed by the university (s. 20(4)(g)).

Another way s. 20(4) may apply to the records is if you seek and obtain consent from the third party to disclose the record. Section 22 sets out the process for obtaining consent from a third party. Best practice is to, where practicable, give written notice to the third party of the request for his/her personal information. Include in the notice a copy of the document at issue and include your proposed severing. These types of notices can be tricky because third parties are unlikely to agree to a disclosure of their personal information unless they know who is asking. You cannot disclose the identity of the requester unless you have his or her permission. You should feel free to ask the applicant/requester if you can disclose his or her identity to third parties. If the applicant/requester agrees, you can disclose his or her identity to the third party when you give notice. Follow the timelines for giving notice set out in s. 22. (See page 29 for a further discussion of the third party notice timelines.)

Step 3: Is the disclosure a presumed unreasonable invasion of privacy?

If s. 20(4) does not apply, then consider whether s. 20(3) applies. This section lists all of the circumstances where the disclosure is a presumed unreasonable invasion of a third party's personal privacy.

20(3) A disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy if

(a) the personal information relates to a medical, dental, psychiatric, psychological or other health-care history, diagnosis, condition, treatment or evaluation;

(b) the personal information was compiled and is identifiable as part of an investigation into a possible violation of law, except to the extent that disclosure is necessary to prosecute the violation or to continue the investigation;

(c) the personal information relates to eligibility for income assistance or social-service benefits or to the determination of benefit levels;

(d) the personal information relates to employment or educational history;

(e) the personal information was obtained on a tax return or gathered for the purpose of collecting a tax;

(f) the personal information describes the third party's finances, income, assets, liabilities, net worth, bank balances, financial history or activities, or creditworthiness;

(g) the personal information consists of personal recommendations or evaluations, character references or personnel evaluations;

(h) the personal information indicates the third party's racial or ethnic origin, sexual orientation or religious or political beliefs or associations; or

(i) the personal information consists of the third party's name together with the third party's address or telephone number and is to be used for mailing lists or solicitations by telephone or other means.

If the information at issue falls into one of the categories under s. 20(3) then disclosing it is a presumed unreasonable invasion of the third party's personal privacy. This presumption can be rebutted. Always move on to step 4 before making a final decision.

Information in university records that typically falls under this section is personal information about a disciplinary matter. This is considered employment history (s. 20(3)(d)). Another example is medical leave information of an employee. This is considered medical or health care history (20(3)(a)). Information contained on a resume may fall into s. 20(3)(d) as employment or educational history.

Just because s. 20(3) applies does not mean the information cannot be disclosed. But there is a presumption that disclosing this information would result in an unreasonable invasion of personal privacy and so evidence would be required showing that other factors outweigh this presumption. Proceed to the final step below to conduct this assessment.

Step 4: Consider all relevant circumstances

Following step 3 you will have determined either that the disclosure is a presumed unreasonable invasion of a third party's personal privacy or it is not. In either case, you must still decide whether or not you may disclose the information. You do so by considering all of the relevant factors including (but not limited to) factors listed in s. 20(2).

20 (2) In determining pursuant to subsection (1) or (3) whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy, the head of a public body shall consider all the relevant circumstances, including whether

(a) the disclosure is desirable for the purpose of subjecting the activities of the Government of Nova Scotia or a public body to public scrutiny;
(b) the disclosure is likely to promote public health and safety or to promote the protection of the environment;
(c) the personal information is relevant to a fair determination of the applicant's rights;
(d) the disclosure will assist in researching the claims, disputes or grievances of aboriginal people;
(e) the third party will be exposed unfairly to financial or other harm;
(f) the personal information has been supplied in confidence
(g) the personal information is likely to be inaccurate or unreliable; and
(h) the disclosure may unfairly damage the reputation of any person referred to in the record requested by the applicant.

Other factors that the Commissioner has considered a relevant within the meaning of s. 20(2) are:

- Sensitivity of the information
- Passage of time
- Death of the third party
- Compassion for family members
- Purposes of the Act

Weigh all of the factors for and against disclosure of the personal information, including any presumed unreasonable invasion of personal privacy. Then make a decision that addresses the test in s. 20(1) - would the disclosure be an unreasonable invasion of a third party's personal privacy?

Recent Examples:
Recent examples of the application of this process to are:

Review Report 16-02:	UserIDS, incident reporting form
Review Report 16-03:	Former foster child seeks father's name
Review Report 16-08:	Death scene photographs requested by mother of deceased
Review Report FI-10-19	Workplace investigation
	https://oipc.novascotia.ca/

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 for Nova Scotia cannot approve in advance any proposal from a municipality. 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 Information and Privacy Commissioner for Nova Scotia will keep an open mind. It remains the responsibility of each municipality to ensure that they comply with their responsibilities under the relevant legislation. Visit us at: https://oipc.novascotia.ca/

Disclosure Exemption Fact Sheet #2
s. 21 FOIPOP – Third Party Business Information

Section 21 of *FOIPOP* is a mandatory exemption which means if all of the requirements of the section are satisfied, the information must be withheld. This exemption has a three part test to it; all three parts must be satisfied for the section to apply.

Step 1: Is the information commercial, financial or technical information of a third party? (s. 21(1)(a))
Step 2: Was the information supplied in confidence? (s. 21(1)(b))
Step 3: Is there evidence of a reasonable expectation of harm? (s. 21(1)(c))

How to Apply the Third Party Business Information Exemption

Another issue that must be considered is whether or not the third party business should be given notice of the access to information request. The notice serves two purposes: to provide the university with information that may assist in determining whether the requirements of s. 21 of *FOIPOP* are met and to determine if the third party is willing to consent to the disclosure of the information. See page 29 for a discussion of how to give third party notice.

Confidential information
21 (1) The head of a public body shall refuse to disclose to an applicant information
(a) that would reveal
(i) trade secrets of a third party, or
(ii) commercial, financial, labour relations, scientific or technical information of a third party;
(b) that is supplied, implicitly or explicitly, in confidence; and
(c) the disclosure of which could reasonably be expected to
(i) harm significantly the competitive position or interfere significantly with the negotiating position of the third party, 24 freedom of information and protection of privacy
(ii) result in similar information no longer being supplied to the public body when it is in the public interest that similar information continue to be supplied,
(iii) result in undue financial loss or gain to any person or organization, or
(iv) reveal information supplied to, or the report of, an arbitrator, mediator, labour relations officer or other person or body appointed to resolve or inquire into a labour-relations dispute.

(2) The head of a public body shall refuse to disclose to an applicant information that was obtained on a tax return or gathered for the purpose of determining tax liability or collecting a tax.

(3) The head of a public body shall disclose to an applicant a report prepared in the course of routine inspections by an agency that is authorized to enforce compliance with an enactment.

(4) Subsections (1) and (2) do not apply if the third party consents to the disclosure.

Step 1: Is the information commercial, financial or technical information of a third party? (s. 21(1)(a))

"commercial or financial"

- Dictionary meanings provide the best guide and it is sufficient for the purposes of the exemption that information relate or pertain to matters of finance, commerce, science or technical matters as those terms are commonly understood.
- The information at issue need not have an inherent value, such as a client list might have for example. The value of information ultimately depends upon the use that may be made of it, and its market value will depend upon the market place, who may want it and for what purposes; a value that may fluctuate widely over time.
- Information in agreements relating to global contract amounts, or prices, expenses and fees can qualify as commercial or financial information of third parties.

"technical information"

- Information belonging to an organized field of knowledge which would fall under the general categories of applied sciences or mechanical arts. Examples of these fields would include architecture, engineering or electronics. It will usually involve information prepared by a professional in the field and describe the construction, operation or maintenance of a structure, process, equipment or thing.
- Plans that show the exterior design and dimensions of a house can qualify as technical information.

"of a third party"

- Information that has already been made public, is of a standard nature, or is intertwined with the public body's input during the negotiation process may not qualify as being "of the third party".
- Information that reveals information belonging to a third party may qualify as information "of the third party".

Step 2: Was the information supplied in confidence? (s. 21(1)(b))

"supplied"

- The use of the word "supplied" focuses more on whether the supplier of the information expected it to be kept confidential. This does not mean the intention or understanding of the recipient of information is irrelevant to s. 21, it simply means that the legislature intended that the focus under this section should be more on the intention or expectation of the information supplier.
- Whether information was "supplied" does not depend on the use that is made of it once it is received.
- Where the information at issue is a negotiated document, the third party's proprietary interest in any confidential information may be so clouded by the negotiating process and by the significant and evidenced input of university information that only strong proof evidencing such information as distinct and severable part of the agreement will suffice.

"in confidence"
Factors relevant to determining whether information has been supplied in confidence include:

- The nature of the information: Would a reasonable person regard it as confidential? Would it ordinarily be kept confidential by the supplier or recipient?
- The purpose of the information: Was the record prepared for a purpose that would not be expected to require or lead to disclosure in the ordinary course?
- Explicit statements: Was the record in question explicitly stated to be provided in confidence? This may not be enough but it is a relevant consideration.
- Voluntary or compulsory supply: Compulsory supply will not ordinarily be confidential, but in some cases there may be indications in the legislation relevant to the compulsory supply that establish confidentiality.
- Agreement or understanding between the parties: Was there an agreement between the parties with respect to confidentiality? Keep in mind that identifying a record as "confidential" does not automatically exempt it from disclosure and that no public body can be relieved of its responsibilities under access legislation merely by agreeing to keep matters confidential. In other words, no municipality or public body can "contract out" of access legislation.
- Actions of the university and supplier: Do the actions of the parties provide objective evidence of an expectation of confidentiality?

Step 3: Is there evidence of a reasonable expectation of harm? (s. 21(1)(c))

Reasonable expectation of harm

- Evidence of speculative harm will not meet the test, certainty of harm need not be established, rather the test is a middle ground requiring evidence well beyond a mere possibility of harm but somewhat lower than harm that is more likely than not to occur.
- There must be a clear and direct connection between the disclosure of specific information and the injury that is alleged.
- Evidence of harm must be more than just a well-intentioned but unjustifiably cautious approach to the avoidance of any risk whatsoever.
- Stating disclosure of a record will cause undue harm or loss does not alone constitute harm.

Remember: All three steps must be satisfied. If any one test is not met, s. 21 cannot apply.

Recent Examples:

Review Report FI-10-59(M)	land transfer agreement with a municipality
Review Report FI-12-01(M)	building permit correspondence file information
Review Report FI-13-28	IBM contract for SAP services
Review Report 16-01	FTE numbers and payroll rebate program information
Review Report 16-07	BMO Arena naming rights agreement
Review Report 16-09	Landfill management records
Review Report 16-10	Irving Shipbuilding loan agreement

How to Give Third Party Notice

Step 1: Assess the records
Determine whether or not s. 20 or s. 21 applies to the record or a portion of the record. The essential conditions precedent to the issuance of the notice is that the university has reason to believe the disclosure of the record might be contrary to the obligation set out in s. 20 or s. 21. This standard is quite low. If you have some concern that the record may contain third party business information or third party personal information as set out in s. 21 and s. 20, then proceed with a notice.

Step 2: **Time extension**
If you have decided that a third party notice is necessary you will need to take a time extension. If you have already taken your own time extension, make a request for a further time extension from the Information and Privacy Commissioner for Nova Scotia (s. 9(1)).

Step 3: Third party notice
Send a notice to third parties. Notices sent to third parties should include the following:

- All of the information set out in s. 22(1) which requires that the university provide an explanation that a request has been made, a description of the content of the record and requiring a reply within 14 days;
- A copy of the record at issue with notations indicating which portions of the record the university believes s. 21 or s. 20 might apply to;
- A request that the third party review the record and provide any comment it might have on the application of the exemption cited to the record;
- A request that the third party indicate whether or not it consents to the disclosure of the record.
- Do not disclose the identity of the third party to the applicant or of the applicant to the third party (s. 22(4)).

Step 4: Notice to applicant
At the same time as you send out notice to the third party, send a notice to the access applicant advising him/her that the record requested contains information the disclosure of which may affect the interests of a third party and so the third party is being given an opportunity to make representations concerning disclosure (s. 22(2)). Include the timeline for the process in your letter.

Step 5: Make a decision & advise the parties
After the 14 days have expired, evaluate the third party's response and all of the information at your disposal to determine if the three part test has been satisfied. If the third party does not respond, conduct your evaluation based only on the information already at your disposal. If the third party consents to the disclosure, s. 21 or s. 20 (depending on the case) cannot apply to the records (s. 21(4)). Make a decision and inform the third party and the original access applicant of your decision within 30 days after notice is given to the applicant under s. 22(2). If you decide to give access to all or a portion of the record, s. 23(3) lists the necessary content requirements. Remember do not disclose the identity of the applicant to the third party or of the third party to the applicant (s. 22(4)).

Step 6: Wait 20 days

Before releasing the records to the access applicant you must wait 20 days from when the third party is given notice. Contact the Office of the Information and Privacy Commissioner to confirm whether or not the third party has filed a request for review within the 20 day time frame. If the third party has filed a request for review of your decision, you cannot release the records until the review process is completed.

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 for Nova Scotia cannot approve in advance any proposal from a municipality. 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 Information and Privacy Commissioner for Nova Scotia will keep an open mind. It remains the responsibility of each municipality to ensure that they comply with their responsibilities under the relevant legislation. Visit us at: https://oipc.novascotia.ca

Disclosure Exemption Fact Sheet #3
s. 16 FOIPOP – Solicitor-Client Privilege

There are two types of privilege found at common law, both of which are encompassed by s. 16: legal advice privilege and litigation privilege. Section 16 is a discretionary exemption which means that a two-step process is involved. First, determine if the exemption actually applies to the records. Are all elements of the tests described below satisfied? Then, if the exemption applies, determine whether you should exercise discretion in favour of disclosure despite the fact that the exemption applies.

Step 1: Does the exemption apply?

Legal advice privilege
In order to decide if legal advice privilege applies, four things must be true:

1. There must be a communication, whether oral or written;
2. The communication must be of a confidential nature;
3. The communication must be between a client (or his agent) and a legal advisor; and
4. The communication must be directly related to the seeking, formulating or giving of legal advice.

Review the documents at issue and determine if any portion of the documents satisfy all four parts of the test. Included in this category is information that could indirectly reveal the information protected by solicitor client privilege.

Litigation privilege
There are five characteristics of records subject to litigation privilege:

1. Attachments to communications and materials;
2. Communications and/or materials were produced or brought into existence for the dominant purpose of being used to prepare for or conduct litigation;
3. The litigation was under way at the time the record was produced or litigation was in reasonable prospect at that time;
4. Privilege applies to communications between the lawyer and client and the lawyer and third parties; and
5. Privilege ends with the litigation.

Step 2: Exercise of discretion

As a matter of regular practice, whenever a public body determines that it has the authority to apply a discretionary exemption, before actually severing the information, the head of the public body must consider whether or not to exercise discretion in favour of disclosure despite the fact that the exemption applies. During the sign-off process, access coordinators should provide the individuals who have the delegated authority to apply exemptions with a list of considerations relevant to the exercise of discretion. That way, if the exemption is questioned, the administrator is in a position to clearly identify the factors considered – both for and against the exercise of discretion in favour of disclosure.

Factors that may be relevant in the exercise of discretion are:

- Public interest in disclosure;
- All of the relevant circumstances of the case and the purposes of the Act;
- The historical practice of the public body with respect to the release of similar types of documents;
- The nature of the record and the extent to which the document is significant and/or sensitive to the public body;
- Whether the disclosure of the information will increase public confidence in the operations of the public body;
- The age of the record;
- Whether there is a sympathetic or compelling need to release materials and,
- Whether previous orders of the Information and Privacy Commissioner have recommended that similar types of records or information should or should not be subject to disclosure.

Recent Examples:
Recent examples of the application of this exemption are:

Review Report FI-10-71	Email exchange between government lawyer and government department https://oipc.novascotia.ca

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 for Nova Scotia cannot approve in advance any proposal from a municipality. 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 Information and Privacy Commissioner for Nova Scotia will keep an open mind. It remains the responsibility of each municipality to ensure that they comply with their responsibilities under the relevant legislation. Visit us at: https://oipc.novascotia.ca

Disclosure Exemption Fact Sheet #4
s. 18 FOIPOP– Threat to Safety

Section 18 of *FOIPOP* is a discretionary exemption that permits the university to refuse to disclose information, including personal information about the applicant, if the disclosure could reasonably be expected to:

a) threaten anyone else's safety or mental or physical health; or
b) interfere with public safety.

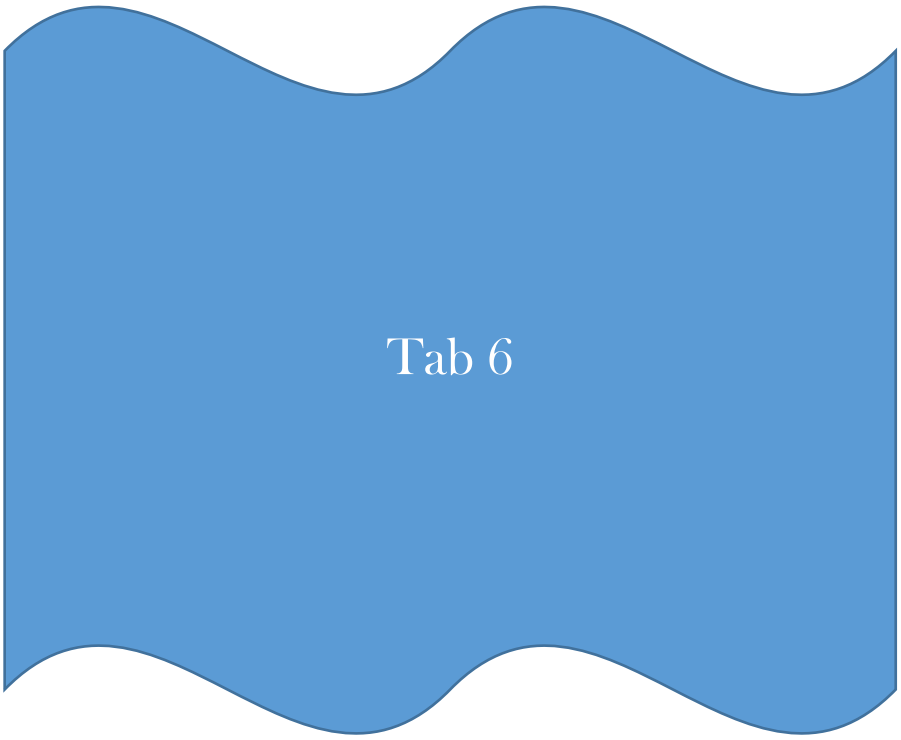
The public body may refuse to disclose to an applicant personal information about the applicant, if the disclosure could reasonably be expected to result in immediate and grave harm to the applicant's safety or mental or physical health.

In summary then, in determining whether the objective test set out in s. 18(1)(a) has been met:

- The harm must be related to the disclosure of the information at issue, there must be evidence to connect the disclosure of the information to the risk identified;
- The public body must provide evidence the clarity and cogency of which is commensurate with a reasonable person's expectation that disclosure of the information could threaten the safety, or mental or physical health, of anyone else;
- Safety includes freedom from danger or risks;
- The public body must demonstrate that disclosure will result in a risk of harm that is well beyond the merely possible or speculative to reach the middle ground between what is probable and what is merely possible;
- Relevant factors will include: factual background, the nature of the information being sought, the circumstances affecting the public body or third party individuals, the identity of the requester, evidence as to possible uses of the information and the subjective fear of individuals.

