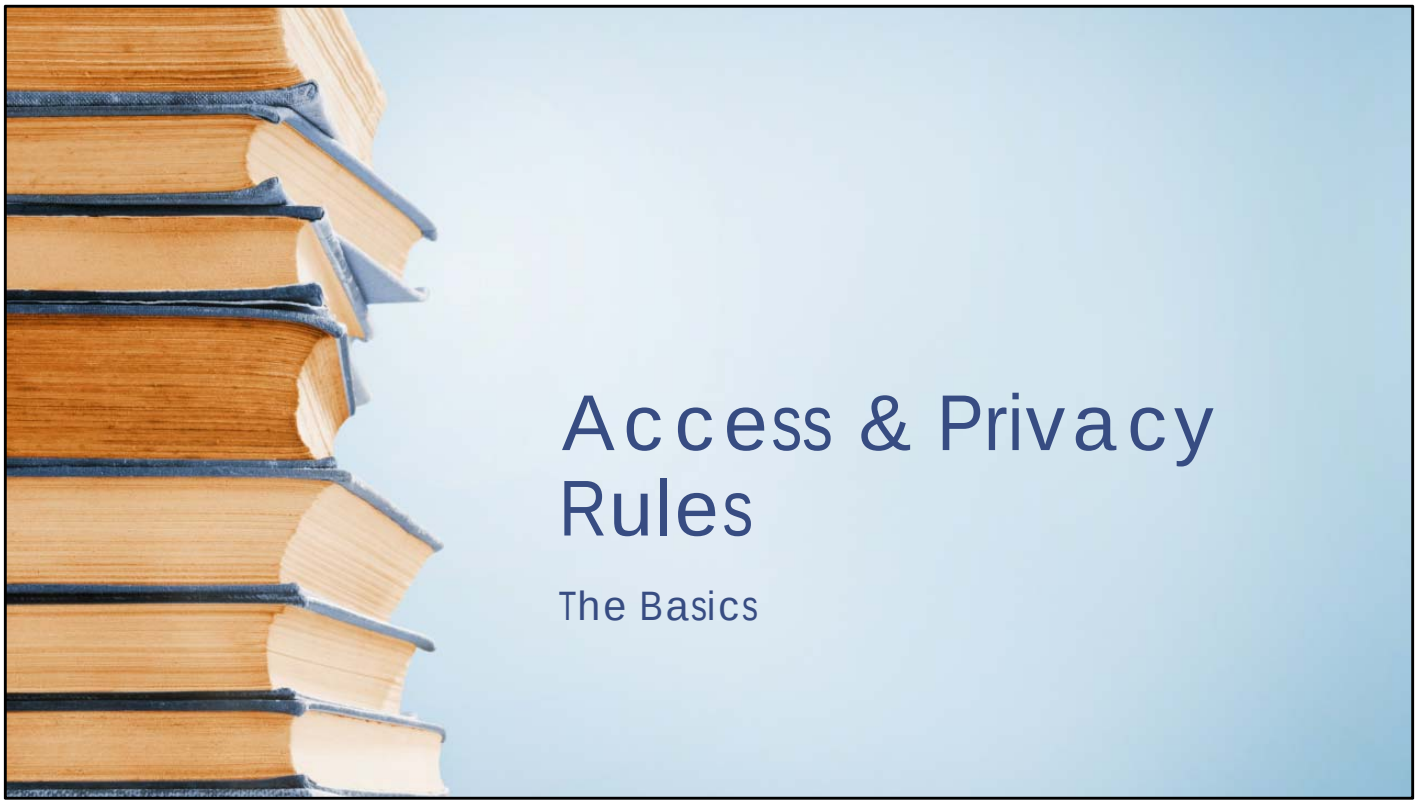


Note to presenter-
The following pages include speaking notes. Text in **red** indicates a recommendation to insert a name or other text before using this presentation.

This deck was prepared by the Office of the Information and Privacy Commissioner for Nova Scotia. All images are used with permission for the sole purpose of illustrating this presentation.

Access & Privacy Basics

In this course you will learn:

1. When access & privacy rules apply;
2. What the basic access & privacy rules are;
3. How to properly protect personal information; and
4. What to do if you think a privacy breach has occurred.