Recent Example:
Recent example of the application of this exemption is:

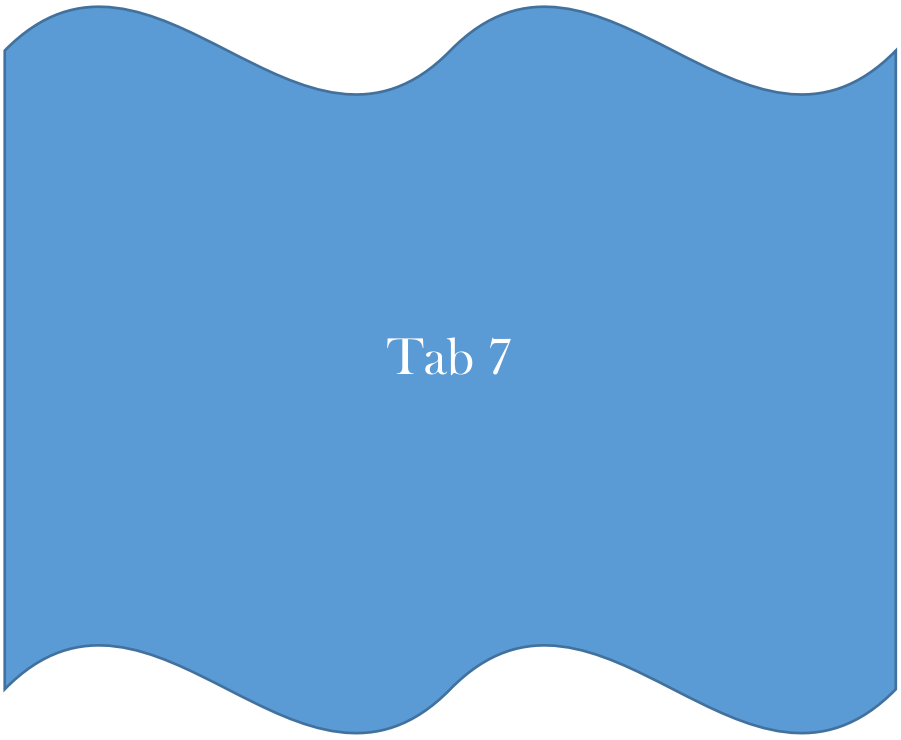
Review Report FI-10-71 witness statement


Tab 6

Sample Routine Access Policy for Universities & Colleges

Instructions for use: This routine release policy was drafted by the Office of the Information and Privacy Commissioner for Nova Scotia (OIPC). The OIPC does not have the authority to approve routine release lists for universities or colleges. The sample routine access policy contains a list of records typically created by universities and colleges that could be made publicly available without a formal access request. Universities will have to carefully review each record type before adding the record types to the routine release list. Always ensure that no personal information is disclosed unless authorized under *FOIPOP*. Ideally, routinely releasable information 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
Administrative	• General overview of the business unit responsibilities • Contact information of business unit staff • Statistics • Program evaluations • OHS routine inspection reports
Human Resources	• Generic information about current benefits and hours of work • Current job descriptions, salary ranges or hourly rate, classification of positions • Organizational charts with position titles • Staff lists with position titles • Hiring process including # of applicants for a position, # of people interviewed, successful candidate's name after offer accepted, identity of selection panel • Overtime expenditures • Employee expense reports
Financial	• Audited financial statements • Costs of specific or special events • Expenditure reports by cost elements (salaries, office supplies, travel etc.) • Budgets including capital budget • Project overviews • Business plans • Procurement information • Tender results
Policies, Procedures & Plans	• Access and privacy obligations • Annual service plans • Human resources business plan • Policies and procedures
Polls & Surveys	• Results of polls or surveys


Tab 7

Sample Records Retention Schedule

Instructions for use:
The *Freedom of Information and Protection of Privacy Act* does not set out rules for how long information must be retained, with one exception – personal information that is used to make a decision that directly affects an individual, must be kept for at least one year. This template was drafted by the Office of the Information and Privacy Commissioner for Nova Scotia. The OIPC does not have the authority to approve record retention schedules of universities or colleges. The schedule below is an example of a potential records retention schedule focused on records typically held by universities and colleges. Before adopting a schedule you must ensure that the retention selected meets all contractual, legislated and industry requirements in Nova Scotia.

The schedule below is based primarily on records retention schedules prepared by Sheridan College and Simon Fraser University. For further information, such as a detailed description of what information should and should not be included in a particular series, please review the full records retention schedules available on the Sheridan College and Simon Fraser University websites.

Number	Record Series	Active Retention	Semi-active	Total retention	Final disposition
Department: Administration					
	General	CY+2	0	CY+2	Destroy
	Associations/Societies/Commissions	CY+1	0	CY+1	Destroy
	Councils – Internal	CY+4	Perm	Perm	Archive
	Councils – External	CY+1	0	CY+1	Destroy
	Committees – Internal	CY+2	Perm	Perm	Archive
	Committees – External	CY+3	3	CY+5	Destroy
	Task Forces	T+2	0	T+2	Destroy
	Faculty/Staff Meetings	CY+2	0	CY+2	Destroy
	Department of Education/High Schools	CY+5	0	CY+5	Destroy
	Community Colleges/Universities	CY+2	0	CY+2	Destroy
	Community Agencies/Services	CY+2	0	CY+2	Destroy
	Company/Industry/Employer Files	CY+2	0	CY+2	Destroy
	Printing	CY+1	0	CY+1	Destroy
	Computer Information Systems	CY+5	0	CY+5	Destroy
	Computer/Technical Information	CY+2	0	CY+2	Destroy
	Telecommunications	S/O	0	S/O	Destroy
	Departmental Process Manuals	S/O	1	S/O+1	Destroy
Department: Building/Equipment					
	General	CY+1	0	CY+1	Destroy
	Building and Grounds Maintenance	CY+1	Perm	Perm	Archive
	Floor Plans/Space Requirements	S/O	0	S/O	Destroy
	Security	CY+10	0	CY+10	Destroy
	Capital Projects	T+2	Perm	Perm	Archive
	Athletic and Gymnasium Rental	CY+2	5	CY+7	Destroy
	Vehicles	S/O	0	S/O	Destroy

Number	Record Series	Active Retention	Semi-active	Total retention	Final disposition
Department: Course/Curriculum/Program					
	General	CY+2	0	CY+2	Destroy
	Program Proposals and Development	CY+5	0	CY+5	Destroy
	Direct Purchase Programs/Sponsored Programs	T+2	3	T+5	Destroy
	Program Descriptions	CY+2	Perm	Perm	Archive
	Course Information	CY+2	Perm	Perm	Archive
	Course Program Handouts	CY+1	4	CY+5	Destroy
	Examination Papers and Course Assignments	CY+1	0	CY+1	Destroy
	Evaluation of Student Work	T+1	0	T+1	Destroy
	Evaluation of Teaching	Per collective agreement			
	Room Allocation Timetables	S/O+1	0	S/O+1	Destroy
	International Education Files	CY+5	0	CY+5	Destroy
	Accreditation Support Records	CY+10	0	CY+10	Destroy
	Library	CY+2	0	CY+2	Destroy
	Field Trips	CY+1	0	CY+1	Destroy
	Festivals/Competitions	CY+2	0	CY+2	Destroy
	Sponsored Projects	CY+2	0	CY+2	Destroy
Department: Finance					
	General	CY+2	0	CY+2	Destroy
	Signing Authorities	T+7	0	T+7	Destroy
	Accounts Payable Invoices	CY+2	5	CY+7	Destroy
	Fixed Assets Invoices	CY+2	Perm	Perm	Archive
	Audit	CY+7	0	CY+7	Destroy
	Bank Reconciliations	CY+2	5	CY+7	Destroy
	Banking	CY+2	5	CY+7	Destroy
	Petty Cash	CY+3	3	CY+6	Destroy
	Budget	CY+2	5	CY+7	Destroy
	Financial Statements	CY+2	Perm	Perm	Archive
	Chargebacks	CY+1	0	CY+1	Destroy
	Inventory	S/O	0	S/O	Destroy
	Investments/Trusts	Perm	0	Perm	Archive
	Journal Vouchers	CY+2	5	CY+7	Destroy
	Purchase Orders	CY+2	5	CY+7	Destroy
	Standing Agreements	S/O+1	6	S/O+7	Destroy
	Expense Accounts	CY+2	5	CY+7	Destroy
	Parking	CY+2	5	CY+7	Destroy
	Taxes	CY+2	5	CY+7	Destroy
	Cheque Registers	CY+2	5	CY+7	Destroy
	Collections/NSF/Stop Payments	T+2	4	T+6	Destroy
	Accounts Receivable Invoices	CY+2	5	CY+7	Destroy
	Enrollment Audit	CY+2	Perm	Perm	Archive

Number	Record Series	Active Retention	Semi-active	Total retention	Final disposition
	Tuition Payment Files	CY+2	5	CY+7	Destroy
	Refunds	CY+2	5	CY+7	Destroy
	Requests for Proposal	CY+6	0	CY+6	Destroy
	Endowment accounting	T+7	0	T+7	Archive
Department: Human Resources					
	General	CY+2	0	CY+2	Destroy
	Recruitment	T+1	2	T+3	Destroy
	Staffing Competition	T+2	2	T+4	Destroy
	Position Description	S/O	0	S/O	Destroy
	Personnel/Payroll	T+2	48	T+50	Destroy
	Benefits	T+2	48	T+50	Destroy
	Workers Compensation Assessment	CY+2	Perm	Perm	Archive
	Workers Compensation Claims	CY+2	Perm	Perm	Archive
	Staff/Faculty Lists and Seniority Lists	S/O	0	S/O	Destroy
	Standard Workload Inventory Forms	CY+2	4	CY+6	Destroy
	Attendance (staff and faculty)	CY+2	8	CY+10	Destroy
	Retirement/Pension	T+2	48	T+50	Destroy
	Professional Development	CY+2	4	CY+6	Destroy
	Human Resources Projects	CY+2	4	CY+6	Destroy
	Employee Disability Projects	CY+2	Perm	Perm	Archive
	Salary/Payroll	CY+2	8	CY+10	Destroy
	Grievances	CY+2	13	CY+15	Destroy
	Strikes	S/O+5	0	S/O+5	Destroy
	Union	CY+2	0	CY+2	Destroy
	Non-union	CY+2	0	CY+2	Destroy
	Human Rights and Harassment Case Files	CR+3	10	CR+13	Destroy
	Employee Assistance Program	CY+2	0	CY+2	Destroy
	Occupational Health and Safety (Accident Reports)	CY+1	49	CY+50	Destroy
	Human Resources Working Notes	CR+2	4	CR+6	Destroy
	VP's Meeting Notes	CR+2	4	CR+6	Destroy
Department: Legal/Government Affairs					
	General	CY+2	0	CY+2	Destroy
	Contracts/Agreements/Warranties	T+2	10	T+12	Destroy
	Personnel Contracts/Agreements	T+2	4	T+6	Destroy
	Direct Purchase/Government Sponsored Agreements	T+2	5	T+7	Destroy
	Land Use and Environmental Records	T+1	Perm	Perm	Archive
	Leases	T+1	6	T+7	Destroy
	Insurance	CY+5	0	CY+5	Destroy
	Liquor Licenses	CY+2	5	CY+7	Destroy
	Municipalities/Cities/Towns	CY+2	0	CY+2	Destroy
	Department of Advanced Education	Perm	0	Perm	Archive

Number	Record Series	Active Retention	Semi-active	Total retention	Final disposition
	Litigation	T+2	5	T+7	Destroy
	Other NS Departments, Agencies, Boards and Commissions	CY+2	0	CY+2	Destroy
	Federal Departments, Agencies, Boards and Commissions	CY+2	0	CY+2	Destroy
	Acts/Regulations	S/0	0	S/0	Destroy
	Permits – General	CY+1	0	CY+9	Destroy
	Permits – Environmental	CY	Perm	Perm	Archive
	Trademark/Copyright	Perm	0	Perm	Archive
	Legal Opinions	CY+10	0	CY+10	Archive
	Waivers of Liability	T	10	T+10	Destroy
	Consent to Use of Image	T+1	4	T+5	Destroy
	Procurement Documentation	CY+1	6	CY+7	Destroy
	Freedom of Information/Access Requests	T+2	3	T+5	Destroy
	Privacy Breaches, Assessments, and Investigations	T+2	8	T+10	Destroy
	Privacy, Records and Information Management Program	CY+2	5	CY+7	Destroy
	Records and Information Lifecycle Management	CY+2	Perm	Perm	Archive
Department: Governance					
	Legal Opinions	CY+10	0	CY+10	Archive
	Ombudsman Case Files	T+1	0	T+1	Archive
	Senate Agendas, Minutes and Supporting Papers	Perm	0	Perm	Archive
	Senate Committee Records	CY+5	10	CY+15	Archive
	Senate Working Papers	CY+2	0	CY+2	Destroy
Department: Research					
	Research Grants - External	T+1	0	T+1	Destroy
	Research Grants - Internal	T+1	0	T+1	Destroy
	Research Agreements	Perm	0	Perm	Archive
	Research Contract and Agreement Files	T+2	8	T+10	Destroy
	Research Expenditures	T+2	8	T+10	Destroy
	Research Reporting	T+2	8	T+10	Destroy
Department: Medical/Health					
	General	CY+2	0	CY+2	Destroy
	Health and Safety	CY+5	Perm	Perm	Archive
	Client Health Records	T+2	8	T+10	Destroy
	Nurse's Daily Record	CY+2	18	CY+20	Destroy
	Medical Directives/Orders	CY+2	18	CY+20	Destroy

Number	Record Series	Active Retention	Semi-active	Total retention	Final disposition
Department: Organization/Planning					
	General	CY+2	0	CY+2	Destroy
	Policies/Procedures	S/0	0	S/0	Destroy
	Annual Reports	CY+2	Perm	Perm	Archive
	Organization	S/0	0	S/0	Destroy
	Board of Governors	CY+2	Perm	Perm	Archive
	Strategic Planning	CY+2	8	CY+10	Destroy
	Program Review	CY+3	3	CY+6	Destroy
	Employment Equity	CY+5	0	CY+5	Destroy
	Pay Equity	CY+5	0	CY+5	Destroy
	Race Relations	CY+5	0	CY+5	Destroy
	Operational Review	CY+3	3	CY+6	Destroy
Department: Public Relations/Marketing					
	General	CY+2	0	CY+2	Destroy
	Market Research	CY+5	0	CY+5	Destroy
	Articulation	CY+2	0	CY+2	Destroy
	Student Recruitment	CY+2	3	CY+5	Destroy
	Speeches/Speaking Engagements	CY+3	0	CY+3	Destroy
	Prospects	CY+3	0	CY+3	Destroy
	Mailing Lists	S/0	0	S/0	Destroy
	Media/News Releases	CY+2	Perm	Perm	Archive
	Newspaper Clippings	CY+2	Perm	Perm	Archive
	Advertising	CY+2	3	CY+5	Destroy
	Photographs	S/0	0	S/0	Destroy
	Publications/Newsletters	CY+2	8	CY+10	Destroy
	Special Events	CY+2	3	CY+5	Destroy
	Convocation	CY+5	5	CY+10	Destroy
	Development and Fundraising	CY+2	5	CY+7	Destroy
Department: Student Activities/Services					
	General	CY+2	0	CY+2	Destroy
	Intercampus Student Corporation	CY+2	0	CY+2	Destroy
	Housing Registry	S+1	0	S+1	Destroy
	Theatre Productions	CY+2	3	CY+5	Destroy
	Daycare Centre	T+2	18	T+20	Destroy
	Accommodation Records	T+2	8	T+10	Destroy
	Student Rights and Responsibilities Office Case Files	T+4	51	T+55	Destroy
	Tutoring	CY+1	0	CY+1	Destroy
	Player Eligibility Files	CY+2	8	CY+10	Destroy
	Varsity Sports	CY+2	3	CY+5	Destroy
	Intramural Sports	CY+2	3	CY+5	Destroy
	Instructional/Recreational Sports	CY+1	0	CY+1	Destroy
	Alumni Sports	CY+2	0	CY+2	Destroy
	Alumni	S/0	0	S/0	Destroy

Number	Record Series	Active Retention	Semi-active	Total retention	Final disposition
Department: Student Records					
	General	CY+2	0	CY+2	Destroy
	Administration and Registration Reports	CY+2	5	CY+7	Destroy
	Criminal Record Checks	T+1	0	T+1	Destroy
	Permanent Student Record	T+3	52	T+55	Destroy
	Financial Aid Administration	CY+3	0	CY+3	Destroy
	Financial Aid/Loan Files	CY+3	0	CY+3	Destroy
	Financial Aid Verification	T+1	0	T+1	Destroy
	Financial Assistance to Non-NS Residents	CY+2	0	CY+2	Destroy
	NS Work/Study Program	CY+2	0	CY+2	Destroy
	In-Progress Registration Materials – Short-term	CY+1	0	CY+1	Destroy
	In-Progress Registration Materials – Long-term	CY+2	3	CY+5	Destroy
	Applicant Information	CY+1	0	CY+1	Destroy
	Co-op/Employment Student Files	T+1	0	T+1	Destroy
	Employment Statistics	CY+5	0	CY+5	Destroy
	Appeals	CY+1	0	CY+1	Destroy
	Awards	CY+5	Perm	Perm	Archive
	Diplomas/Certificates	CY+1	2	CY+3	Destroy
	Transcript Requests	CY+1	0	CY+1	Destroy
	Career Employment and Preparation Program	T+3	12	T+15	Destroy
	Prior Learning	CY+1	0	CY+1	Destroy

CY = Current year;
S/O = Superseded or obsolete;
T = Completion of Task/Termination;
CR = Creation;
Perm = Permanent

Sample Records Disposition Authorization Form

Instructions for use:
This sample form was drafted by the Office of the Information and Privacy Commissioner for Nova Scotia. The OIPC does not have the authority to approve record retention schedules of universities or colleges. You should adapt this form to meet the needs of your organization. The form below is based primarily on the form produced by the Nova Scotia Archives and Records Management, which is used by the OIPC.

Records Disposition Authorization

This form requests and documents the disposition of government records.

Contact Information

Organization Name and Address:	
Records management designate name and telephone number:	

Disposition Description

The records described below are eligible for disposition in accordance with the organization's records retention schedule. The records described below are eligible for disposition in the manner indicated:

	Destruction
	Transfer to the control of the organization's archives

Records Description (list box numbers and file list)

Disposition Authorization (must be signed by the head of the organization)

I certify that the records described above have been retained for the scheduled retention period, required audits have been completed, and no pending or ongoing access to information requests, litigation or investigation involving these records is known to exist.