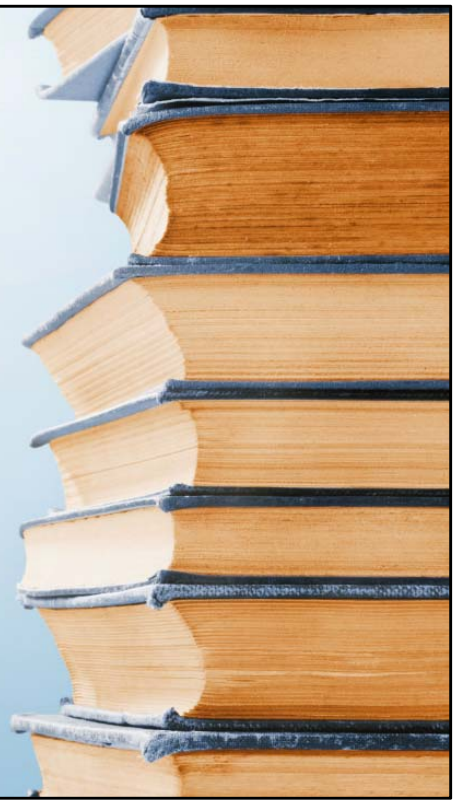
This 30 minute presentation is intended to provide staff with some very basic information about access and privacy law in Nova Scotia.

You will learn some of the basic rules and what your obligations as a staff member are.

If you have questions or concerns you should speak to {**insert contact name here**}, the access coordinator or privacy officer for {**insert your organization's name here**}.

We are subject to the access and privacy rules in the **{choose either *Freedom of Information and Protection of Privacy Act or Municipal Government Act}*** – we will refer to this as the Act.

1. When do access & privacy rules apply?



When do access rules apply?

- All records are “foi-able”
- “records” include emails, texts, pins, photographs

Records are defined in the Act to include anything on which information is recorded.

All records in the custody or under the control of **{insert organization’s name here}** are subject to the Act.

If an employee does work on a personal device, or uses their personal email account for work, that record must be produced in response to an access to information request.

For a further discussion see: *Instant Messaging & Personal Email Accounts: Meeting Your Access & Privacy Obligations* available on the OIPC website at https://oipc.novascotia.ca/sites/default/files/publications/Instant%20Messaging%20Guide%202019%2012%2004.pdf

When do privacy rules apply?

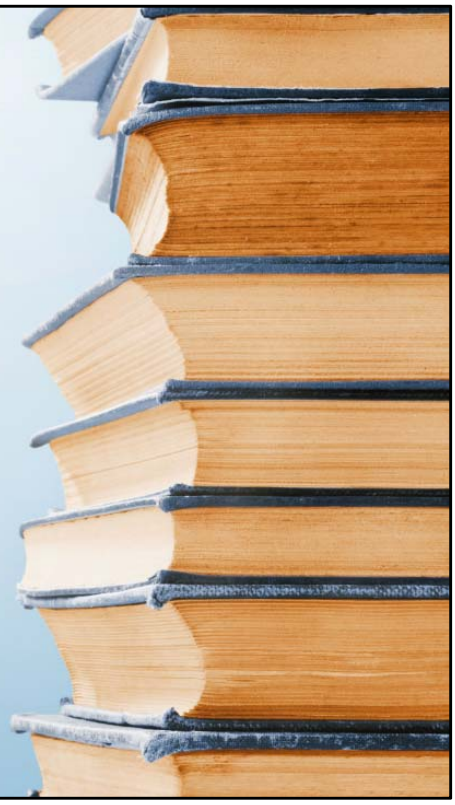
- Privacy rules apply to all collection, use & disclosure of personal information

- Privacy rules apply to all personal information collected, used or disclosed by **{insert organization's name here}**

- "personal information" means recorded information about an identifiable individual such as:
  - Name, address
  - Race, religious or political beliefs
  - Identifying number
  - Fingerprints, blood type
  - Health care history
  - Educational, employment or criminal history

- Our largest personal information collections include employee information and citizen information.

2. Basic access & privacy rules



What are the basic access to information rules?

- Anyone can apply
- $5 fee for general information
- $0 for personal information
- 30 days to respond

- If you receive an access to information request, immediately forward it to **{insert name here}** the access coordinator.
- The 30 day timeline begins the moment the request is received anywhere in **{insert organization name here}**.
- In addition to the application fee for general information, we may charge processing fees – for requests that take more than 2 hours.

What are the basic access to information rules?

- Full disclosure unless exemption applies
- 15 limited & specific exemptions
- Duty to sever
- Access coordinator processes the request

- Basic rule in FOIPOP is that the whole record must be disclosed unless limited & specific exemptions set out in the Act apply.

- 15 exemptions under the Act including:
  - Personal privacy
  - Harm to third party business
  - Solicitor-client privilege
  - Policy advice or recommendations

- Can only withhold the information to which the exemption applies – so must sever (remove) just the limited information to which the exemption applies and disclose the rest.

Duty to Assist

- Every reasonable effort to assist
  - Respond without delay
  - Openly
  - Accurately
  - Completely

When we respond to an access to information request we have a “duty to assist” the applicant.

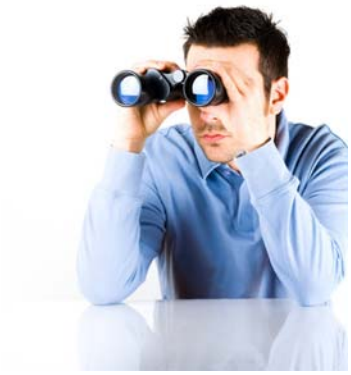
The law says we must make every reasonable effort to assist the applicant by:

- Responding without delay
- Openly
- Accurately
- Completely

-respond promptly
-help applicants identify responsive records
-tell applicants about everything that is available
-give applicants a complete response

Access rules for staff

- Keep good records, always file centrally
- Follow records retention schedules
- Respond promptly and thoroughly to any search request



- Keep complete records of decisions, actions and deliberations.
- No matter where you originally recorded the information (text, email, etc.) always file the record centrally in our filing system.
- Follow approved records retention schedules.
- If you're asked to produce records responsive to an access to information request remember:
  - Be thorough
  - Be accurate
  - Be complete
  - Be timely

What are the basic privacy rules?

- No collection unless authorized
- No use unless authorized
- No disclosure unless authorized
- Keep personal information secure

- A public body cannot collect, use or disclose personal information unless specifically authorized under Nova Scotia's privacy laws.

- For example, personal information may only be collected in three circumstances:
    - When expressly authorized by law
    - For law enforcement
    - Because its directly related to and necessary for an operating program or activity

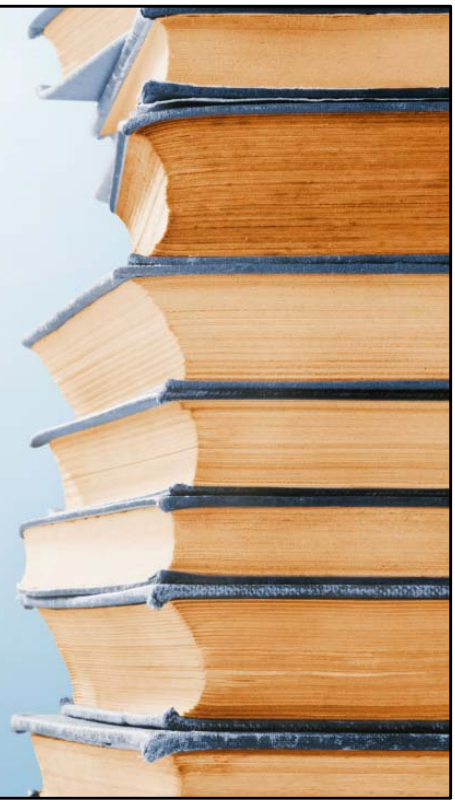
- We must make reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal of personal information.

Privacy rules for staff

- Know the privacy rules that apply to your work
- Use privacy impact assessments
- Keep personal information secure

- If your work involves the use of personal information be sure you know exactly what information you are authorized to collect, use and disclose.
- If you are planning a new project, program or system that will involve personal information, conduct a privacy impact assessment (PIA) to identify and mitigate your privacy risks.
- PIA templates are available at on the OIPC website: https://oipc.novascotia.ca/ .
- You must keep personal information secure.

3. How to Protect Personal Information



The law requires that we protect personal information by making “reasonable security arrangements” against such risks as unauthorized access, collection, use, disclosure or disposal.

Are you keeping personal information reasonably secure?

Note to presenter: Hand out the 5 Minute Privacy Check Up

Take a few minutes to complete the 5 minute privacy check up. Think only about personal information you have – on your computer, in your office or in your work area. Think about your personal privacy practices as you answer this quiz.

Any "no" answer is a red flag – think about how you can get your answer to "yes".

How to Protect Personal Information

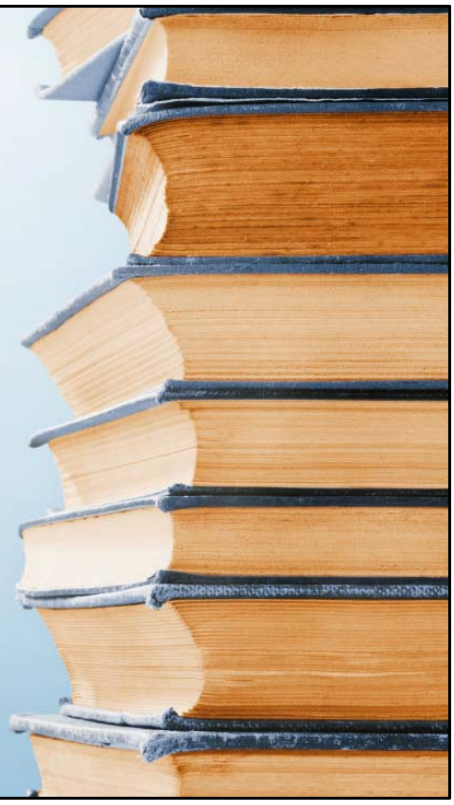
- Physical security
- Technical security
- Administrative security

Physical security
Locks, security systems, pass cards.