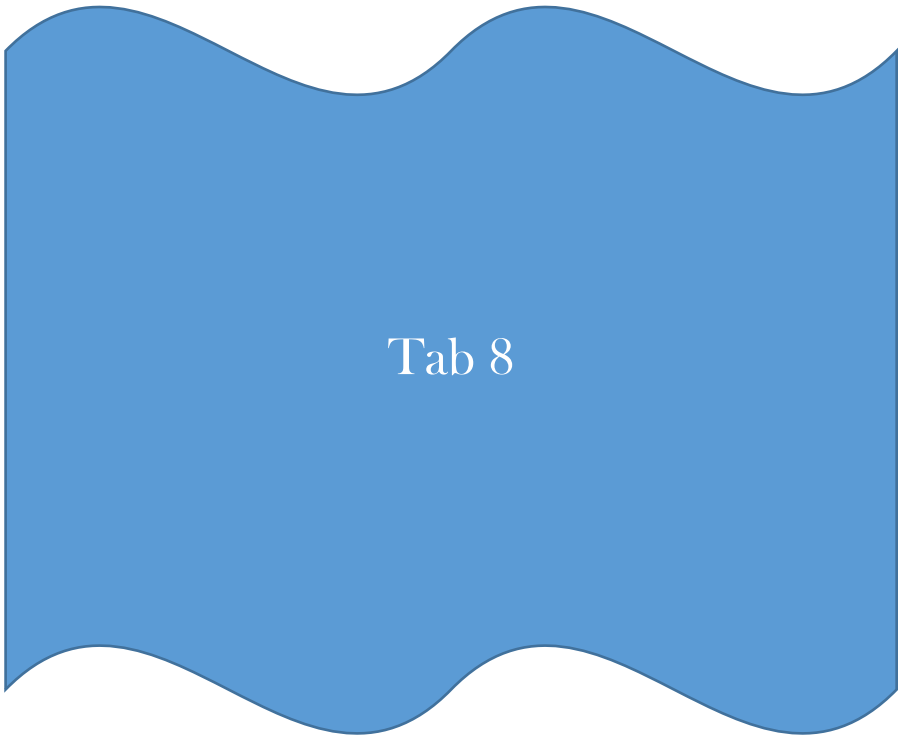
Name and Title Signature Date

Certification of Disposition (signed when disposition is completed)

I certify that the manner of disposition has been carried out for the records described above.

Name and Title Signature Date

Privacy Rules & Tools


Tab 8

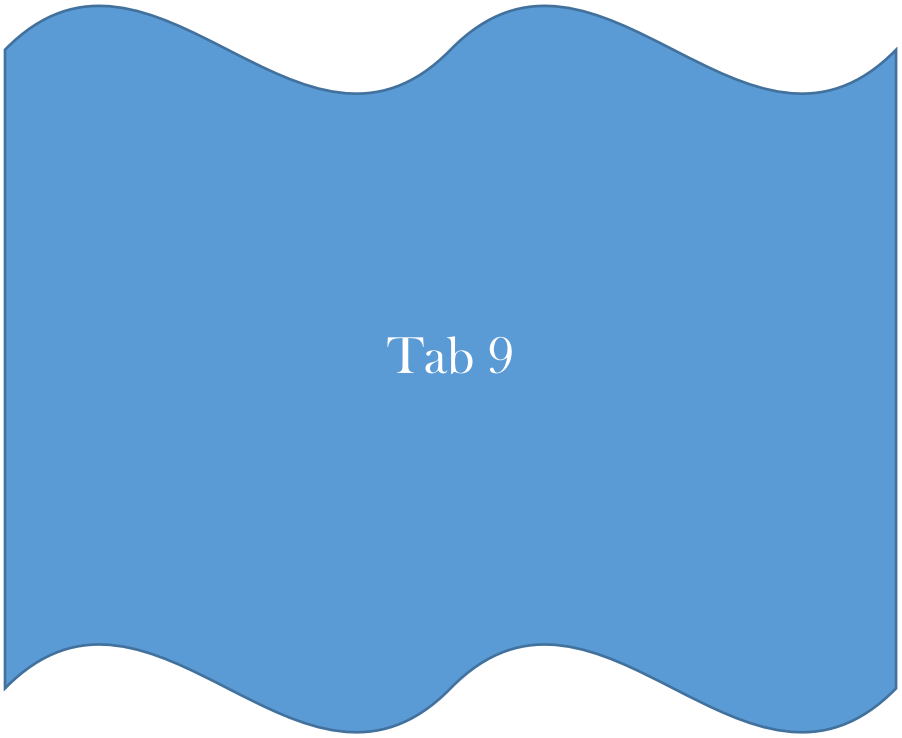
Freedom of Information and Protection of Privacy Act - Privacy Rules At a Glance

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 and is 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 **Note:** "compatible" is defined in s. 28 to mean a use of the personal information that has a reasonable and direct connection with the purpose for which it was originally collected <u>and</u> that is necessary for performing the statutory duties of, or for operating a legally authorized program of the public body. **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 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* at: http://nslegislature.ca/legc/statutes/freedom%20of%20information%20and%20protection%20of%20privacy.pdf


Tab 9

Freedom of Information and Protection Of Privacy Act
Disclosures Without Consent

1. General Rule

2. Approach
   Step 1: Is the disclosure authorized?
   Step 2: Applying your discretion, should the information be disclosed?
   Step 3: Release only the minimum amount of information necessary for the approved disclosure.
   Step 4: Document the disclosure

3. FOIPOP Disclosure Decision Table

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 for Nova Scotia (also known as the FOIPOP Review Office) cannot approve in advance any proposal from a public body, municipal body 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, municipal body and health custodian to ensure that they comply with their responsibilities under the relevant legislation. Visit us at: https://oipc.novascotia.ca

1. General Rule

A public body cannot disclose personal information unless authorized under *FOIPOP*. Section 27 of *FOIPOP* lists all of the circumstances where disclosure is permitted. All disclosures of personal information under s. 27 are discretionary. This means that the public body holding the personal information need not disclose the personal information even if it is authorized. Sometimes though, the authorization provided, for example a warrant, turns the request into a mandatory disclosure. However, in every case, the public body must only disclose the minimum personal information necessary to meet the identified purpose.

2. Approach

Step 1: Is the disclosure authorized?
When another public body or authority such as a police force seeks access to personal information in the custody and control of a public body, they should be required to provide an explanation for why the disclosure is authorized under s. 27. Further, they must satisfy the public body that they have the authority claimed. So, for example, if an authority claims it is making the request in accordance with an enactment, require the authority to provide a copy of the enactment and all documentation supporting that the enactment applies in the particular circumstances.

Step 2: Should the information be disclosed?
All of the disclosures without consent that are permitted under s. 27 (and described below) are discretionary. That is, *FOIPOP* says the public body "may" disclose the information without consent. As noted above, some disclosures become mandatory because the authority cited (for example, a warrant or sometimes certain other enactments) make the disclosure mandatory.

Therefore, each time the public body receives a request for disclosure, the public body must consider a variety of factors.

If your public body is subject to frequent requests for disclosure of personal information without consent, the public body should develop a disclosure policy setting out the circumstances when identified staff are permitted to disclose personal information. For example, larger health custodians frequently choose to limit disclosures to strictly defined circumstances such as only where there is a risk of imminent harm, a warrant has been produced or where there is consent.

Some general considerations in the exercise of discretion are:

- The historical practice of the public body with respect to the release of similar types of documents;
- The nature of the record and the extent to which the document is significant and/or sensitive to the affected individual;
- The original purpose for the collection of the personal information;
- Whether the disclosure of the information will increase public confidence in the operation of the public body;
- The age of the record;
- Whether there is a sympathetic or compelling need to release materials; and
- Whether there is a public interest in the release of the records.

The courts have confirmed that discretionary decisions under privacy and access legislation must not be made in bad faith or for an improper purpose, must not take into account irrelevant considerations and must take into account relevant considerations.

Step 3: Disclose the minimum amount of information necessary
If you have determined that the disclosure is authorized and that a proper exercise of your discretion leads you to confirm that you should disclose the information, the final step is to decide what information to disclose. Just because the organization asks for an entire file does not mean that you disclose the entire file. Disclose only the minimum amount of information necessary to meet the approved purpose.

Step 4: Document the disclosure
Best practice is to document any disclosure of personal information by placing a note on the file from which the personal information originated.

The documentation should include:

- A description or copy of the personal information disclosed;
- The name of the person or organization to whom the personal information was disclosed;
- The date of disclosure; and
- The authority for the disclosure.

FOIPOP Disclosure Decision Table	
Consent provided	
Written consent 1. A public body may disclose personal information to anyone if the individual the information is about has identified the information and consented in writing to the disclosure. (s. 27(b))	
Consent not required A public body may disclose personal information without consent in limited circumstances as follows:	
Original and compatible purposes 2. For the purpose for which it was obtained or compiled, or a use compatible with that purpose. (27(c) and 28 – defines compatible purposes as having a reasonable and direct connection to the original purpose and necessary for operating a legally authorized program)	
Disclosures permitted within a public body 3. To an officer or employee of a public body or to a minister if the information is necessary for the performance of the duties of or for the protection of the health or safety of the officer, employee or minister. (s. 27(f)) 4. To a public body to meet the necessary requirements of government operation. (s. 27(g))	
Next of kin 5. So that next of kin or a friend of an injured, ill or deceased individual may be contacted. (s. 27(p))	
Collection of a debt or making payments 6. To collect a debt or fine owing by an individual to the Province or to a public body. (s. 27(h)(i)) 7. To make a payment owing by the Province or a public body to an individual. (s. 27(h)(ii))	
Health or safety related disclosures 8. To an officer or employee of a public body or to a minister if the information is necessary for the protection of the health or safety of the officer, employee or minister. (s. 27(f)) 9. If the head of the public body determines that compelling circumstances exist that affect anyone's health or safety. (s. 27(o)) 10. Where there is a risk of significant harm to the environment or to the health or safety of the public or a group of people or for any other reason, the disclosure is clearly in the public interest. (s. 31 – note there are notice requirements set out in s. 31)	

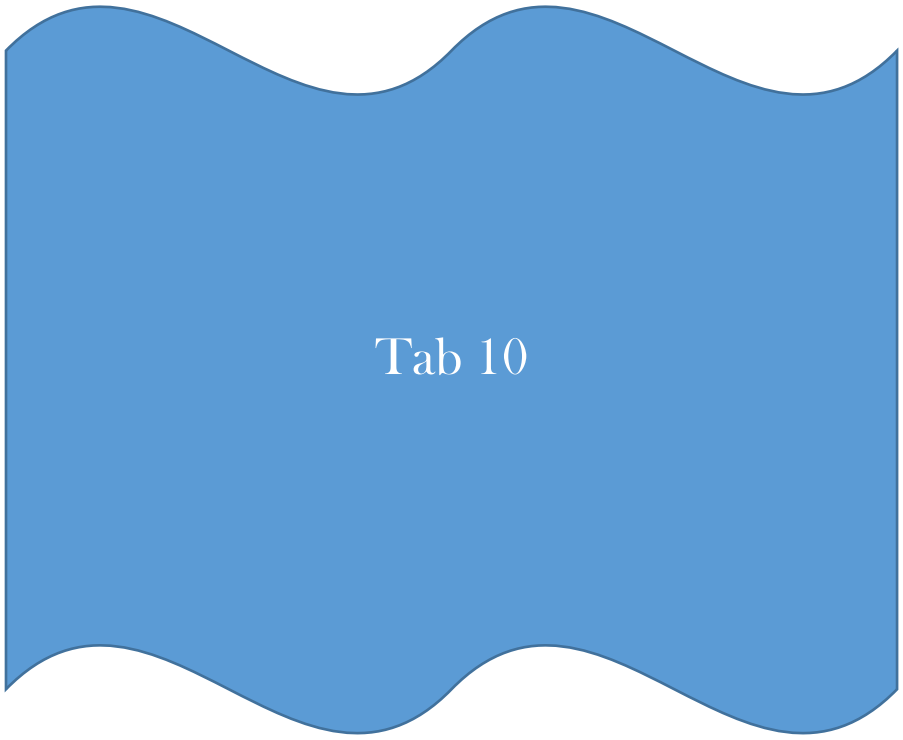
FOIPOP Disclosure Decision Table

Consent not required

A public body may disclose personal information without consent in limited circumstances as follows:

Legal proceedings, law and investigations 11. To respond to an access to information request under *FOIPOP.* (s. 27(a)) 12. Pursuant to another enactment. (s. 27(a)) 13. To comply with an enactment or with a treaty, arrangement or agreement made pursuant to an enactment. (s. 27(d)) 14. To comply with a subpoena, warrant, summons or order. (s. 27(e)) 15. To a public body or law enforcement agency in Canada to assist with an investigation undertaken with a view to a law enforcement proceeding or from which a law-enforcement proceeding is likely to result.[3] (s. 27(m)) 16. If the pubic body is a law enforcement agency and the information is disclosed to another law enforcement agency in Canada or in a foreign country under an agreement or legislative authority. (s. 27(n))	
Audits, research, public archives 17. To the Auditor General for audit purposes. (s. 27(i)) 18. To a researcher for research or statistical purposes if the requirements of s. 29 are satisfied. (s. 27(q)) 19. To the public archives of Nova Scotia or the archives of a public body. (s. 27(l)) 20. The public archivers of Nova Scotia or of the public body may disclose personal information for archival and historical purposes as set out in s. 30. (s. 27(q))	
MLAs, union representatives 21. To an MLA who has been requested by the individual, whom the information is about, to assist in resolving a problem. (s. 27(j)) 22. 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. (s. 27(k))	

[3] "Law enforcement" is defined in s. 3 of *FOIPOP* as policing, including criminal intelligence operations, investigations that lead or could lead to a penalty or sanction being imposed and proceedings that lead, or could lead to a penalty or sanction being imposed. "Proceeding" and "investigation" are not defined.


Tab 10

Authority to Disclose, Access & Store Personal Information Outside of Canada

Personal Information International Disclosure Protection Act **(PIIDPA)**

Application of the Act		
3 4	*PIIDPA* applies to every public body and municipality and to all directors, officers and employees as well as to all employees and associates of a service provider. *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)	**Rule**	A public body shall ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada unless *PIIDPA* permits otherwise.
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 accessed 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))
6(1)	**Foreign demand for disclosure**	A public body or employee must immediately notify the minister of any foreign demand for disclosure.
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.

Disclosure Outside Canada - Authorities		
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 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' licenses.
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.

Tab 11

Privacy Impact Assessment Template

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.[4]

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.[5] 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.

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

[5] 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

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[6] answer the following four questions before proceeding:

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

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.*

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)*:** *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? (See s. 24(4) of *FOIPOP*).

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)).
    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 and 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 (i.e: 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 and 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
1				
2				
3				
4				

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 Employee**	**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

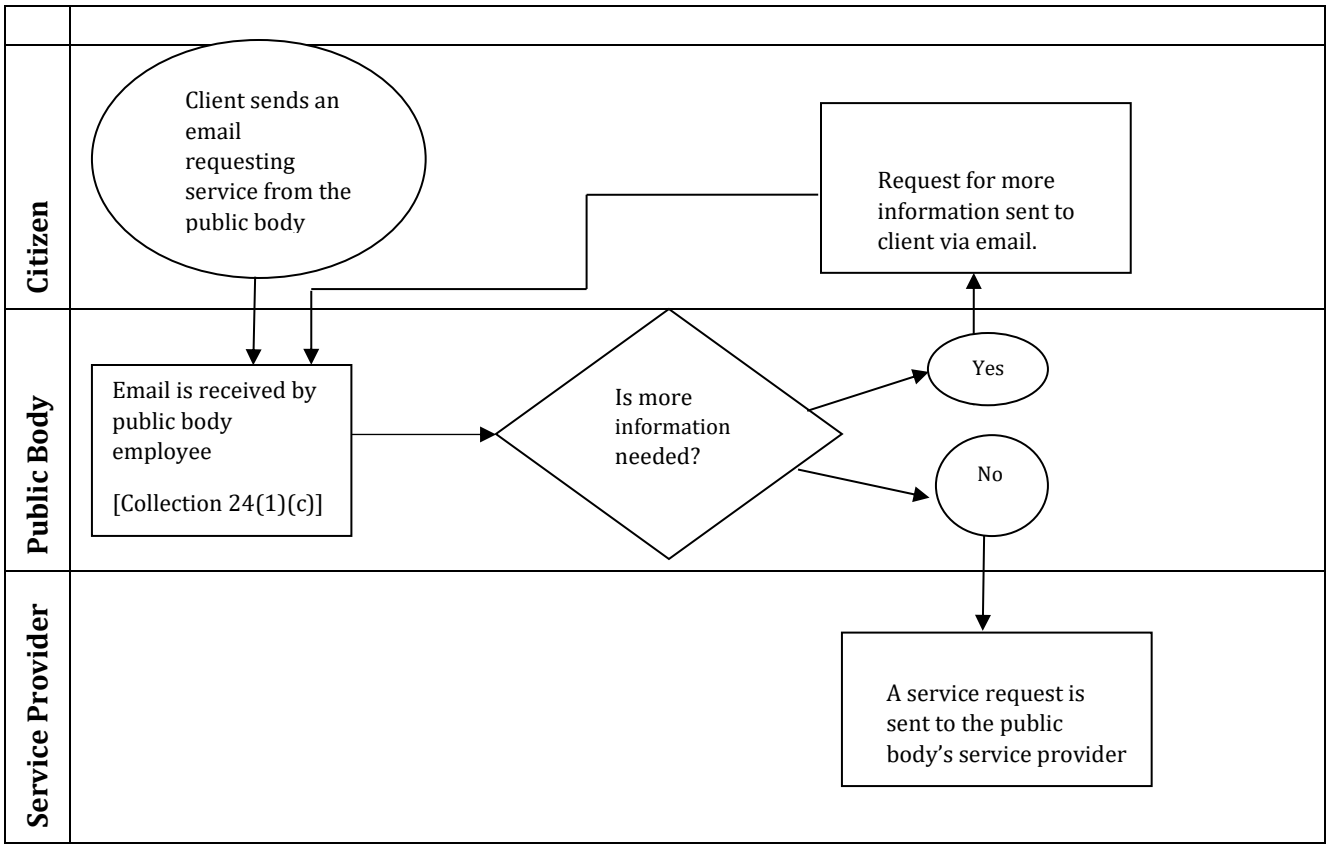
[Insert position] Date

Approved by:

[Insert Executive Sponsor] Date

Appendix A: Sample Information Flow Diagram

Example:



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 to 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 government 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 & Store Personal Information Outside of Canada

Personal Information International Disclosure Protection Act

Application of the Act		
3	*PIIDPA* applies to every public body and municipality and to all directors, officers and employees as well as to all employees and associates of a service provider.	
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)	**Rule**	A public body shall ensure that personal information is stored and accessed only in Canada unless authorized under *PIIDPA.*
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 accessed 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 or 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' licenses.
9(2)(j)	**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 next of kin or friend of injured or deceased individual may be contacted.
9(2)(l)	**Research** **Public archives**	For 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.

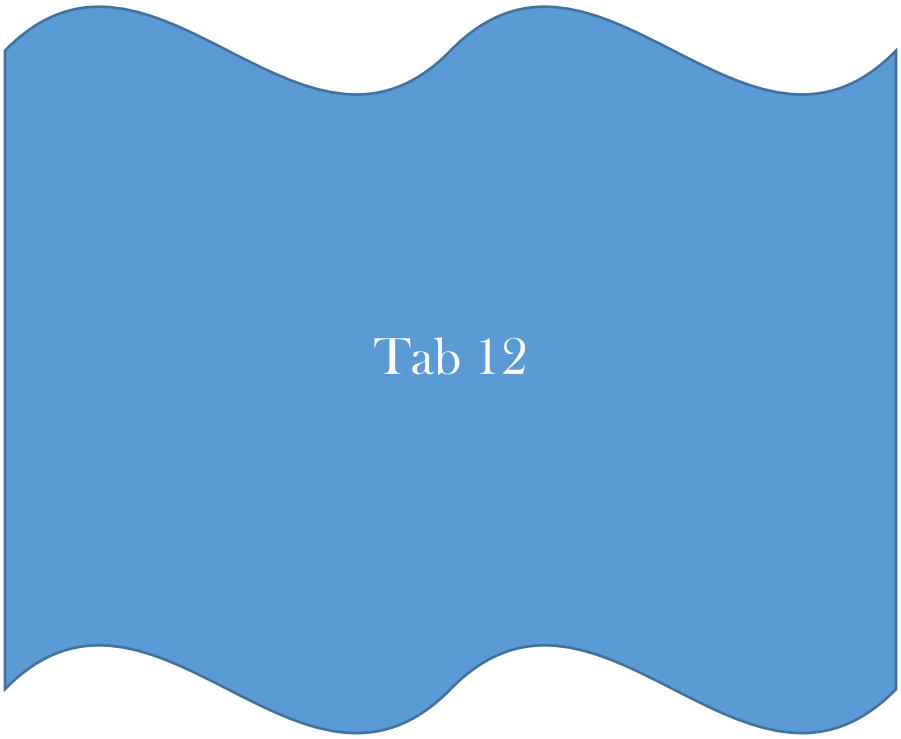
	Landlord Information[7]	**Tenant Information**	**Complaint Summary**	**Investigation Notes**	**Enforcement Outcome**
Clerical	✓	✓	✓		✓
Program Director	✓	✓	✓		✓
Manager of Investigations	✓	✓	✓	✓	✓
Investigator	✓	✓	✓	✓	✓
Deputy Minister					

[7] 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 considerations as above


Tab 12

Reasonable Security Checklist

This checklist was prepared by the Office of the Information and Privacy Commissioner for Nova Scotia.[8] Under Nova Scotia's privacy legislation, public bodies, municipalities and health custodians must all ensure that they have made reasonable security arrangements against such risks as unauthorized access to or use, disclosure, copying or modifications of personal information.[9] This checklist is intended to give a quick snap shot of some key security standards. Failure to meet the standards set out in this checklist is an indication that personal information may be at risk and that a thorough review of security should be undertaken immediately.

The checklist includes questions in each of the 17 areas of security compliance listed below and should take about 30 minutes to complete:

1. Risk Management
2. Policies
3. Records Management
4. Human Resources Security
5. Physical Security
6. Systems Security
7. Network Security
8. Wireless
9. Database Security
10. Operating systems
11. Email and Fax Security
12. Data Integrity and Protection
13. Access Control
14. Information Systems Acquisition, Development and Maintenance
15. Incident Management
16. Business Continuity Planning
17. Compliance

[8] This document is based on "Securing Personal Information: A Self-Assessment Tool for Organizations" created by the Office of the Information and Privacy Commissioners in Alberta and British Columbia and the Office of the Privacy Commissioner of Canada. The full self-assessment tool is available at: https://www.oipc.bc.ca/guidance-documents/1439 and as an interactive tool at: https://www.priv.gc.ca/resource/tool-outil/security-securite/english/AssessRisks.asp?x=1.

[9] *Personal Health Information Act* s. 62, *Freedom of Information and Protection of Privacy Act* s. 24(3), *Municipal Government Act* s. 483(3).

Risk Management		
	Yes	No
1. We have identified all of our personal information assets and their sensitivity.		
2. We have analyzed, evaluated and documented the likelihood of security failures occurring.		
3. We have a risk treatment plan identifying the appropriate management action, resources, responsibilities and priorities for managing personal information security risks.		
Policies		
4. We have operational security policies (such as secure faxing, end-of-day closing, use of couriers).		
5. Employees, contractors and partners have easy access to our personal information security policy.		
6. We have an acceptable use policy.		
Records Management		
7. Specific retention periods have been defined for all personal information.		
8. Personal information contained on obsolete electronic equipment or other assets is securely destroyed before the equipment or asset is disposed of.		
9. Hard copy records containing personal information is shredded, mulched or otherwise securely destroyed.		
Human Resources Security		
10. Training has been implemented for all employees, data custodians and management to ensure they are aware of and understand their security responsibilities, permitted access, use and disclosure of personal information and retention and disposal policies.		
11. All employee are required to sign confidentiality agreements.		
12. Contractors and other third parties are required to return or securely destroy personal information to the public body upon completion of the contract.		
Physical Security		
13. We have strong physical security measures for storing personal information including locked cabinets, pass cards and motion detectors or other intrusion alarm systems.		
14. Our publicly accessible service counters are kept clear of personal information.		
15. We have a nightly closing protocol that requires employees to clear personal information from their desks and lock it away, log out of all computers and remove all documents containing personal information from fax machines and printers.		
System Security		
16. All terminals and personal computers used for handling personal information are positioned so that unauthorized personnel cannot see the screens.		
17. If a user walks away from her terminal there is an automatic process to lock out all users after a short defined period of inactivity.		
18. Personal information is always stored either on a secure server or is encrypted when stored on mobile and portable devices.		

Network Security		
	Yes	No
19. We use perimeter defence safeguards including firewalls, routers, intrusion detection, anti-virus/anti-spyware/anti-malware software) to mediate all traffic and to protect systems that are accessible from the internet.		
20. All systems exposed to the internet or servers supporting sensitive applications are "hardened" (e.g. by removing or disabling unnecessary services and applications and properly configuring user authentication).		
Wireless		
21. We have a policy in place that addresses the use of wireless technology.		
22. We have enabled the strongest available security features of the wireless devices, including encryption and authentication.		
23. A wireless intrusion detection and prevention capability is deployed on our network to detect suspicious behaviour.		
Database Security		
24. Automated and/or manual controls have been implemented to protect against unauthorized disclosure of personal information.		
25. There is a formal approval process in place for handling requests for disclosure of database contents or for database access that includes an evaluation of the privacy impacts and security risks.		
Operating Systems		
26. Our operating systems are kept up-to-date with all patches and fixes.		
27. We use a regular schedule for updating definitions and running scans with anti-virus, anti-spyware, anti-malware and anti-rootkit software.		
28. We regularly check expert websites and vendor software websites for alerts about new vulnerabilities and patches.		
Email and Fax Security		
29. We regularly update our fax and email lists.		
30. All of our faxes include a fax cover sheet with sender contact information and a confidentiality notice.		
31. We do not send emails with sensitive personal information unless the recipient has consented to the use of email, the email service is secure or the email itself is encrypted.		
Data Integrity and Protection		
32. We have a procedure in place to ensure that any removal of personal information from the premises has been properly authorized.		
33. We use automated and/or manual controls to prevent unauthorized copying, transmission or printing of personal information.		
Access Control		
34. We have a role-based access control policy.		
35. We have a formal user registration process in place.		
36. Each user of our system is uniquely identified.		
37. We limit access privileges to the least amount of personal information required to carry out job-related functions.		
38. Users of our system must first be authenticated by username and unique password that is changed at least every 90 days.		

Information Systems Acquisition, Development and Maintenance		
	Yes	No
39. We always identify security requirements as part of any new system development, acquisition or enhancements.		
40. We have controls in place to prevent or detect unauthorized software.		
Incident Management		
41. We have a privacy incident management policy in place and we have assigned an individual to coordinate our response to any incident.		
Business Continuity Planning		
42. We have a backup process in place to protect essential business information.		
Compliance		
43. We regularly monitor system audit logs that relate to the handling of personal information.		
44. We maintain an up to date software/hardware inventory.		
45. We conduct a regular physical inventory of all portable storage devices (laptops, thumb drives, portable hard drives, cell phones).		

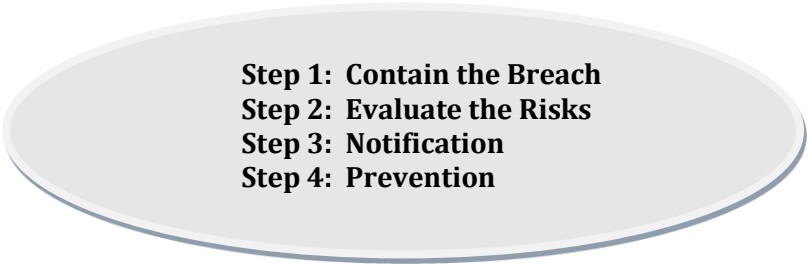
Tab 13

Key Steps to Responding to Privacy Breaches[10]

What is a privacy breach?

A privacy breach occurs whenever there is unauthorized access to or collection, use, disclosure or disposal of personal information. Such activity is unauthorized if it occurs in contravention of the *Freedom of Information and Protection of Privacy Act* (*FOIPOP*), the *Municipal Government Act Part XX* (*MGA*) or the *Personal Health Information Act* (*PHIA*).

What are the four key steps?



The first three steps should be undertaken immediately upon discovery of the breach or in very quick succession. The fourth step is undertaken once the causes of the breach are known, in an effort to find longer term solutions to the identified problem.

Purpose of the key steps document

Privacy breaches take many different forms, from misdirected faxes containing tax data, to the loss of hard drives containing personal information, to medical files blowing out the back of a garbage truck. Public bodies, municipalities and health custodians in Nova Scotia should be prepared to manage their responses to privacy breaches. The four key steps to responding to privacy breaches are steps that have been adopted across most Canadian jurisdictions in both the public and private sector. They represent best privacy practices for mitigating the harm arising from a privacy breach.

Use this document in combination with the Privacy Breach Checklist (p. 93 of this document) also available on our website at https://oipc.novascotia.ca.

[10] This document is adapted from material prepared by the Office of the Information Commissioner of British Columbia entitled: *Privacy Breaches: Tools and Resources* available at https://www.oipc.bc.ca/tools-guidance/guidance-documents.

Step 1: Contain the Breach

Before continuing, you should ensure that you record all steps taken to investigate and manage the breach. The Privacy Breach Checklist tool can be used to complete all of the steps set out below and to record all relevant information. That tool is available at p. 93 of this document and at: https://oipc.novascotia.ca.

You should take immediate and common sense steps to limit the breach including:

- **Contain:** Immediately contain the breach by, for example, stopping the unauthorized practice, shutting down the system that was breached, revoking or changing computer access codes, sending a remote "kill" signal to a lost or stolen portable storage device, correcting weaknesses in physical security or searching the neighborhood or used item websites (such as Kijiji) for items stolen from a car or house.

- **Initial Investigation:** Designate an appropriate individual to lead the initial investigation. Begin this process the day the breach is discovered. This individual should have the authority within the public body or organization to conduct the initial investigation and make initial recommendations. If necessary, a more detailed investigation may subsequently be required.

- **Privacy Officer & Other Internal Notifications:** Immediately contact your Privacy Officer and the person responsible for security in your organization. Determine others who need to be made aware of the incident internally at this stage. It is helpful to prepare in advance a list of all of the individuals who should be contacted along with current contact information.

- **Incident Response Team:** Determine whether an incident response team must be assembled which could include representatives from appropriate business areas (labour relations, legal, communications, senior management). Representatives from privacy and security should always be included and generally the privacy team is responsible for coordinating the response to the incident.

- **Police:** Notify the police if the breach involves theft or other criminal activity.

- **Preserve Evidence:** Do not compromise the ability to investigate the breach. Be careful not to destroy evidence that may be valuable in determining the cause, or, that will allow you to take appropriate corrective action.

Step 2: Evaluate the Risks

To determine what other steps are immediately necessary, you must assess the risks. Consider the following factors:

Personal Information Involved

- As soon as possible get a complete list of all of the personal information at risk. Generally this means developing a list of the data elements lost, stolen or inappropriately accessed. For example, the data could include, name, address, date of birth, medical diagnosis and health card number (MSI). At this stage it is important that the investigator confirm the data at risk as quickly as possible. Be aware that if the breach is caused by an error or oversight by an employee, he or she may be reluctant to fully disclose the scope of the lost data.

- Next, evaluate the sensitivity of the personal information. Some personal information is more sensitive than others. Generally, information including health information, government-issued pieces of information such as social insurance numbers, health care numbers and financial account numbers such as credit card numbers, is considered sensitive.

- Also consider the context of the information when evaluating sensitivity. For example, a list of customers on a newspaper carrier's route may not be sensitive. However, a list of customers who have requested service interruption while on vacation would be more sensitive.

- Finally, in your evaluation of sensitivity, consider the possible use of the information. Sometimes it is the combination of the data elements that make the information sensitive or capable of being used for fraudulent or otherwise harmful purposes.

- The more sensitive the information, the higher the risk.

Cause and Extent of the Breach

The cause and extent of the breach must also be considered in your analysis of the risks associated with the breach. Answer all of the following questions:

- What is the cause of the breach?
- Is there a risk of ongoing or further exposure of the information?
- What was the extent of the unauthorized collection, use or disclosure, including the number of likely recipients and the risk of further access, use or disclosure, including in mass media or online?
- Was the information lost or stolen? If it was stolen, can it be determined whether the information was the target of the theft or not?
- Is the information encrypted or otherwise not readily accessible?
- Has the personal information been recovered?
- What steps have you already taken to minimize the harm?
- Is this a systemic problem or an isolated incident?

Individuals Affected by the Breach

Knowing who was affected by the breach will shape your strategies in managing the breach and may also determine who will help manage the breach (e.g. union employees affected likely means labour relations should be on the incident response team), it will also determine who you decide to notify – if business partners are affected, then you will likely want to notify them.

- How many individuals are affected by the breach?
- Who was affected by the breach: employees, public, contractors, clients, service providers, other organizations?

Foreseeable Harm from the Breach

- Who is in receipt of the information? For example, a stranger who accidentally receives personal information and voluntarily reports the mistake is less likely to misuse the information than an individual suspected of criminal activity.

- Is there any relationship between the unauthorized recipients and the data subject? A close relationship between a victim and the recipient may increase the likelihood of harm – an estranged spouse is more likely to misuse information than a neighbour.

- What harm to the individuals will result from the breach? Harm that may occur includes:
    - Security risk (e.g. physical safety)
    - Identity theft or fraud
    - Loss of business or employment opportunities
    - Hurt, humiliation, damage to reputation or relationships
    - Basis for potential discriminatory action that may be taken against the individual
    - Social/relational harm (damage to the individual's relationships)

- What harm could result to the public body or organization as a result of the breach? For example:
    - Loss of trust in the public body or organization
    - Loss of assets
    - Financial exposure including class action lawsuits
    - Loss of contracts/business

- What harm could result to the public as a result of the breach? For example:
    - Risk to public health
    - Risk to public safety

Once you have assessed all of the risks described above you will be able to determine whether or not notification is an appropriate mitigation strategy. Further, the risk assessment will help you to identify appropriate prevention strategies.

The table below summarizes the risk factors and suggests a **possible** risk rating. Each public body, health custodian or municipality must make its own assessment of the risks given the unique circumstances of the situation. The table is intended to provide a rough guide to ratings.

Risk Rating Overview			
Factor	**Risk Rating**		
	Low	Medium	High
Nature of personal information	✓ Publicly available personal information not associated with any other information	✓ Personal information unique to the organization that is not medical or financial information	✓ Medical, psychological, counselling, or financial information or unique government identification number
Relationships	✓ Accidental disclosure to another professional who reported the breach and confirmed destruction or return of the information	✓ Accidental disclosure to a stranger who reported the breach and confirmed destruction or return of the information	✓ Disclosure to an individual with some relationship to or knowledge of the affected individual(s), particularly disclosures to motivated ex-partners, family members, neighbors or co-workers ✓ Theft by stranger
Cause of breach	✓ Technical error that has been resolved	✓ Accidental loss or disclosure	✓ Intentional breach ✓ Cause unknown ✓ Technical error – if not resolved
Scope	✓ Very few affected individuals	✓ Identified and limited group of affected individuals	✓ Large group or entire scope of group not identified

Risk Rating Overview			
Factor	**Risk Rating**		
	Low	Medium	High
Containment efforts	✓ Data was adequately encrypted ✓ Portable storage device was remotely wiped and there is evidence that the device was not accessed prior to wiping ✓ Hard copy files or device were recovered almost immediately and all files appear intact and/or unread	✓ Portable storage device was remotely wiped within hours of loss but there is no evidence to confirm that the device was not accessed prior to wiping ✓ Hard copy files or device were recovered but sufficient time passed between the loss and recovery that the data could have been accessed	✓ Data was not encrypted ✓ Data, files or device have not been recovered ✓ Data at risk of further disclosure particularly through mass media or online
Foreseeable harm from the breach	✓ No foreseeable harm from the breach	✓ Loss of business or employment opportunities ✓ Hurt, humiliation, damage to reputation or relationships ✓ Social/relational harm ✓ Loss of trust in the public body ✓ Loss of public body assets ✓ Loss of public body contracts or business ✓ Financial exposure to public body including class action lawsuits	✓ Security risk (e.g. physical safety) ✓ Identify theft or fraud risk ✓ Hurt, humiliation, damage to reputation may also be a high risk depending on the circumstances ✓ Risk to public health or safety

Step 3: Notification

Notification can be an important mitigation strategy that has the potential to benefit the public body, municipality, health custodian and the individuals affected by a breach. Prompt notification can help individuals mitigate the damage by taking steps to protect themselves. The challenge is to determine when notice should be required. Each incident needs to be considered on a case-by-case basis to determine whether the privacy breach notification is required. In addition, public bodies, municipalities and health custodians are encouraged to contact the Office of the Information and Privacy Commissioner for Nova Scotia for assistance in managing a breach.[11]

Review your risk assessment to determine whether notification is appropriate. If sensitive information is at risk, if the information is likely to be misused, if there is foreseeable harm, then you will likely want to notify. The list below provides further information to assist in decision making.

Note to health custodians: There are additional considerations set out specifically in *PHIA*. In particular, *PHIA* requires notification be given to either the affected individual or the Information and Privacy Commissioner in accordance with ss. 69 and 70 of *PHIA*.

Neither *FOIPOP* nor *Part XX* of the *MGA* requires notification. However, as noted above, notification in appropriate circumstances is best privacy practice and will help mitigate the losses suffered by individuals as a result of the breach. The steps taken in response to a breach have the potential to significantly reduce the harm caused by the breach, which will be relevant in any lawsuit for breach of privacy.

Notifying Affected Individuals

As noted above, notification of affected individuals should occur if it is necessary to avoid or mitigate harm to them. Some considerations in determining whether to notify individuals affected by the breach include:

- Legislation requires notification – s. 69 and s. 70 of *PHIA* for example;
- Contractual obligations require notification;
- There is a risk of identity theft or fraud – usually because of the type of information lost, stolen, accessed or disclosed, such as a SIN, banking information, identification numbers;
- There is a risk of physical harm – if the loss puts an individual at risk of stalking or harassment;

[11] The Office of the Information and Privacy Commissioner for Nova Scotia has the responsibility for monitoring how privacy provisions are administered and the ability to provide advice and comments on the privacy provisions when requested by public bodies and custodians. Our contact information is included on the last page of this document.

- There is a risk of hurt, humiliation or damage to reputation – for example when the information lost includes medical or disciplinary records;
- There is a risk of loss of business or employment opportunities – if the loss of information could result in damage to the reputation of an individual, affecting business or employment opportunities; and
- There is a risk of loss of confidence in the public body or organization and/or good citizen relations dictates that notification is appropriate.

When and How to Notify

Notification should occur as soon as possible following the breach – within days whenever possible. However, if you have contacted law enforcement authorities, you should determine from those authorities whether notification should be delayed in order not to impede a criminal investigation.

On very rare occasions, medical evidence may indicate that notification could reasonably be expected to result in immediate and grave harm to the individual's mental or physical health. In those circumstances, consider alternative approaches, such as having the physician give the notice in person or waiting until the immediate danger has passed.

Direct notification is preferred – by phone, by letter or in person. Indirect notification, via websites, posted notices or media reports, should generally only occur in rare circumstances such as where direct notification could cause further harm or contact information is lacking.

Using multiple methods of notification in certain cases may be the most effective approach.

What Should be Included in the Notification?

Notifications should include the following information:

- Date of the breach;
-
- Description of the breach;
- Description of the information inappropriately accessed, collected, used or disclosed;
- Risk(s) to the individual caused by the breach;
- The steps taken so far to control or reduce the harm;
- Where there is a risk of identity theft as a result of the breach, typically the notice should offer free credit watch protection as part of the mitigation strategy;
- Further steps planned to prevent future privacy breaches;
- Steps the individual can take to further mitigate the risk of harm (e.g. how to contact credit reporting agencies to set up a credit watch, information explaining how to change a personal health number or driver's license number);

- Contact information of an individual within the public body, municipality or health organization who can answer questions or provide further information;

- Information and Privacy Commissioner for Nova Scotia contact information and the fact that individuals have a right to complain to the Information and Privacy Commissioner under the *Privacy Review Officer Act* and *PHIA*. If the public body, municipality or health custodian has already contacted the Information and Privacy Commissioner, include this detail in the notification letter.

Other Sources of Information

As noted above, the breach notification letter should include a contact number within the public body, municipality or health custodian, in case affected individuals have further questions. In anticipation of further calls, you should prepare a list of frequently asked questions and answers to assist staff responsible for responding to further inquiries.

Others to Contact

Regardless of what you determine your obligations to be with respect to notifying individuals, you should consider whether the following authorities or organizations should also be informed of the breach:

- Police – if theft or other crime is suspected;

- Insurers or others - if required by contractual obligations;

- Professional or other regulatory bodies - if professional or regulatory standards require notification of these bodies;

- Other internal or external parties not already notified – your investigation and risk analysis may have identified other parties impacted by the breach such as third party contractors, internal business units or unions;

- Office of the Information and Privacy Commissioner for Nova Scotia - the mandate of the Office of the Information and Privacy Commissioner includes a responsibility to monitor how the privacy provisions are administered and to provide advice and comments on the privacy provisions when requested by public bodies and health custodians.

The following factors are relevant in deciding whether or not to report a breach to the Office of the Information and Privacy Commissioner for Nova Scotia:

- For health custodians, s. 70 of *PHIA* sets out when the Office of the Information and Privacy Commissioner for Nova Scotia must be contacted. Health custodians may wish to contact the Office of the Information and Privacy Commissioner even when notification is not required, based on some of the factors listed below:

- The sensitivity of the information – generally the more sensitive the information at risk, the more likely the Office of the Information and Privacy Commissioner for Nova Scotia will be notified;
- Whether the disclosed information could be used to commit identity theft;
- Whether there is a reasonable chance of harm from the disclosure including non-pecuniary losses;
- The number of people affected by the breach;
- Whether the information was fully recovered without further disclosure;
- Your public body, municipality or health custodian wishes to seek advice or comment from the Information and Privacy Commissioner to aid in managing the privacy breach;
- Your public body, municipality or health custodian requires assistance in developing a procedure for responding to the privacy breach, including notification;
- Your public body, municipality or health custodian is concerned that notification may cause further harm; and/or
- To ensure steps taken comply with the public body's obligations under privacy legislation.

Step 4: Prevention

Once the immediate steps are taken to mitigate the risks associated with the breach, you need to take the time to thoroughly investigate the cause of the breach. This could require a security audit of both physical and technical security. As a result of this evaluation, you should develop or improve as necessary adequate long-term safeguards against further breaches.

Typically, prevention strategies will address privacy controls in all of the following areas:

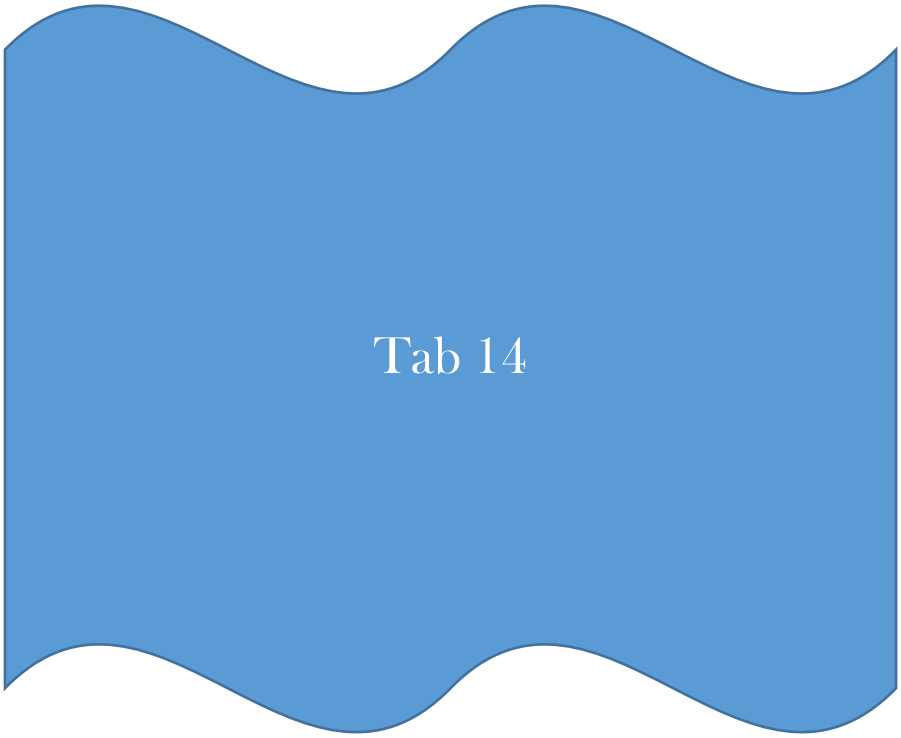
- Physical
- Technical
- Administrative
- Personnel

So, for example, if any physical security weaknesses contributed to the breach, changes made to prevent a recurrence should be undertaken. Systems controls should also be reviewed to ensure that all necessary technical safeguards are in place. This could mean encrypting all portable storage devices or improving firewall protections on a database.

Administrative controls would include ensuring that polices are reviewed and updated to reflect the lessons learned from the investigation and regularly after that. Your resulting plan should also include a requirement for an audit at the end of the process to ensure that the prevention plan has been fully implemented. If you do not already have a privacy breach protocol in place, ensure that one is developed as part of your plan.

Staff of public bodies, municipalities and health custodians should be trained to know the organization's privacy obligations under *FOIPOP*, *MGA Part XX* and/or *PHIA*.

In the longer term, public bodies, health custodians and municipalities should review and refresh their privacy management framework to ensure that they continue to comply with their privacy obligations. For more information on privacy management frameworks visit the Office of the Information and Privacy Commissioner for Nova Scotia website at: https://oipc.novascotia.ca.


Tab 14

Privacy Breach Checklist

Use this checklist to evaluate your response to a privacy breach and to decide whether or not to report the breach to the Office of the Information and Privacy Commissioner for Nova Scotia.[12] For a further explanation of how to manage a privacy breach see *Key Steps to Responding to Privacy Breaches* available at: https://oipc.novascotia.ca.

Date of report: _____

Date breach initially discovered: _____

Contact information:

Public Body/Health Custodian/Municipality: _____

Contact Person (Report Author): _____

Title: _____

Phone: _____ Fax: _____

E-Mail: _____

Mailing Address: _____

Incident Description

Describe the nature of the breach and its cause. How was the breach discovered and when? Where did it occur?

_____

_____

_____

_____

[12] The Office of the Information and Privacy Commissioner for Nova Scotia's mandate includes an obligation to monitor how privacy provisions are administered and to provide advice and comments on privacy provisions on the request of health custodians and public bodies.

Steps 1 & 2: Containment & Risk Evaluation

Answer each of the following questions and then, based on those answers, complete the risk evaluation summary on page 97.

(1) Containment

Check all of the factors that apply:

- ❑ The personal information has been recovered and all copies are now in our custody and control.
- ❑ We have confirmation that no copies have been made.
- ❑ We have confirmation that the personal information has been destroyed.
- ❑ We believe (but do not have confirmation) that the personal information has been destroyed.
- ❑ The personal information is encrypted.
- ❑ The personal information was not encrypted.
- ❑ Evidence gathered so far suggests that the incident was likely a result of a systemic problem.
- ❑ Evidence gathered so far suggests that the incident was likely an isolated incident.
- ❑ The personal information has not been recovered but the following containment steps have been taken (check all that apply):
    - ❑ The immediate neighbourhood around the theft has been thoroughly searched.
    - ❑ Used item websites are being monitored but the item has not appeared so far.
    - ❑ Pawn shops are being monitored.
    - ❑ A remote wipe signal has been sent to the device but no confirmation that the signal was successful has been received.
    - ❑ A remote wipe signal has been sent to the device and we have confirmation that the signal was successful.
    - ❑ Our audit confirms that no one has accessed the content of the portable storage device.
    - ❑ We do not have an audit that confirms that no one has accessed the content of the portable storage device.
    - ❑ All passwords and system user names have been changed.

Describe any other containment strategies used:

_____

_____

_____

_____

(2) Nature of Personal Information Involved

List all of the data elements involved (e.g. name, date of birth, SIN, address, medical diagnoses, connection with identified service provider such as welfare or counselling etc.)

- ❑ Name
- ❑ Address
- ❑ Date of birth
- ❑ Government ID number (specify) _____
- ❑ SIN
- ❑ Financial information
- ❑ Medical information
- ❑ Personal characteristics such as race, religion, sexual orientation
- ❑ Other (describe)

_____

_____

_____

_____

(3) Relationship

What is the relationship between the recipient of the information and the individuals affected by the breach?

- ❑ Stranger
- ❑ Friend
- ❑ Neighbour
- ❑ Ex-partner
- ❑ Co-worker
- ❑ Unknown
- ❑ Other (describe)

_____

_____

_____

_____

(4) Cause of the Breach

Based on your initial investigation of the breach, what is your best initial evaluation of the cause of the breach?

- ❑ Accident or oversight
- ❑ Technical error
- ❑ Intentional theft or wrongdoing
- ❑ Unauthorized browsing
- ❑ Unknown
- ❑ Other (describe)

_____

_____

_____

(5) Scope of the Breach

How many people were affected by the breach?

- ❑ Very few (less than 10)
- ❑ Identified and limited group (>10 and <50)
- ❑ Large number of individuals affected (>50)
- ❑ Numbers are not known

(6) Foreseeable Harm

Identify the types of harm that may result from the breach. Some relate strictly to the affected individual, but harm may also be caused to the public body and other individuals if notifications do not occur:

- ❑ **Identify theft** (most likely when the breach includes loss of SIN, credit card numbers, driver's licence numbers, debit card information etc.)
- ❑ **Physical harm** (when the information places any individual at risk of physical harm from stalking or harassment)
- ❑ **Hurt, humiliation, damage to reputation** (associated with the loss of information such as mental health records, medical records, disciplinary records)
- ❑ **Loss of business or employment opportunities** (usually as a result of damage to reputation to an individual)
- ❑ **Breach of contractual obligations** (contractual provisions may require notification of third parties in the case of a data loss or privacy breach)
- ❑ **Future breaches due to technical failures** (notification to the manufacturer may be necessary if a recall is warranted and/or to prevent a future breach by other users)
- ❑ **Failure to meet professional standards or certification standards** (notification may be required to a professional regulatory body or certification authority)
- ❑ **Other** (specify)

_____

(7) Other Factors

The nature of the public body's relationship with the affected individuals may be such that the public body wishes to notify no matter what the other factors are because of the importance of preserving trust in the relationship. Consider the type of individuals that were affected by the breach.

- ❑ Client/customer/patient
- ❑ Employee
- ❑ Student or volunteer
- ❑ Other (describe)

_____

Risk Evaluation Summary:

For each of the factors reviewed above, determine the risk rating.

Risk Factor	**Risk Rating**		
	Low	Medium	High
1) Containment			
2) Nature of the personal information			
3) Relationship			
4) Cause of the breach			
5) Scope of the breach			
6) Foreseeable harm from the breach			
7) Other factors			
Overall Risk Rating			

Use the risk rating to help decide whether notification is necessary and to design your prevention strategies. Foreseeable harm from the breach is usually the key factor used in deciding whether or not to notify affected individuals. Step 3 below analyzes this in more detail. In general though, a medium or high risk rating will always result in notification to the affected individuals. A low risk rating may also result in notification depending on the unique circumstances of each case.

Step 3: Notification

(1) Should Affected Individuals be Notified?

Once you have completed your overall risk rating, determine whether or not notification of affected individuals is required. If any of the following factors apply, notification should occur. If the *PHIA* test is satisfied, notification must occur.

Consideration	Description	Factor applies
Legislation	Health custodians in Nova Scotia must comply with sections 69 & 70 of *PHIA* which require notification.	
Risk of identity theft	Most likely when the breach includes loss of SIN, credit card number, driver's license number, debit card information, etc.	
Risk of physical harm	When the information places any individual at risk of physical harm from stalking or harassment.	
Risk of hurt, humiliation, damage to reputation	Often associated with the loss of information such as mental health records, medical records or disciplinary records.	
Loss of business or employment opportunities	Where the breach could affect the business reputation of an individual.	
Explanation required	The public body may wish to notify if the affected individuals include vulnerable individuals, or where individuals require information to fully understand the events, even when the risks have been assessed as low.	
Reputation of public body	Where the public body is concerned that the breach will undermine trust of citizens, the public body may decide to notify in order to ease concerns and to provide clear information regarding the risks and mitigation strategies undertaken, even when risks assessed are low.	

(2) When and How to Notify

When: Notification should occur as soon as possible following a breach. However, if you have contacted law enforcement authorities, you should determine from those authorities whether notification should be delayed in order not to impede a criminal investigation.

How: The preferred method is direct – by phone, letter, email or in person. Indirect notification via website information, posted notices or media should generally only occur where direct notification could cause further harm, is prohibitive in cost, or contact information is lacking. Using multiple methods of notification in certain cases may be the most effective approach.

Considerations Favouring Direct Notification	**Check If Applicable**
The identities of individuals are known	
Current contact information for the affected individuals is available	
Individuals affected by the breach require detailed information in order to properly protect themselves from the harm arising from the breach	
Individuals affected by the breach may have difficulty understanding an indirect notification (due to mental capacity, age, language, etc.)	
Considerations Favouring Indirect Notification	
A very large number of individuals are affected by the breach, such that direct notification could be impractical	
Direct notification could compound the harm to the individuals resulting from the breach	

(3) What to Include in Breach Notification Letters

The information included in the notice should help the individual to reduce or prevent the harm that could be caused by the breach. Include all of the information set out below:

Essential Elements in Breach Notification Letters	**Included**
Date of breach	
Description of breach	
Description of personal information affected	
Steps taken so far to control or reduce harm (containment)	
Future steps planned to prevent further privacy breaches	
Steps individuals can take - consider offering credit monitoring where appropriate	
Information and Privacy Commissioner's contact information – Individuals have a right to complain to the Information and Privacy Commissioner for Nova Scotia	
Public body, municipality or health custodian contact information – for further assistance	

(4) Others to Contact

Authority or Organization	Reason for Contact	Applicable
Law enforcement	If theft or crime is suspected.	
Information and Privacy Commissioner for Nova Scotia	• For assistance with developing a procedure for responding to the breach, including notification to ensure steps taken comply with obligations under privacy legislation. • The personal information is sensitive. • There is a risk of identity theft or other significant harm. • A large number of people are affected. • The information has not been fully recovered. • The breach is a result of a systemic problem or a similar breach has occurred before.	
Professional or regulatory bodies	If professional or regulatory standards require notification of the regulatory or professional body.	
Insurers	Where required in accordance with an insurance policy.	
Technology suppliers	If the breach was due to a technical failure and a recall or technical fix is required.	

Confirm notifications completed

Key contact	Notified
Privacy officer within your public body, municipality or health custodian	
Police (as required)	
Affected individuals	
Information and Privacy Commissioner for Nova Scotia	
Professional or regulatory body – identify:	
Technology suppliers	
Others (list):	

Step 4: Prevention

Once the immediate steps are taken to mitigate the risks associated with the breach, you need to take the time to thoroughly investigate the cause of the breach. This could require a security audit of both physical and technical security. As a result of this evaluation, you should develop or improve as necessary adequate long term safeguards against future breaches.

Consider making improvements in each of the following areas listed below. Also, take the opportunity to revisit your privacy management framework,[13] and assess if any further adjustments are necessary as part of your prevention strategy.

Physical Controls
What physical controls were in place at the time of the breach? Describe any modifications to physical controls such as locks, alarms, security monitoring, or visitor access control.

Technical Controls
Was there an IT security strategy in place at the time of the breach? Describe any modification to technical controls intended to prevent future similar breaches.

Administrative Controls
Administrative controls refer to the procedural safeguards implemented for safe handling of personal information, which includes the enforcement of an institution's policies, directives and processes for the protection of personal information throughout its lifecycle. Describe the administrative controls in place at the time of the breach. Describe improvements made to administrative controls in response to the breach. If you do not already have a privacy breach protocol in place, ensure that one is developed as part of your plan.

Personnel Security Controls
Personnel security controls refer to a public body's (or health custodian's) management of its employees – suitability, proper training, supervision and disciplinary procedures. What personnel security controls were in place at the time of the breach - for example, security clearances, confidentiality agreements and privacy training requirements? What steps have been taken to improve personnel security controls in this particular case and in general to prevent future similar breaches?

[13] For information on what constitutes a privacy management framework visit the tools page on the Office of the Information and Privacy Commissioner for Nova Scotia's website at: https://oipc.novascotia.ca.

Tab 15

Insert Organization Name
Nova Scotia
Privacy Breach Management Protocol Template

Introduction:
This template was drafted by the Office of the Information and Privacy Commissioner for Nova Scotia. All words highlighted require consideration by the organization adapting this template for its own purposes. Sometimes the words need to be deleted (as with this paragraph) or sometimes the organization may wish to substitute words or names in place of the highlighted text (for example insert the organization's name in every place where "the organization" is mentioned). Use this document in combination with the *Key Steps to Responding to Privacy Breaches* document produced by the OIPC Nova Scotia and available at: https://oipc.novascotia.ca.

Organization:
Date:

Author:

Index:

1. What is the purpose of the privacy breach management protocol?

The protocol allows the organization to identify, manage and resolve privacy breaches. It applies to all of the organization's information assets – such as personal information, personal health information, workforce personal information, and employee personal information. All workers at the organization must follow this protocol, including all full-time and part-time employees, contract employees, contractors, people on secondment, temporary workers and students. (municipalities should add elected officials to this list).

2. What is a privacy breach?

A breach is any event that results in personal information in the custody or control of the organization being accessed, used, copied, modified, disclosed or disposed of in an unauthorized fashion, either deliberately or inadvertently.

Some examples of breaches include:

- A USB key with unencrypted personal information being lost or stolen.
- An excel spreadsheet containing employee benefit information being emailed to the wrong person.
- Employees inappropriately browsing data files containing personal information for non-work related purposes.
- Hacker engaging in malicious activity resulting in the compromise of the organization's personal information assets.

3. Roles and responsibilities

Note: Below is a sample of the positions that will have some responsibility for managing a privacy breach. Titles may vary from organization to organization and so when completing this template, insert the appropriate title for your organization. The responsibilities listed must be assigned to someone within your organization if the breach is to be properly managed. The responsibilities listed are described in more detail in the breach management process section of this document.

The following table summarizes the responsibilities of staff when a privacy breach is discovered.

Position	Responsibilities
• All staff	• Complete preliminary breach assessment report. (Appendix 1) and immediately report privacy breach to Chief Privacy Officer. • Immediately undertake containment efforts. • Assist with breach investigations as required.
• Chief Privacy Officer	• Receive preliminary breach assessment reports. • Assess the preliminary report to determine whether a privacy breach has occurred. • Recommend immediate containment efforts. • Identify and contact individuals to form an Incident Response Team. • Conduct appropriate internal notifications of the breach.

	• Conduct a full assessment of the breach – complete the privacy breach checklist (Appendix 2). • With the Incident Response Team, determine whether notification of affected individuals is required. • In consultation with communications staff, complete notification. • Notify and liaise with the Information and Privacy Commissioner. • With the Incident Response Team, identify risk mitigation and prevention strategies. • Assign responsibility for completing mitigation and prevention strategies. Follow up to ensure actions are completed. • Conduct trend analysis of privacy breaches. • Keep executive informed of all actions and decisions of the Incident Response Team.
• Chief Security Officer	• Participate on Incident Response Teams when the privacy breach involves systems. • Assist in investigations as to the cause of system-related breaches. • Identify containment and prevention strategies. • Assist in implementation of containment and prevention strategies involving IT or security resources.
• Legal counsel	• Participate as required on the Incident Response Team. • Assist Chief Privacy Officer in assessing whether notification is required.
• Communications staff	• Assist in the drafting of breach notification letters.
• Labour relations/human resources staff.	• Assist in implementation of containment and prevention strategies that require cooperation of staff, particularly unionized staff.
• Office of primary responsibility – manager or supervisor	• Participate on Incident Response Team. • Assist in identifying containment, mitigation and prevention strategies. • Implement containment, mitigation and prevention strategies.
• Executive	• Receive and review all reports of privacy breaches. • Follow up with Chief Privacy Officer to ensure that containment, notification and prevention actions have been completed.

4. Breach management process

Step 1: Preliminary Report, Assessment & Containment
Step 2: Full Assessment
Step 3: Notification
Step 4: Mitigation and Prevention
Step 5: Lessons Learned

Step 1: Preliminary Report, Assessment & Containment
When a suspected privacy breach occurs, the employee who discovers the breach must conduct a preliminary assessment to identify the nature of the breach and to identify potential containment steps.

Employees who discover potential breaches must:

- Immediately complete the Preliminary Breach Assessment Report (Appendix 1). The report assists employees in identifying a privacy breach and in identifying useful containment strategies. The preliminary report should be completed on the day the breach is discovered.
- Contact the Chief Privacy Officer and provide a copy of the Preliminary Breach Assessment Report on the day the breach is discovered.
- Advise his/her supervisor of the potential privacy breach and of steps taken to contain the breach on the day the breach is discovered.

Supervisors and employees who discover potential breaches must:

- Take immediate action to contain the breach and to secure the affected records, systems, email or websites. Review the Preliminary Breach Assessment Report (Appendix 1) for suggested containment strategies.

Step 2: Full Assessment
Upon receipt of a notification of a potential privacy breach, the Chief Privacy Officer must:

- Obtain a copy of the Preliminary Breach Assessment Report from the reporting employee (Appendix 1).
- Identify appropriate staff to form an Incident Response Team and organize an immediate meeting of the team.
- Identify breach containment strategies and assign responsibility for their implementation. Containment strategies should be identified and implemented on the day the breach is discovered.
- Conduct an investigation and complete the Privacy Breach Checklist including a risk assessment (Appendix 2). Conduct this step within one to five days of the breach.
- Based on the Privacy Breach Checklist and in consultation with the Incident Response Team, determine whether notification is appropriate and identify prevention strategies. Conduct this step within one to five days of the breach.
- Complete notification of affected individuals and notification of the Information and Privacy Commissioner. Conduct this step as soon as possible, generally within one to five days of the breach.

Step 3: Notification
The Incident Response Team, in consultation with the Chief Privacy Officer, will determine whether and to whom notification will be given. Notification is an important mitigation strategy that can benefit both the organization and the individuals affected by a breach. There are a number of individuals and organizations that may require notification:

(a) Internal officials: The Incident Response Team should identify appropriate officials within the organization who require notification of the breach.

(b) Affected individuals: If a breach creates a risk of harm to any individuals, those affected should be notified. The Privacy Breach Checklist (Appendix 2) includes an assessment for whether notification should occur and how notification should be completed. The Privacy Breach Checklist also identifies the information that must be included in any breach notification letter.

(c) Office of the Information and Privacy Commissioner
The Chief Privacy Officer will notify the Office of the Information and Privacy Commissioner by phone, fax or email.

(d) Others
Appendix 2 includes a list of other organizations or individuals who may require notification depending on the facts of the breach. The Chief Privacy Officer is responsible for implementing any notification decisions made by the Incident Response Team.

Caution: In responding to a privacy breach, be careful not to take steps that may exacerbate the existing breach or create a new one (i.e. disclosing additional personal information, notification letters addressed to the wrong person, notification letters that disclose information in the return address).

Step 4: Mitigation and Prevention
Once the immediate steps have been taken to mitigate the risks associated with the privacy breach and to provide appropriate notification, the Office of Primary Responsibility (the office where the breach occurred), the Chief Privacy Officer and the Incident Response Team must investigate the cause of the breach thoroughly, consider whether to develop a prevention plan and consider what that plan might include.

Mitigation and prevention strategies developed should reflect the significance of the breach and whether the breach was a systemic or isolated event. Mitigation and prevention plan may include the following:

Physical controls
- Audit physical controls to identify outstanding weaknesses.
- Modify physical controls such as locks, alarms, security monitoring, or visitor access control to improve level of security.

Technical controls
- Tighten restrictions on access to certain personal information based on roles, responsibilities and need to know.
- Encrypt personal information particularly on portable storage devices.
- Limit the ability to copy data to thumb drives.
- Limit access to non-work email.

Administrative controls

- Review the enforcement of the organization's policies, directives and process for the protection of personal information throughout its lifecycle.
- Revise or develop internal procedures and policies to address shortcomings identified.
- Develop contractual clauses to deal with breaches of privacy by third party service providers.

Personnel security controls

- Training and education
- Coaching/mentoring
- Disciplinary actions (reprimands, suspension, reassignment, termination)
- Revoke privileges and/or user access to system or records

Step 5: Lessons Learned

The Chief Privacy Officer will track all privacy breaches across the organization and will use that information to identify trends both in the types of breaches occurring and within each step of the privacy breach management process. Collecting this information can facilitate identifying underlying patters with respect to personal information handling practices and may prevent future breaches.

Appendix 1: Preliminary Privacy Breach Assessment Report

Report Prepared by: **Date:**

Email:

Phone:

A. Breach Identification and Containment

Instructions: Review the preliminary assessment list below. If you answer yes to any of the questions below, complete the remainder of this assessment report and immediately (same day) forward a copy of this report to the Chief Privacy Officer.

Preliminary Assessment	Yes/ No	Suggested Containment Strategies
1. Was there an abuse of access privileges (e.g. unauthorized access or use of records that contain personal information)?		a) Immediately restrict, suspend or revoke access privileges until completion of the investigation. b) Determine whether personal information was further disclosed to others (verbally or via copies). c) Attempt to retrieve the documents in question, and document the steps taken. d) Complete this *Preliminary Report* and contact the Chief Privacy Officer.
2. Was personal information inappropriately disclosed (e.g. improper application of severances (material removed or blacked out), incomplete de-identification)?		a) Attempt to retrieve documents. b) Determine whether personal information was further disclosed to others (verbally or via copies). c) Document the steps taken. d) Complete this *Preliminary Report* and contact the Chief Privacy Officer.
3. Was personal information lost (e.g. through the mail, during a move or on a misplaced electronic device)?		a) Attempt to retrace steps and find the lost document(s). b) Determine whether personal information was further disclosed to others (verbally or via copies). c) Document the steps taken. d) Conduct an inventory of the personal information that was or may have been compromised. e) Complete this *Preliminary Report* and contact the Chief Privacy Officer.

Preliminary Assessment	Yes/ No	Suggested Containment Strategies
4. Was personal information stolen (e.g. theft of computer equipment or devices)?		a) Attempt to retrieve the stolen equipment or device. b) Document the steps taken. c) Complete this *Preliminary Report* and contact the Chief Privacy Officer.
5. Was personal information in an unencrypted email sent to the wrong address?		a) Cease transmission of email or correspondence to the incorrect address. b) Determine whether the email address is incorrect in the system (e.g. programmed incorrectly into the system). c) Attempt to recall the message. d) Determine where the email went. e) Request that the recipient delete all affected email or correspondence, with confirmation via email that this has been done. f) Determine whether personal information was further disclosed to others (verbally or via copies). g) Document the steps taken. h) Complete this *Preliminary Report* and contact the Chief Privacy Officer.
6. Was personal information faxed, mailed or delivered to a wrong address?		a) Determine where the document went. b) Determine whether the address is incorrect in the system (e.g. programmed incorrectly into system). c) Request that the recipient return the document(s) if mailed, or request that the fax be destroyed, with confirmation that this has been done. d) Determine whether personal information was further disclosed to others (verbally or via copies). e) Document the steps taken. f) Complete this *Preliminary Report* and contact the Chief Privacy Officer.
7. Did a third party compromise (hack into) a system that contains personal information?		a) Contact security and IT to isolate the affected system, disable the affected system, or disable the user account to permit a complete assessment of the breach and resolve vulnerabilities. b) Document the steps taken. c) Complete this *Preliminary Report* and contact the Chief Privacy Officer.
8. Did the sale or disposal of equipment or devices that contain personal information occur without a complete and irreversible purging of the item before its sale or disposal?		a) Contact IT. b) Document the steps taken. c) Complete this *Preliminary Report* and contact the Chief Privacy Officer.
9. Was there an inappropriate display of personal information clearly visible to employees or clients? (e.g.		a) Remove, move or segregate exposed information or files. b) Preserve evidence. c) Determine whether personal information was further disclosed to others (verbally or via copies).

Preliminary Assessment	Yes/ No	Suggested Containment Strategies
posting of medical appointments or types of leave, home telephone numbers, slides of PowerPoint presentations that contain personal information, etc.)?		d) Document the steps taken. e) Complete this *Preliminary Report* and contact the Chief Privacy Officer.
10. Was there an inappropriate collection of personal information?		a) Determine whether personal information was further disclosed to others (verbally or via copies). b) Complete this *Preliminary Report* and contact the Chief Privacy Officer.
11. Was there an unexpected or unintended use of collected data? Is there a risk for re-identification of an affected individual or another identifiable individual?		a) Determine whether personal information was further disclosed to others (verbally or via copies) b) Complete this *Preliminary Report* and contact the Chief Privacy Officer.
12. Was there an improper or unauthorized creation of personal information?		a) Complete this *Preliminary Report* and contact the Chief Privacy Officer.
13. Was there an improper or unauthorized retention of personal information?		a) Complete this *Preliminary Report* and contact the Chief Privacy Officer.
14. Remarks/Other:		

B. Breach Details		
1. Date(s) of breach:	2. Time of breach:	3. Location of breach:
4. When and how was the breach discovered?		
5. Provide a brief description of the breach (what happened, how it happened, etc.):		
6. Identify the person whose information was compromised (name and personal record identifiers, if applicable). If information regarding more than one person was compromised, please attach a list.		7. Is/are the affected individual(s) aware of the breach? __ Yes __ No Whether yes or no, request direction from the Chief Privacy Officer or the OIPC.
8. Format of information involved: ____ Electronic records ____ Paper records ____ Other (describe): _____	9. What information was involved (check all that apply): ____ Medical _____ Employee ____ Other (describe): _____	
10. List the immediate containment actions and/or interventions, if any:		
11. Is there information or evidence to support the allegation of the breach? If yes, please specify:		
12. Has your supervisor been notified of the breach? __ Yes __ No		
C. Please name the person(s) directly involved in this breach (witnesses, investigator, individual who may have caused the breach, victims, etc.). Attach a list if necessary.		
1. Name	Title/Position	Contact information:
2. How was this person involved?		
3. Name	Title/Position	Contact information:
4. How was this person involved?		

Send this form immediately to the Chief Privacy Officer at [insert contact information – email & phone #]

Appendix 2: Privacy Breach Checklist

Use this checklist to evaluate your response to a privacy breach and to decide whether or not to report the breach to the Office of the Information and Privacy Commissioner.[14] For a further explanation of how to manage a privacy breach see *Key Steps to Responding to Privacy Breaches* available at: https://oipc.novascotia.ca.

Date of report: _____

Date breach initially discovered: _____

Contact information:

Public Body/Health Custodian/Municipality: _____

Contact Person (Report Author): _____

Title: _____

Phone: _____ Fax: _____

E-Mail: _____

Mailing Address: _____

Incident Description

Describe the nature of the breach and its cause. How was the breach discovered and when? Where did it occur?

_____

_____

_____

_____

[14] The OIPC can be reached by phone at 902-424-4684 or 1-866-243-1564, by fax at (902) 424-8303 and by email at oipcns@novascotia.ca.

Steps 1 & 2: Containment & Risk Evaluation

Answer each of the following questions and then, based on those answers, complete the risk evaluation summary on page 117.

(1) Containment

Check all of the factors that apply:

- ❑ The personal information has been recovered and all copies are now in our custody and control.
- ❑ We have confirmation that no copies have been made.
- ❑ We have confirmation that the personal information has been destroyed.
- ❑ We believe (but do not have confirmation) that the personal information has been destroyed.
- ❑ The personal information is encrypted.
- ❑ The personal information is not encrypted.
- ❑ Evidence gathered so far suggests that the incident was likely a result of a systemic problem.
- ❑ Evidence gathered so far suggests that the incident was likely an isolated incident.
- ❑ The personal information has not been recovered but the following containment steps have been taken (check all that apply):
    - ❑ The immediate neighbourhood around the theft has been thoroughly searched.
    - ❑ Used item websites are being monitored but the item has not appeared so far.
    - ❑ Pawn shops are being monitored.
    - ❑ A remote wipe signal has been sent to the device but no confirmation that the signal was successful has been received.
    - ❑ A remote wipe signal has been sent to the device and we have confirmation that the signal was successful.
    - ❑ Our audit confirms that no one has accessed the content of the portable storage device.
    - ❑ We do not have an audit that confirms that no one has accessed the content of the portable storage device.
    - ❑ All passwords and system user names have been changed.

Describe any other containment strategies used:

_____

_____

_____

_____

(2) Nature of Personal Information Involved

List all of the data elements involved (e.g. name, date of birth, SIN, address, medical diagnoses, connection with identified service provider such as welfare or counselling etc.)

- ❑ Name
- ❑ Address
- ❑ Date of birth
- ❑ Government ID number (specify) _____
- ❑ SIN
- ❑ Financial information
- ❑ Medical information
- ❑ Personal characteristics such as race, religion, sexual orientation
- ❑ Other (describe)

_____

_____

_____

_____

(3) Relationship

What is the relationship between the recipient of the information and the individuals affected by the breach?

- ❑ Stranger
- ❑ Friend
- ❑ Neighbour
- ❑ Ex-partner
- ❑ Co-worker
- ❑ Unknown
- ❑ Other (describe)

_____

_____

_____

_____

(4) Cause of the Breach

Based on your initial investigation of the breach, what is your best initial evaluation of the cause of the breach?

- ❑ Accident or oversight
- ❑ Technical error
- ❑ Intentional theft or wrongdoing
- ❑ Unauthorized browsing
- ❑ Unknown
- ❑ Other (describe)

_____

_____

_____

(5) Scope of the Breach

How many people were affected by the breach?

- ❑ Very few (less than 10)
- ❑ Identified and limited group (>10 and <50)
- ❑ Large number of individuals affected (>50)
- ❑ Numbers are not known

(6) Foreseeable Harm

Identify the types of harm that may result from the breach. Some relate strictly to the affected individual; but harm may also be caused to the public body and other individuals if notifications do not occur:

- ❑ **Identify theft** (most likely when the breach includes loss of SIN, credit card numbers, driver's licence numbers, debit card information etc.)
- ❑ **Physical harm** (when the information places any individual at risk of physical harm from stalking or harassment)
- ❑ **Hurt, humiliation, damage to reputation** (associated with the loss of information such as mental health records, medical records, disciplinary records)
- ❑ **Loss of business or employment opportunities** (usually as a result of damage to reputation to an individual)
- ❑ **Breach of contractual obligations** (contractual provisions may require notification of third parties in the case of a data loss or privacy breach)
- ❑ **Future breaches due to technical failures** (notification to the manufacturer may be necessary if a recall is warranted and/or to prevent a future breach by other users)
- ❑ **Failure to meet professional standards or certification standards** (notification may be required to a professional regulatory body or certification authority)
- ❑ **Other** (specify)

_____

(7) Other Factors

The nature of the public body's relationship with the affected individuals may be such that the public body wishes to notify no matter what the other factors are because of the importance of preserving trust in the relationship. Consider the type of individuals that were affected by the breach.

- ❑ Client/customer/patient
- ❑ Employee
- ❑ Student or volunteer
- ❑ Other (describe)

_____

Risk Evaluation Summary:

For each of the factors reviewed above, determine the risk rating.

Risk Factor	**Risk Rating**		
	Low	Medium	High
1) Containment			
2) Nature of the personal information			
3) Relationship			
4) Cause of the breach			
5) Scope of the breach			
6) Foreseeable harm from the breach			
7) Other factors			
Overall Risk Rating			

Use the risk rating to help decide whether notification is necessary and to design your prevention strategies. Foreseeable harm from the breach is usually the key factor used in deciding whether or not to notify affected individuals. Step 3 below analyzes this in more detail. In general though, a medium or high risk rating will always result in notification to the affected individuals. A low risk rating may also result in notification depending on the unique circumstances of each case.

Step 3: Notification

(1) Should affected Individuals be Notified?

Once you have completed your overall risk rating, determine whether or not notification of affected individuals is required. If any of the following factors apply, notification should occur. If the *PHIA* test is satisfied, notification must occur.

Consideration	Description	Factor applies
Legislation	Health custodians in Nova Scotia must comply with sections 69 & 70 of *PHIA* which require notification.	
Risk of identity theft	Most likely when the breach includes loss of SIN, credit card number, driver's licence number, debit card information, etc.	
Risk of physical harm	When the information places any individual at risk of physical harm from stalking or harassment.	
Risk of hurt, humiliation, damage to reputation	Often associated with the loss of information such as mental health records, medical records or disciplinary records.	
Loss of business or employment opportunities	Where the breach could affect the business reputation of an individual.	
Explanation required	The public body may wish to notify if the affected individuals include vulnerable individuals, or where individuals require information to fully understand the events, even when the risks have been assessed as low.	
Reputation of public body	Where the public body is concerned that the breach will undermine trust of citizens, the public body may decide to notify in order to ease concerns and to provide clear information regarding the risks and mitigation strategies undertaken, even when risks assessed are low.	

(2) When and How to Notify

When: Notification should occur as soon as possible following a breach. However, if you have contacted law enforcement authorities, you should determine from those authorities whether notification should be delayed in order not to impede a criminal investigation.

How: The preferred method is direct – by phone, letter, email or in person. Indirect notification via website information, posted notices or media should generally only occur where direct notification could cause further harm, is prohibitive in cost, or contact information is lacking. Using multiple methods of notification in certain cases may be the most effective approach.

Considerations Favouring Direct Notification	**Check If Applicable**
The identities of individuals are known	
Current contact information for the affected individuals is available	
Individuals affected by the breach require detailed information in order to properly protect themselves from the harm arising from the breach	
Individuals affected by the breach may have difficulty understanding an indirect notification (due to mental capacity, age, language, etc.)	
Considerations Favouring Indirect Notification	
A very large number of individuals are affected by the breach, such that direct notification could be impractical	
Direct notification could compound the harm to the individuals resulting from the breach	

(3) What to Include in Breach Notification Letters

The information included in the notice should help the individual to reduce or prevent the harm that could be caused by the breach. Include all of the information set out below:

Essential Elements in Breach Notification Letters	**Included**
Date of breach	
Description of breach	
Description of personal information affected	
Steps taken so far to control or reduce harm (containment)	
Future steps planned to prevent further privacy breaches	
Steps individuals can take - consider offering credit monitoring where appropriate	
Information and Privacy Commissioner's contact information – Individuals have a right to complain to the Information and Privacy Commissioner	
Public body, municipality or health custodian contact information – for further assistance	

(4) Others to Contact

Authority or Organization	Reason for Contact	Applicable
Law enforcement	If theft or crime is suspected	
Information and Privacy Commissioner for Nova Scotia	• For assistance with developing a procedure for responding to the breach, including notification to ensure steps taken comply with obligations under privacy legislation • The personal information is sensitive • There is a risk of identity theft or other significant harm • A large number of people are affected • The information has not been fully recovered • The breach is a result of a systemic problem or a similar breach has occurred before	
Professional or regulatory bodies	If professional or regulatory standards require notification of the regulatory or professional body	
Insurers	Where required in accordance with an insurance policy	
Technology suppliers	If the breach was due to a technical failure and a recall or technical fix is required	

Confirm notifications completed

Key contact	Notified
Privacy officer within your public body, municipality or health custodian	
Police (as required)	
Affected individuals	
Information and Privacy Commissioner for Nova Scotia	
Professional or regulatory body – identify:	
Technology suppliers	
Others (list):	

Step 4: Prevention

Once the immediate steps are taken to mitigate the risks associated with the breach, you need to take the time to thoroughly investigate the cause of the breach. This could require a security audit of both physical and technical security. As a result of this evaluation, you should develop or improve as necessary adequate long-term safeguards against future breaches.

Consider making improvements in each of the following areas listed below. Also, take the opportunity to revisit your privacy management framework,[15] and assess if any further adjustments are necessary as part of your prevention strategy.

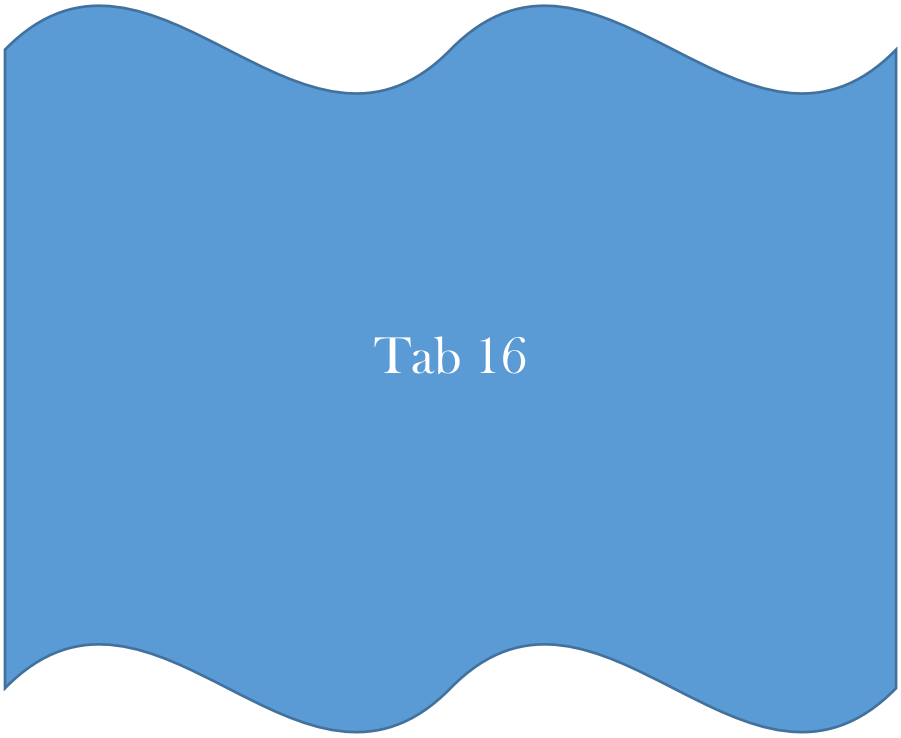
Physical Controls
What physical controls were in place at the time of the breach? Describe any modifications to physical controls such as locks, alarms, security monitoring, or visitor access control.

Technical Controls
Was there an IT security strategy in place at the time of the breach? Describe any modification to technical controls intended to prevent future similar breaches.

Administrative Controls
Administrative controls refer to the procedural safeguards implemented for safe handling of personal information, which includes the enforcement of an institution's policies, directives and processes for the protection of personal information throughout its lifecycle. Describe the administrative controls in place at the time of the breach. Describe improvements made to administrative controls in response to the breach. If you do not already have a privacy breach protocol in place, ensure that one is developed as part of your plan.

Personnel Security Controls
Personnel security controls refer to a public body's (or health custodian's) management of its employees – suitability, proper training, supervision and disciplinary procedures. What personnel security controls were in place at the time of the breach - for example, security clearances, confidentiality agreements and privacy training requirements? What steps have been taken to improve personnel security controls in this particular case and in general to prevent future similar breaches?

[15] For information on what constitutes a privacy management framework visit the tools tab on the Office of the Information and Privacy Commissioner website at: https://oipc.novascotia.ca.


Tab 16

Privacy Management Program – At a Glance[16]

A. Building Blocks		
Public Body Commitment	**Executive-level support**	Senior executive-level management support is key to a successful privacy management program and essential for a privacy respectful culture. Core elements of support include approval of adequate funding and regular review of reports.
	Privacy Officer	• Role is defined and is fundamental to business decision-making process. • Role and responsibilities for monitoring compliance are clearly identified and communicated throughout the public body. • Responsible for the development and implementation of the program controls and their ongoing assessment and revision. • Adequate resources are identified. • Public body, municipality or health custodian structure supports the ability of staff to monitor compliance and foster a culture of privacy within the public body. • Ensures privacy protection is built into every major function involving the use of personal information.
	Reporting	Reporting mechanisms should be established and they need to be reflected in the public body's program controls.
Program Controls	**Personal information inventory**	The public body, municipality or health custodian is able to identify: • The personal information in its custody or control, • Its authority for the collection, use and disclosure of personal information, and • The sensitivity of the personal information.
	Policies	• Privacy policy • How to request access or correction • Complaints policy
	Risk assessment tools	• Privacy impact assessments • System risk and threat assessments
	Training	• Privacy basics for all staff • Privacy breach training for all staff • Advanced and refresher training as required
	Breach management protocols	• Privacy breach policy • Breach notification assessment tool • Breach management protocol
	Service provider management	• Have standard clauses available to ensure service provider compliance with privacy law requirements& monitor compliance.
	Communication	• Inform individuals of their rights and the public body's policies.

[16] These materials are based on the paper, "Getting Accountability Right with a Privacy Management Program" prepared by the Office of the Information and Privacy Commissioner of Alberta, the Office of the Privacy Commissioner of Canada and the Office of the Information and Privacy Commissioner of British Columbia.

B. Ongoing Assessment and Revision		
Oversight & Review Plan	**Develop an oversight and review plan**	Privacy Officer should develop an oversight and review plan on an annual basis that sets out how she will monitor and assess the effectiveness of the public body's program controls.
Assess and Revise Program Controls	**Updates and revisions**	• Update personal information inventory • Revise policies • Treat risk assessment tools as evergreen • Modify training and education • Adapt breach and incident response protocols • Fine-tune service provider management

Tab 17

How to Build a Privacy Management Framework
Getting Started

Introduction:

This document was developed by the Office of the Information and Privacy Commissioner for Nova Scotia and is intended to assist smaller public bodies and municipalities with beginning to develop and implement a robust privacy management program. An overview of the elements of a robust privacy management program is contained in: "Privacy Management Program At a Glance" on the Office of the Information and Privacy Commissioner for Nova Scotia website at: https://oipc.novascotia.ca. This gap analysis document provides detailed information about some of the elements of a privacy management program. The goal of this gap analysis is to identify shortcomings in the program with a view to creating a foundation for a robust privacy management program. The gap analysis results should then be used to develop a privacy oversight and review plan that addresses each of the gaps identified.

Once you have completed this gap analysis and implemented all of the required changes you should review the full Privacy Management Program Gap Analysis for public bodies.

Contact Us:
If you have questions or comments with respect to this document please contact us at:
Office of the Information and Privacy Commissioner for Nova Scotia
PO Box 181, Halifax NS B3J 2M4
5670 Spring Garden Road, Suite 509
Halifax Phone: 902-424-4684 Toll Free: 1-866-243-1564

Instructions: This gap analysis tool begins with a Gap Analysis Summary document (page 128). When complete this will serve as a one page summary of the results of your review. Your goal is to develop a visual gap analysis by assigning red, yellow or green to the outcome of your assessment for each of the elements of your privacy management program.

Step 1: Begin by assessing the two categories of building blocks: organizational commitment and program controls. For each category we have provided a list of essential elements. Record your evaluation of each element by describing the current state of affairs in your university. Be as honest and critical as you can. The goal here is to accurately state your university's current status.

Step 2: For each requirement score your university's compliance on a scale of 1 to 3. Feel free to give partial points. Ratings are explained on page 128.

Step 3: Record the overall score then assign a colour to it and record the colour on the summary sheet at page 128. Colour ratings are explained on page 128.

Step 4: Once you have completed all of your ratings, review the summary sheet at page 128 and develop a plan to move all of your ratings to green (a privacy oversight and review plan).

Sample - Gap Analysis Summary	
PMP Requirement	**Overall Gap Analysis Rating**
Building Blocks – Organizational Commitment	
a. Buy-in from the Top	2.2
b. Privacy Officer	2.6
c. Privacy Office	1.3
d. Reporting	2.5
Building Blocks – Program Controls	
a. Personal Information Inventory	2.8
b. Policies	2.0
c. Risk Assessment Tools	2.0
d. Training and Education Requirements	1.6
e. Breach and Incident Management Protocols	2.4
f. Service Provider Management	2.4
g. External Communication	1.5
Oversight and Review Plan	
a. Develop Oversight and Review Plan	2.0

Gap Analysis Summary	
PMP Requirement	**Overall Gap Analysis Rating**
Building Blocks – Organizational Commitment	
a. Buy-in from the Top	
b. Privacy Officer	
c. Privacy Office	
d. Reporting	
Building Blocks – Program Controls	
a. Personal Information Inventory	
b. Policies	
c. Risk Assessment Tools	
d. Training and Education Requirements	
e. Breach and Incident Management Protocols	
f. Service Provider Management	
g. External Communication	
Oversight and Review Plan	
a. Develop Oversight and Review Plan	

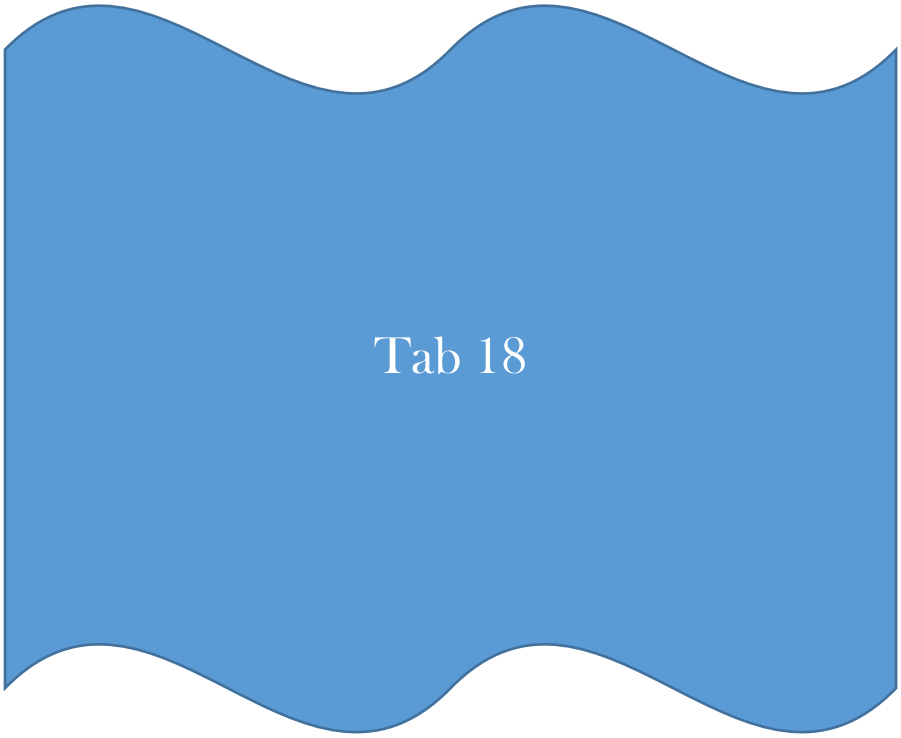
Gap Analysis Ratings & Colour Ratings for Summary Chart

Rating	Colour code	Rating Description
1.0 – 1.9	Red	Little to no evidence of compliance – documented or in practice.
2.0 – 2.5	Yellow	No documented evidence of compliance but some evidence of effective practice in compliance or documented practice requirement with only limited evidence of implementation.
2.6 – 3.0	Green	Documented and substantial practical compliance.

Building Blocks – Organizational Commitment		
List of Expectations	**Evidence of Compliance**	**Gap Rating**
a. Buy-in from the Top	**Overall Rating**	
• Senior management endorses the program controls (policies, risk assessments, training) and provides necessary resources.		
b. Privacy Officer	**Overall Rating**	
• A senior manager is assigned responsibility for overseeing the university's compliance.		
c. Privacy Office	**Overall Rating**	
• Role of the privacy office is defined and staff foster culture of privacy within the organization.		
• Staff work to ensure that privacy protection is built into every major function involving the use of personal information.		
d. Reporting	**Overall Rating**	
• There are privacy reporting mechanisms that ensure that the right people know how the privacy management program is structured and whether it is functioning as expected.		
• The reporting program has documented reporting structures.		
Building Blocks – Program Controls		
a. Personal Information Inventory	**Overall Rating**	
• The organization has completed a personal information inventory or equivalent.		
b. Policies	**Overall Rating**	
Organizations must have in place four key policies: (i) how to access and correct personal information, (ii) retention and disposal of personal information, (iii) responsible use of information and information technology, (iv) privacy breach management policy.		

Building Blocks – Program Controls cont'd		
List of Expectations	**Evidence of Compliance**	**Gap Rating**
c. Risk Assessment Tools	**Overall Rating**	
• Privacy risk assessments are required throughout for all new projects involving personal information and on any new collection use or disclosure of personal information.		
d. Training and Education Requirements	**Overall Rating**	
• All employees require general privacy protection training.		
• Privacy training is mandatory for all new employees.		
• Individuals who handle personal information directly receive additional training specifically tailored to their roles.		
• Training and education are recurrent and the content of the program is periodically revisited and updated to reflect changes.		
e. Breach and Incident Management Response Protocols	**Overall Rating**	
• There is a procedure for the management of personal information breaches.		
• There is a person responsible for managing a breach.		
f. Service Provider Management	**Overall Rating**	
• Contractual or other means are in place to protect personal information.		
• Transborder data flows and requirements of the foreign regime are addressed in service provider arrangements.		
g. External Communication	**Overall Rating**	
• Individuals are aware of how to access & correct their personal information.		
• Individuals are aware of how to complain including the right to submit a complaint to the Privacy Commissioner.		

Oversight and Review Plan		
List of Expectations	**Evidence of Compliance**	**Gap Rating**
h. Develop Oversight and Review Plan	**Overall Rating**	
• The Privacy Officer develops an oversight and review plan on an annual basis that sets out how the privacy management program's effectiveness will be monitored and assessed.		
• The plan establishes performance measures.		
• The plan includes a schedule of when all policies and other program controls will be reviewed.		


Tab 18

Office of the Information and Privacy Commissioner for Nova Scotia

Guidance for the Use of Criminal Record Checks By Universities and Colleges

This guidance document was prepared by the Office of the Information and Privacy Commissioner for Nova Scotia. It is intended to assist universities and colleges in deciding whether or not the organization has the authority under Nova Scotia's privacy legislation to collect, use, and disclose criminal record checks from students and potential students. It also makes 17 best practice recommendations for how to implement a criminal record check program.

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 the *Freedom of Information and Protection of Privacy Act*, 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 it complies with its responsibilities under the legislation. Visit us at: https://oipc.novascotia.ca.

Background

It came to the attention of the Information and Privacy Commissioner[17] that many colleges and universities ("schools") in Nova Scotia have made it a practice to collect criminal record checks from students, and potential students, for some of their program areas. This information is then used by the schools to make decisions about student placements for program practicums and in some cases whether or not the student will be admitted to the program at all.

One of the purposes of the *Freedom of Information and Protection of Privacy Act (FOIPOP)* is to ensure that public bodies are fully accountable to the public by preventing the unauthorized collection, use or disclosure of personal information. Criminal record checks, by their nature, contain very sensitive personal information.

The following provides the rules and 17 best practice suggestions that schools should consider when deciding whether to collect, use or disclose criminal record checks as part of their admittance and placement processes.

COLLECTION

Collection Rules

Schools have identified that the authority they rely on, for the collection of personal information through criminal record checks, is that the information relates directly to and is necessary for an operating program or activity of the school.[18] Schools with programs that require a student practicum placement state that some employers (placement partners) require that any student placed with them for work experience must have completed a criminal record check. Where the practicum placement is a requirement for graduation, schools take the position that the criminal record check is therefore necessary for the school program – they must ensure students will be eligible for placement so they can complete the program.

Collection occurs when a school gathers, acquires, receives or obtains personal information. There is no restriction on how the information is collected, which can mean obtaining a physical copy or simply viewing it.

Schools must establish on a program-by-program basis whether or not they have the authority under *FOIPOP* to collect personal information regarding the criminal history of individuals. *FOIPOP* states that personal information may be collected if it "relates directly to and is necessary for an operating program or activity". Therefore, in order to have authority to collect the personal information, the school must establish three things:

1. To "relate directly to", the information must have a <u>direct</u> bearing on the operating program or activity of the college or university.
2. To be "necessary for" means that without the information the program (part of the school's mandate) or activity (steps to carry out the mandate) would not be viable.

---

[17] The Information and Privacy Commissioner for Nova Scotia is also known as the Review Officer and is appointed as the independent oversight authority under the *Freedom of Information and Protection of Privacy Act*, the *Municipal Government Act*, the *Personal Health Information Act*, and the *Privacy Review Officer Act*. It is the role of the Commissioner to monitor how the privacy provisions are administered, by conducting investigations into compliance, undertaking research and informing the public.

[18] This is a purpose authorized by s. 24(1)(c) of *FOIPOP*. *FOIPOP* authorizes two other purposes – if an Act expressly authorizes it (s. 24(1)(c)) or if it is for law enforcement purposes (s. 24(1)(b)).

3. The collection must relate to an operating program or activity of the college or university, not to another organization (i.e. a placement partner).

A school that determines it does not have authority to collect must stop collecting the information. All criminal record checks that were collected previously should be destroyed in accordance with the school's records retention schedule and in accordance with *FOIPOP*.[19]

If a school establishes that it does have authority to collect personal information through criminal record checks, best practice is to then consider if it should proceed with collection and if so, to what extent. The following 17 best practices will help to guide colleges and universities in establishing a *FOIPOP* compliant program.

Collection Best Practices

Minimize. Schools should be careful to only collect the minimum amount of personal information that is necessary for the intended program or activity. This can be accomplished in two ways:

1. Conduct the least invasive form of check required: If only a criminal record check is required, ensure other forms of checks are not also conducted – such as a vulnerable sector check or a child abuse registry check.

2. Don't make copies: Schools only need to check if the criminal record check is "clean" or not. If the criminal record check is clean, it does not need to be kept at all. Schools should have a way to note on collection day that the criminal record check was viewed and was clean - a copy should not be retained.

   In cases where the record is not clean, an appointment should be set up with an advisor to discuss the student's options (see more below in "Use Best Practices").

Formalize. It is important to document the reasons for the collection of personal information. Best practices include:

3. Document placement partner requirements: If the primary reason for the criminal record check is because placement partners will only accept students who meet the organization's human resources requirements (a clean record or acceptable convictions only), formalize the expectation of each of the placement partners in writing. Documentation must include a list of relevant offences for each placement type to aid the school in deciding whether or not a student is eligible for placement.

4. Update expectations: The school should periodically confirm with each placement partner that their expectations remain the same and update the documentation as needed.

5. Develop employee guidance: Schools should develop appropriate written policies and procedures to guide their employees who are responsible for collecting and assessing the relevance of criminal record checks, and to ensure compliance with the privacy provisions of *FOIPOP*.

[19] Section 24(4) of *FOIPOP* states that when a public body uses personal information to make a decision that directly affects the individual, the public body must retain the information for at least one year.

Notify. Whether or not a copy of the criminal record check is retained, a collection is occurring. Schools should have a notice of purpose available to students.

6. Notify and obtain consent from students: Provide a clear notification to students and applicants of the reason for the collection of criminal record check information. The notice should explain the purpose, nature and extent of collection of their personal information and should seek student consent for any intended uses or disclosures of the information.

USE

Use Rules

Schools have identified that the authority they rely on for using criminal record checks is that it is for the same purpose it was collected for - to assess the student's ability to be accepted into a practicum placement and program admittance.[20] However, as noted above, best practice is to obtain consent from students for the use of their personal information.

Accessing (looking at) personal information is a use. Schools should be careful to only use personal information for authorized purposes and should limit access to only those that require the information to do their jobs.

Use Best Practices

Formalize. It is important to document the reasons for the use of personal information. Best practice includes:

7. Develop tools: Create a conviction relevance matrix. For each program area list the relevant convictions based on the information supplied by employers.

Centralize. Centralize the decision making about a student's ability to be placed with a placement partner or accepted into a program based on his or her criminal history. This practice will achieve the following privacy supportive practices:

8. Develop expertise: Centralizing decision making will allow the person making decisions to develop expertise (including the development of a conviction relevance matrix).

9. Limit access: Only those who are making the decisions will have access to the sensitive information. In cases where the criminal record check is not clean, the student/potential student would book an appointment with the central criminal record check contact for further investigation. If that person cannot make a decision based on his or her understanding of the conviction relevance matrix, then a call can be made to the placement partner to discuss what it thinks in the form of a hypothetical question. If the placement partner is willing to accept the student, the process would move on. If not, the school would follow its screening process.

[20] This is a purpose authorized by s. 26(a) of *FOIPOP*. *FOIPOP* authorizes two other purposes – with consent (s. 26(b)) or if *FOIPOP* authorized another public body to disclose the information to the school (s. 26(c)).

DISCLOSURE

Disclosure Rules

FOIPOP provides for the disclosure of personal information with consent of the affected individual or in limited circumstances without consent. Disclosure includes the sharing of personal information with a placement partner. The school practices may vary in what is disclosed to placement partners about the criminal record checks.

Disclosure Best Practices

Don't disclose. Disclosure, even if authorized, is discretionary. Schools should consider the following when deciding if disclosure is appropriate:

10. Passage of time: Given placement generally happens well into the student's training, a criminal record check that was provided to the school prior to or just after beginning the program will be out of date (normally they are valid for six months). A lot can happen in a student's life during that time, so the criminal record check may no longer be accurate and therefore would not serve the purpose it is intended for.

11. Shift responsibility: The placement partner could make its own request to the student directly, identifying its own authority for collection and keeping in mind that it is no longer for the school's purposes, it is the placement partner's purposes. In this case, there would be no need for the school to collect any criminal record information.

Get consent. If disclosing the actual criminal record check to placement partners, ensure that consent is received from the student at the time of the disclosure. Keep in mind:

12. Informed consent: Having a student sign a blanket consent form at the beginning of the program will not generally be adequate. The consent to disclosure should be signed at or near the time of disclosure and should identify both the information to be disclosed and the organization to which the school is authorized to disclose the information.

Minimize. Schools should be careful to only disclose the minimum amount of personal information that is necessary for the intended purpose. This can be accomplished by:

13. Don't provide copies: Schools can simply confirm that the record is clean. Presumably any student who has not passed the internal school criminal record review process will not be offered as a placement student so there will generally be no need to disclose any negative criminal record information outside of the school.

SECURITY

Security Rules

FOIPOP requires[21] schools to have adequate security arrangements (administrative, physical, technical and personnel) in place to protect privacy.

Security Best Practices

Mitigate risk. Schools should understand what the privacy implications are when collecting, using and disclosing, storing and disposing of personal information. This can be achieved by developing a privacy management framework[22] that includes the following best practices:

14. Conduct an assessment: Prepare a privacy impact assessment ("PIA") to assess and mitigate privacy implications before beginning to collect, use or disclose criminal record check information.[23]

15. Limit access: Criminal record checks should be placed in locked cabinets, accessible to only people that are required to use the criminal record check as a function of their jobs.

16. Develop policy: Without written policies and procedures in place, schools have not taken responsible steps to safeguard personal information in their custody and control. Written policies and procedures will guide employees, who are responsible for programs that involve placements, to ensure compliance with the privacy provisions under *FOIPOP.*[24]

17. Records Management: Do not keep criminal record checks longer than necessary. Schools should develop a retention schedule and ensure it is followed. Keeping records longer than needed increases the risks associated with storing personal information (such as breaches).

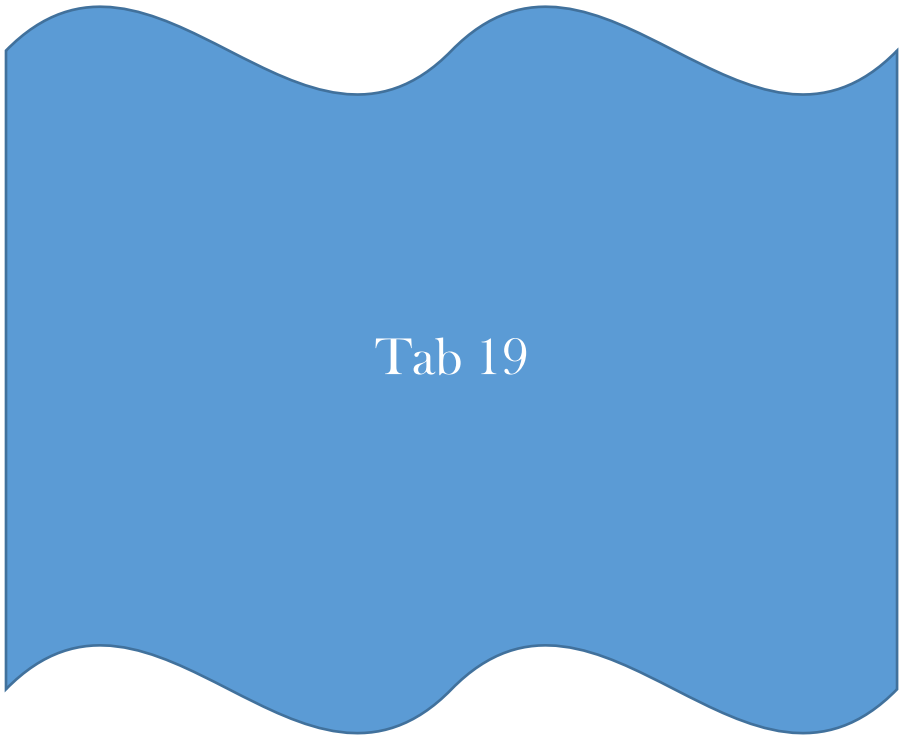
---

[21] S. 24(3) of *FOIPOP*. See the OIPC website for the Security Checklist which provides some preliminary guidance on what practices meet the minimum security requirements under *FOIPOP* Reasonable Security Checklist for Personal Information.

[22] For more details on how to implement a complete privacy management framework see the OIPC website for Privacy Management Program at a Glance and Privacy Management Program: Getting Started, both available at: https://oipc.novascotia.ca.

[23] See the OIPC website for a PIA template for public bodies at: PIA Template.

[24] Essential *FOIPOP* policies include a privacy policy (describing collection, use & disclosure practices), breach management policy, records management policy and security policy. For more details on essential privacy policies review the privacy management program materials on the OIPC website.


Tab 19

Resources

Table of Concordance Between *MGA Part XX* and *FOIPOP*

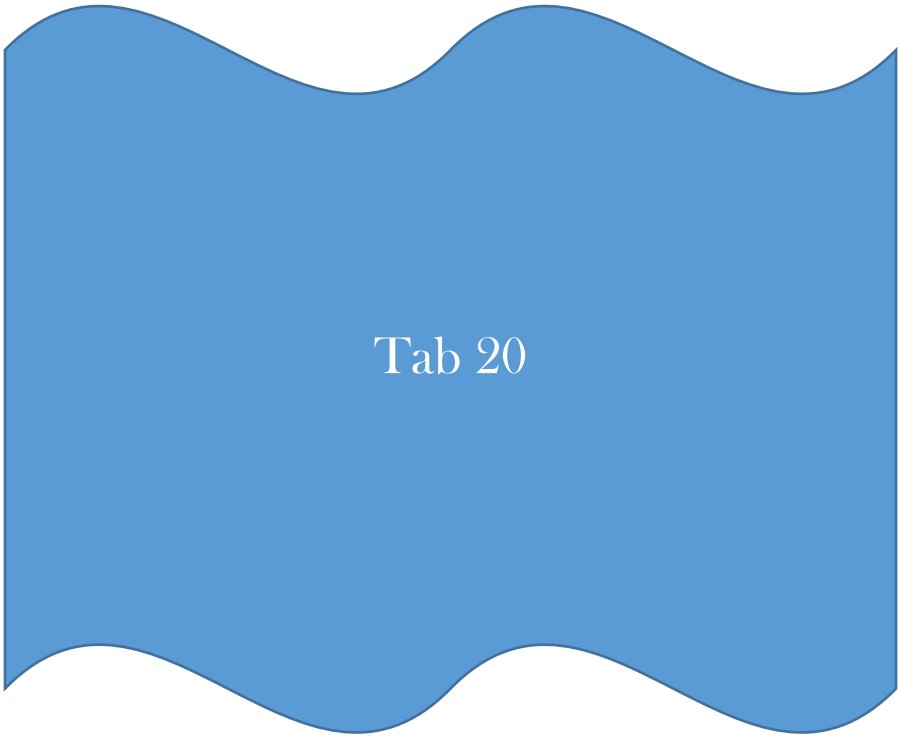
Access to Information Rules		
Discretionary Exemptions		
FOIPOP	**MGA**	**Exemption**
12	472	Intergovernmental Affairs
13	473	Deliberations of Executive Council/Council
14	474	Advice to public body or minister/Council or municipal body
15	475	Law enforcement
16	476	Solicitor client privilege
17	477	Financial or economic interests
18	478	Health & Safety
19	479	Conservation
19A		Local public body - Closed meetings
19B		Local public body - Academic research
19C		University - Certain personal information
19D		Local public body – hospital records
19E	479A	Labour conciliation records/Conciliation Board
Mandatory Exemptions		
20	480	Personal information
21	481	Confidential information

Request Processing Essentials		
FOIPOP	**MGA**	
4	463	Records
6	466	Applicant obligations
7(1)	467(1)	Public body/municipal duty
5(2)	465(2)	Duty to sever
7(2)	467(2)	Time
11	471	Fees
7(2)	467(2)	Response content
22	482	Third Party Notices

Privacy Rules		
FOIPOP	**MGA**	
24	483	Collection
24(2)	483(2)	Accuracy
24(3)	483(3)	Security
24(4)	483(4)	Retention
25	484	Correction
26	485(1)	Use
27	485(2)	Disclosure

Websites

Resource	Website
Office of the Information and Privacy Commissioner for Nova Scotia: ➢ Tools & Guidance ➢ Legislation ➢ Decisions on interpretation of *MGA*	https://oipc.novascotia.ca
Department of Internal Services – Information Access & Privacy Program ➢ Forms ➢ Legislation ➢ FAQs	http://novascotia.ca/just/IAP/
Other Information & Privacy Commissioners ➢ Other Canadian jurisdictions produce orders relating to provisions similar to those found in the *MGA* ➢ The Information Commissioner of Canada has produced an extensive manual explaining her interpretation of the federal *Access to Information Act*: The Investigator's Guide to Interpreting the ATIA.	British Columbia https://www.oipc.bc.ca/ Alberta http://www.oipc.ab.ca/pages/home/default.aspx Ontario https://www.ipc.on.ca/english/Home-Page/ Information Commissioner of Canada http://www.oic-ci.gc.ca/eng/inv_inv-gui-ati_gui-inv-ati.aspx
Cases and Laws ➢ Free online search engine for court cases, Commissioner decisions and laws in Canada	CanLii https://www.canlii.org/en/
Policy Manuals ➢ Governments in other provinces produce policy manuals explaining sections of their access and privacy legislation. Always check to see if the provisions match the *MGA* but these manuals may provide some guidance for processing requests and managing privacy issues.	Treasury Board of Canada https://www.tbs-sct.gc.ca/atip-aiprp/tools/administration-application-eng.asp Alberta Government http://www.servicealberta.ca/foip/resources/guidelines-and-practices.cfm British Columbia Government http://www.cio.gov.bc.ca/cio/priv_leg/manual/index.page
PIIDPA Annual Reports	http://novascotia.ca/just/IAP/


Tab 20

Training for Staff

Access & Privacy Basics for Staff

See the Powerpoint slides provided separately. The slides include note pages to guide the presenter through this 30 minute presentation intended to provide university staff with some very basic information about the access and privacy rules in the *Freedom of Information and Protection of Privacy Act*. The notes include text in red. This text needs to be modified – usually it is a place to input a name – such as the name of the Chief Privacy Officer or *FOIPOP* contact.

As part of the presentation, staff are asked to complete the *5-Minute Privacy Checkup* (mentioned on slide 14) which is also provided on the next four pages.

Office of the Information and Privacy Commissioner for Nova Scotia

5 Minute
Privacy Checkup

As an employee of a public body, municipality or health custodian, you should be aware of your responsibilities to keep personal & sensitive information secure. Current privacy standards require that public bodies, municipalities and health custodians protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

This 5-minute privacy checkup asks a series of questions relating to the security of personal information and sensitive business information both hard copy and electronic. A "no" answer to any of these questions is a warning sign that the information may not be secure.

Physical Security		
	Y	N
Do you have files containing sensitive information stored in your office? • If yes, is the sensitive information stored in a locked filing cabinet? • Do you lock your office door whenever you leave the office?		
At the end of the day do you always: • Clear your desktop of all files containing sensitive information? • Store your laptop and all files in a locked filing cabinet? • Lock your office door? • Log off your computer? • Remove all documents containing sensitive information from faxes and printers?		
Email & Faxing		
Before emailing sensitive information do you: • Ensure that either the owner of the sensitive information has consented to transmission via email or that the information is encrypted? • Always attach a confidentiality notice?		
Before faxing any sensitive information do you: • Only send from a secure fax machine? • Prior to sending, call the receiver to confirm that the receiving fax machine is secure and to confirm the fax number? • Always use a cover sheet that includes both the sender's name and phone number and the intended recipient's name and phone number? • Always attach a confidentiality notice?		

Security of Electronic Files		
	Y	N
Do you always have to login to any system using a unique identifier and password?		
Is your password complex (numbers, symbols, letters etc) and at least 12 characters?		
Have you changed your password in the last 90 days?		
Do you store all electronic files containing sensitive information on a secure central server? (i.e. no sensitive information stored on local hard drive)		
Is your office computer screen positioned so that no unauthorized individuals can view sensitive information displayed?		
Is your screen saver set to automatically log out after 5 minutes of inactivity?		
Training & Knowledge		
In the last 12 months, have you completed training on privacy and security of sensitive information?		
Do you know whether or not you have authority to collect, use or disclose personal information?		
If you do have authority to collect, use or disclose personal information, do you know the limits and conditions of that authority?		
Mobile & Portable Devices		
Do you always store mobile or portable storage device such as laptops in a locked cabinet when not in use?		
Is all sensitive information contained on your portable storage devices limited to the absolute minimum necessary?		
Have you ensured that all sensitive information contained on any portable storage device you use is encrypted?		
Do you permanently delete sensitive information from your portable storage devices as soon as possible after use?		
Secure Disposal of Sensitive Information		
Do you dispose of hard copy records containing sensitive information by placing them in a secure shredding bin or by shredding them yourself?		
Privacy Habits		
Do you avoid discussing personal information in any area where the conversation can be overheard by unauthorized personnel?		
Do you disclose personal information to co-workers only where the information is necessary for the performance of the duties of your co-workers?		
If you must travel with personal information, do you always ensure that any personal information you have is stored in a locked cabinet or cupboard and never in your car?		

Please see our Reasonable Security Checklist, for more detailed information:
https://oipc.novascotia.ca/node/428#overlay-context=PHIA_Custodians

We encourage you to contact us if you have any questions about privacy and security in Nova Scotia.

Phone: 902-424-4684
Toll Free (NS): 1-866-243-1564
TDD/TTY: 1-800-855-0511
Fax: 902-424-8303
Email: oipcns@novascotia.ca

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