Technical security
Unique passwords, unique user names, encryption.
Only use devices controlled by **{insert organization name here}** or only devices with security equivalent or superior to **{insert organization name here}**'s systems.

Administrative security
End of day procedures – clear desk, lock all cabinets, clear all photocopiers, log out of all systems.
Travel procedures – no unencrypted personal information, take minimum necessary, remove all personal information from devices upon return.

4. Privacy Breaches



What is a privacy breach?

1. Must involve personal information

2. Must be an unauthorized activity
   - -collection
   - -use
   - -access
   - -disclosure
   - -destruction

To know if a privacy breach has occurred ask three questions:

1. Was any personal information involved?

2. Was the personal information collected, used, disclosed, accessed, or disposed of?

3. Was the activity authorized under Nova Scotia's privacy law?

Examples of privacy breaches

- Stolen laptop or portable storage device with personal information stored on it
- Mis-sent fax or email
- System hack
- Insecure disposal of personal information (e.g. competition files in non-secure garbage)
- Unauthorized viewing of database records (e.g. looking up your co-worker's birthday)

Consider the situations listed on this slide. Are any of these situations a privacy breach? How do you know?

All of the situations are potential privacy breaches. Every situation appears to be an unauthorized loss of information – either through error or theft.

In the fax, email and systems hack situations you must establish if any personal information was at risk (highly likely). All of the other situations make clear personal information was at risk.

Harder to spot breaches

1. Your daughter sat in your office while you completed a few performance evaluations

2. You left out those performance files over night so you can get back to work in the morning

3. You post work party pictures on Facebook

1. If your daughter could see your computer screen this is an unauthorized disclosure
- If your daughter could overhear any discussion you had about the performance evaluations, this is also an unauthorized disclosure
- Best practice: have her wait in the waiting room

2. Personal information sitting on a desk is not reasonably secure, particularly if you do not lock your office door.
- personal information on a desk even in a locked office is not secure if cleaning staff access your office after hours

3. Posting of pictures is a disclosure. You need consent to do so. Further, if you've capture images of visitors/citizens, files or screen shots, you will not have

consent for this disclosure.

What to do if a privacy breach occurs

Step 1 – Contain the breach

Step 2 – Call the Chief Privacy Officer

Step 3 – Assist in the investigation as requested

{Note to presenter – if you've adopted a privacy breach protocol, adapt this slide to reflect this and hand out the protocol}

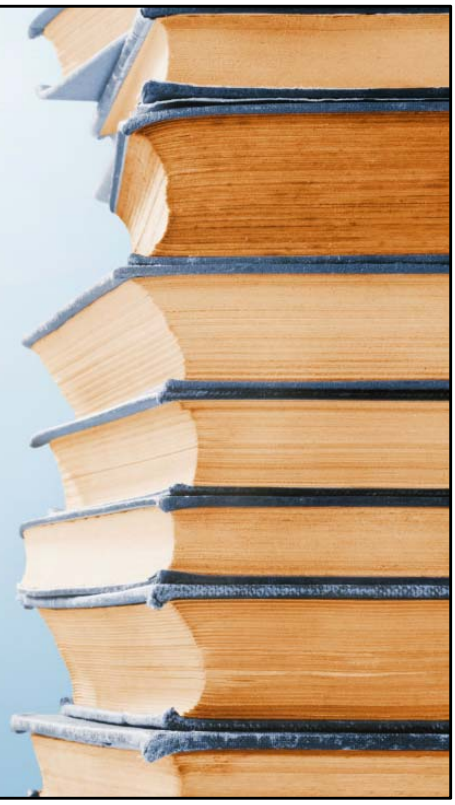
Step 1 – Immediately take steps to contain the breach. For example, attempt to retrieve lost or stolen documents (e.g. if a device is stolen, immediately change passwords, send remote kill if possible).

Step 2 – Call **{insert Chief Privacy Officer's name here}–** this is the person responsible for managing privacy breaches in our organization – if you don't know who to call, immediately call your manager.

Step 3 – Assist with the investigation as requested.

For more information see *Key Steps to Responding to Privacy Breaches* on the OIPC website https://oipc.novascotia.ca/ .

Questions?



Insert organization's access coordinator contact information:

Insert organization's chief privacy officer contact information: