Newfoundland Labrador

IM@WORK:

Making Information Management Work for You

IM Division Services, Office of the Chief Information Officer

Welcome to *IM @ Work: Making Information Management Work for You*

Newfoundland Labrador

This IM@Work Course will provide an overview of Information Management and its importance in your day-to-day work.

Course Objectives

At the end of this course you will be able to:

- Demonstrate knowledge of Information Management and why it is important
- Identify Information Management best practices
- Recognize the roles and responsibilities of those involved in the management and protection of information

Course Outline

SECTION 1: Introduction to Information Management (IM)
SECTION 2: Best Practices for Managing Information
SECTION 3: Information Management Roles and Responsibilities

Section One

Section 1 will:

- Define Information Management and why it is important
- Identify the legislation governing Information Management
- Show the types of records related to Information Management

Importance of IM

Imagine applying for a program or service for your family and submitting the application. What concerns might you have when submitting the application?

- *"How long will the process take?"*
- *"Who will access my family's information?"*
- *"How is my personal information secured?"*

The practice of Information Management ensures that information is managed and protected.

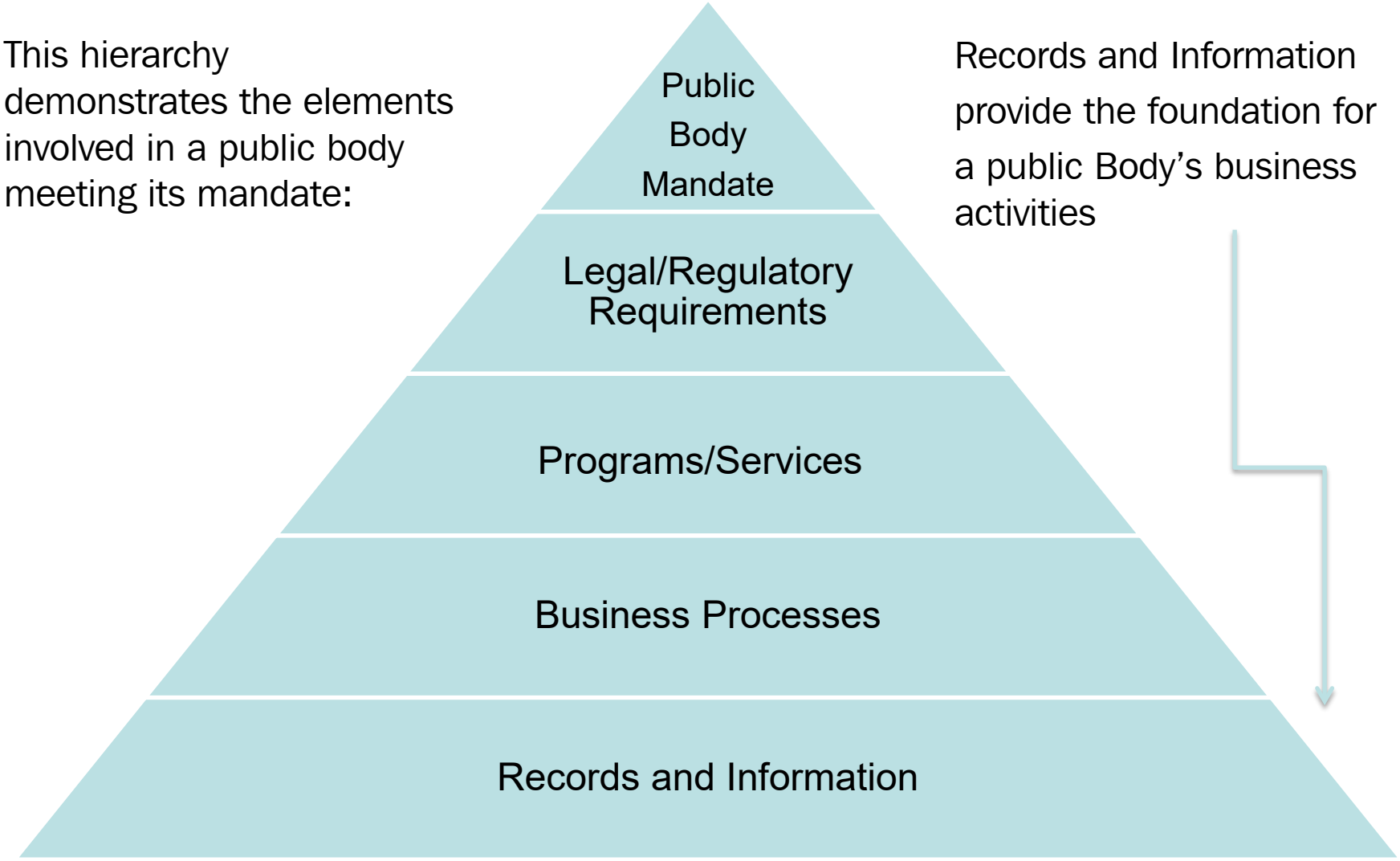
What is Information Management?

Information Management (IM), also known as records management, refers to the day-to-day actions taken when handling information. This includes:

- How to collect, create or receive information
- How to organize and store information
- How to appropriately share and use the information
- How to dispose of information when a public body no longer needs to retain it

Why Information Management?

This hierarchy demonstrates the elements involved in a public body meeting its mandate:



Records and Information provide the foundation for a public Body's business activities

IM Legislation

The legal foundation for information management within the Government of Newfoundland and Labrador is the *Management of Information Act*. This act was proclaimed in 2005, and provides the legal framework for the management of information in all public provincial bodies, including departments and central agencies.

The *MOIA* applies to everyone.

- Listing of Public Bodies as defined by the Act

Some of the important IM elements defined in the legislation are as follows:

- Authorization for the removal and destruction of records
- What is meant by a record?
- Organizational and employee accountability for IM

The violation of the Management of Information Act can result in a maximum fine of $50,000 and in default of payment, maximum jail time of 18 months.

Other Legislation

There is other legislation that impacts public bodies, as well as their information management programs and practices, as follows:

- The **Personal Health Information Act (PHIA)**, administered by the Department of Health and Community Services, contains the specific legislative requirements which are relevant for managing personal health information.
- The **Access to Information and Protection of Privacy Act (ATIPPA)** provides the rules for the protection of personal and confidential information and the guidelines for accessing information held by provincial public bodies in Newfoundland and Labrador.
- The **Rooms Act** mandates that The Rooms Provincial Archives division preserve those records which are deemed to have enduring legal, fiscal, evidential or research value.
- Some public bodies have specific legislation directly related to their mandate, or lines of business, that requires them to manage information accordingly.

What Information Needs to be Managed?

Newfoundland Labrador

ALL records, regardless of media type need to be managed:

- Electronic records used in databases and other business applications
- Records stored in offsite storage locations
- Physical/Paper records stored onsite at workstations, file rooms, etc
- Office records including Adobe PDFs
- Microsoft Word documents, PowerPoint presentations, and Excel spreadsheets
- E-mail messages sent and received by employees

It is important to understand the various information formats that exist in order to understand what the final or official version is, and what is considered a copy.




What is a Record?

A Government record is a record created by or received by a public body in the conduct of its affairs and includes a Cabinet record, transitory record and an abandoned record. Examples of records include:

- Client or case files
- Forms and applications
- Invoices
- Planning records
- Management records
- Policy development
- Cabinet records
- Transitory records

- Research records and data
- Audit logs
- Activity tracking records
- Abandoned records
- Transaction records
- Correspondence or communications on a service, or advice provided

Cabinet Records have special requirements. Follow up with your manager or IM Division if you work with Cabinet Records.

What is a Transitory Record?

A Transitory Record, as defined in the Management of Information Act, is as follows:
A record of temporary usefulness in any format or medium having no ongoing value beyond an immediate and minor transaction or the preparation of a subsequent record.

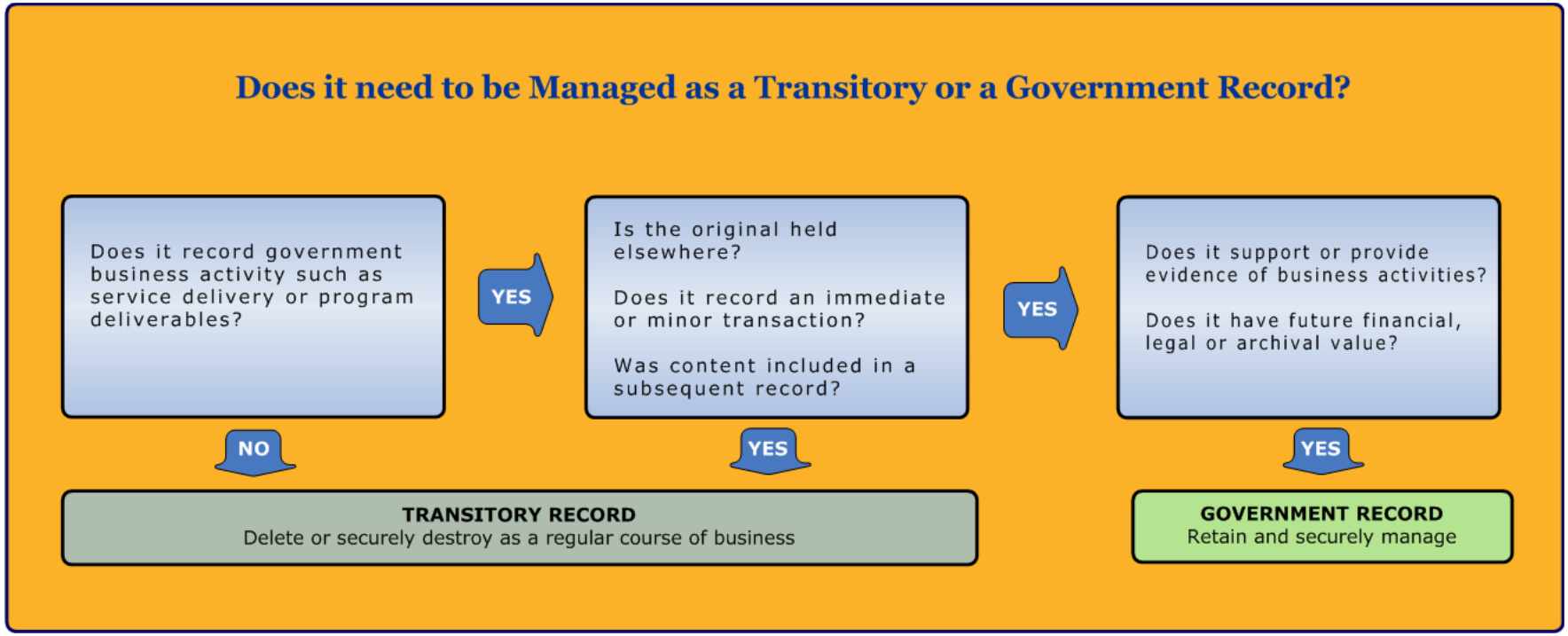
- Drafts of work which reflect content that is included in the final version or contain only minor edits to content or formatting changes
- Electronic version of a signed document, where it has been determined that the signed version is the official record or "original"
- Convenience copies of information retained for reference purpose
- If you copy a record maintained in an electronic records management system, the copy is considered transitory

What is a Transitory Record?

- Transitory records may still contain personal or confidential information so they still need to be managed and protected
- Transitory records are discoverable in the event of a legal discovery process (e.g., litigation, ATIPPA, audit, etc.)
  - Retaining transitory records can make the discovery process more expensive and time consuming
- Transitory records can be securely destroyed when no longer of value without authorization

Determining Transitory Records

When receiving information, follow the chart below to determine if the record is a transitory record or retained as a public body record.



Section Highlights:

- ✓ Information management is also known as records management.
- ✓ The term information management evolved from records management.
- ✓ Management of records is determined by the business and legal value of the information they contain.
- ✓ Employees must manage records in all electronic and paper formats.

Section Highlights:

Information Management can be described as:

- ✓ Day to day actions taken when working with various types of information.
- ✓ Procedures followed by employees to organize information.
- ✓ Storing information with the appropriate amount of protection.
- ✓ Appropriate disposal of information according to disposal schedules.

Summary

- In this section you learned about Information Management, what it is, why it is important and the legislation that governs it. Some examples of records and information formats were introduced as part of delivering services and conducting business for the citizens of Newfoundland and Labrador.

- The next section will focus on information management best practices and how information moves through the organization.

Section Outline

SECTION 1: Introduction to Information Management (IM)
SECTION 2: Best Practices for Managing Information
SECTION 3: Information Management Roles and Responsibilities

Section 2 will:

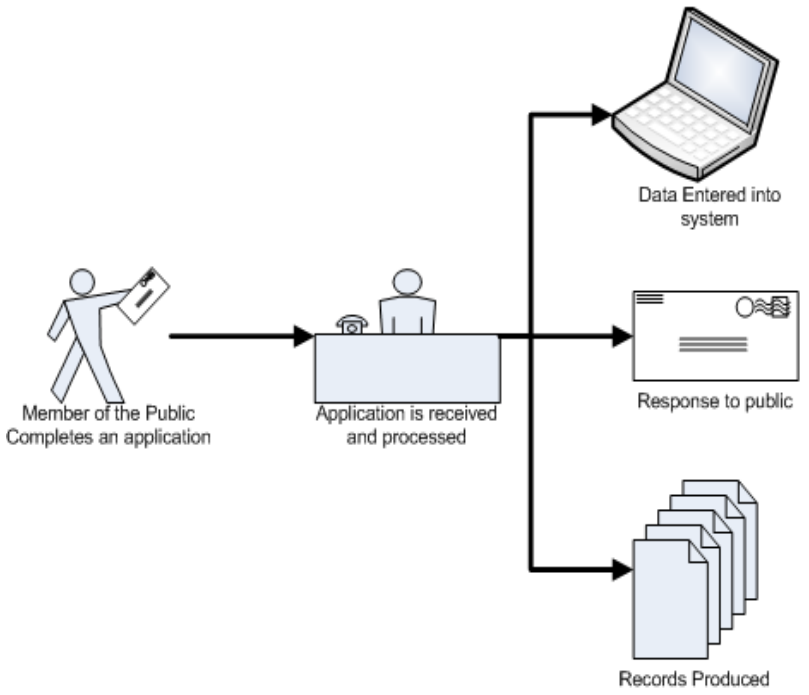
- Show the best practices for managing information
- Focus on the flow of information as it moves through the organization

Information Flow

Information moves throughout organizations daily to support the development of legislation, policy, and programs, as well as the delivery of services (e.g. registering a car or obtaining a birth certificate).

- Data entry accuracy and a clean desk practice are important to protecting privacy and confidentiality.
- Information must be accurate and made available to the public.
- Records are produced daily and in different formats, and need to be managed effectively and securely.

Sample Information Flow: External

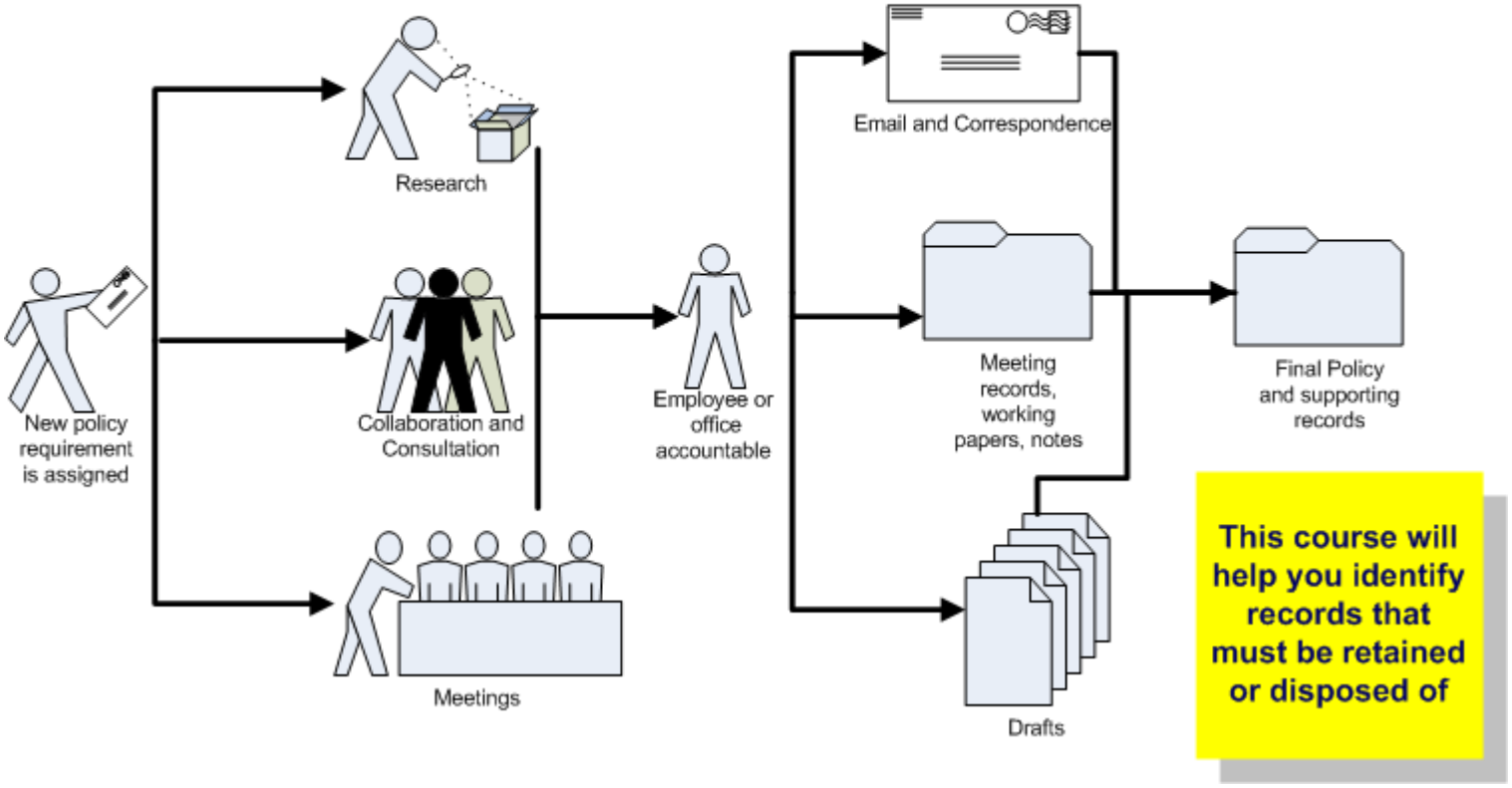


Processes may result in the creation of multiple records in different formats

Information Flow

Sample Information Flow: Internal

Information moves internally from many individuals and groups.

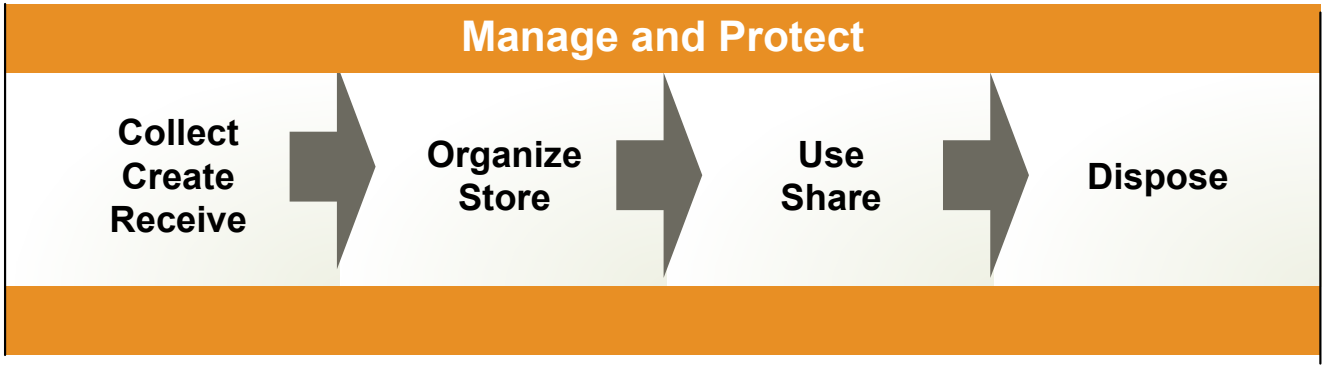


Information Management Best Practices

There are elements to consider when information is moving through the system in support of business activities:

- Create information that is accurate and complete, using the most up to date forms or templates.
- Collect information that accurately reflects the activity or business function being documented.
- When receiving information, quickly determine its value and how it will be used.

The Information Life Cycle

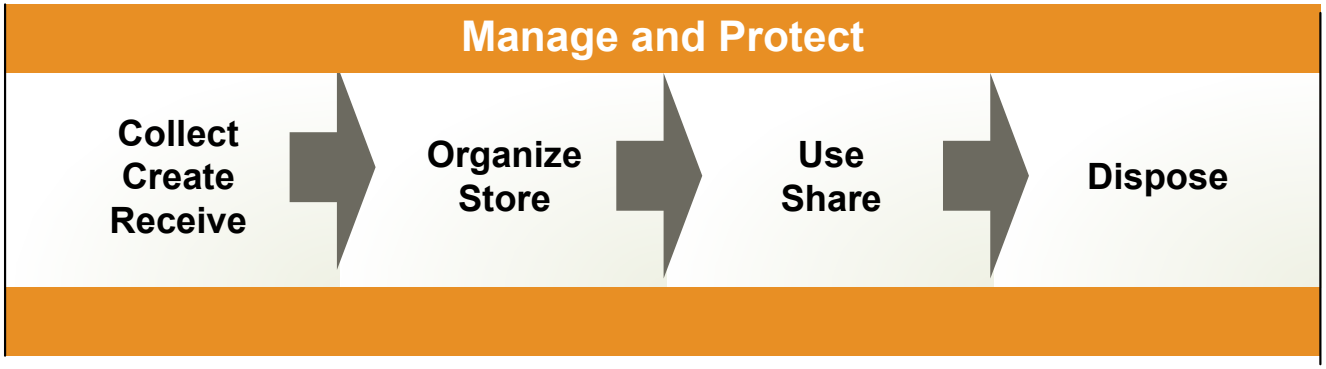


Information Management Best Practices

Other elements to consider:

- Organizing information is critical to finding it quickly, and securing it.
- When sharing information, it is important to share only with people who require it for business purposes.
- Be discreet, and use a screen protector if you must view information in open areas.
- Store information to ensure that it is protected and accessible, and with as little duplication as possible.
- When a record is no longer needed to support the business, this record may be ready for disposal.

The Information Life Cycle



Collecting Information

- When collecting information, only collect the amount and type of information needed to provide a service, or support business activities.
- Employees should only collect information that the public body is authorized to collect.
- Always be aware of your surroundings and ask yourself the following question: What would be the impact or risk if this information was seen accidently by clients, colleagues, or bystanders?

Receiving Information

- We receive information as a regular part of our day-to-day work.
- Information best practice includes quickly analyzing the information and deciding the best way to use it.
- Best practices also include determining which records are transitory and can be disposed of.

Phishing

- When receiving or collecting information, be aware of the potential for Phishing.
- Phishing is a type of fraud that uses deceptive emails, websites and or text messages to gather personal, financial and confidential information for fraudulent and/or unauthorized purposes.
- How do you protect yourself from phishing?

✓ *Never click on links or attachments in e-mails from unknown sources*
✓ *Never disclose your work username and password*
✓ *Never use your work email for personal use*

You are responsible for the activities performed using your IT network username and password including information protection.

Creating Good Records

In the creation of records it is important to ensure:

- A record is **comprehensive**, meaning it contains all elements required to document a complete decision, transaction, process etc.
- A record is **accurate**, meaning that the information correctly reflects the decision, transaction, process etc.
- A record is **complete**, meaning that in addition to the content of the record it contains the structure and context required to understand the decision, transaction, process etc. being recorded.
- A record **documents the regular course of business**/operations meaning that activities necessary, normal, and incidental to the business are followed when a record is created.
- A record is created **within a time period** that is reasonable. This aids in developing clear, accurate content.

Creating Good Records

Imagine being asked about a case, claim, project or policy file in the future. Do the records that exist contain sufficient detail to enable future users of that information to understand the activity, transaction or decision? Records need to be able to stand on their own as a reflection of the event, activity or transaction. Some best practices include but are not limited to:

- Ensure records include sufficient detail to provide an understanding of the event, activity or transaction.
- Use current forms and templates to ensure all required information is captured
- Review to ensure content can be used by other users

Creating Good Records

Email is a very common tool for creating and communicating information. When composing email:

- Use a detailed subject line that reflects content
- Include sufficient information so that an individual not directly engaged in the process will understand the content
- Copy only those individuals that need to action or must be informed
- Ensure that the information recorded is accurate.
- Review forms and templates for accuracy
- Double check data entered into a business application or system

Organizing Information

Categorize information to make it easy to find and secure access to sensitive information.

Schedule needed time to sort, organize and label information.

Information can be organized many ways, as follows:

- Function and/or Business Activity (e.g. Client Management, Events)
- Date - Fiscal or Calendar year (e.g. 2007, 2008, 2009)
- Subject or Type (e.g. Project ABC, Meeting Minutes)
- Work Group or Organizational Unit (e.g. Accounts Division, Payroll)
- Color code or number files

Using Information

When using information, it's important to follow best practices.

Public body records may contain personal and confidential information and their security does not change as a result of becoming transitory.

As a best practice, it is better to delay a response or service than to put information at risk by disclosing it to unauthorized individuals.

Using Information

Newfoundland Labrador

Important Best Practices:

- A “clean desk” practice can limit unauthorized access to information in your work area.
- Information should be viewed in a secure location. Ensure information is not in view of others who do not have authorization to see it.
- Always double check that you do not leave information behind when exiting a car, taxi, boardroom, conference room etc.
- Be cautious when carrying open file folders as information can fall from them. Consider a brief case or secure folder for loose files or documents.
- Consult with your manager or the organization’s Information Management division, if you need to clarify whether personal or confidential information can be accessed.

Sharing Information

When sharing information, it is important to ensure that it is only shared with people who require it for business purposes.

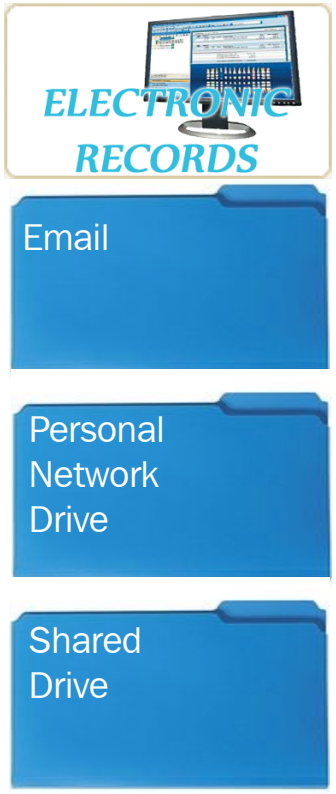
Sharing Information

- Use a coversheet that clearly identifies the sender and the recipient, with appropriate contact information
- Do not fax sensitive or personal information
- Check fax numbers carefully, or use programmed numbers for frequently faxed locations
- Notify the recipient that the fax is being sent, and verify with the recipient that the fax has been received
- Book meeting rooms to discuss sensitive matters instead of talking openly in a cafeteria, around a workstation, etc.
- Erase content from whiteboards and remove pages from flip charts before leaving a meeting room
- Ensure that copies of records are retrieved from the meeting site and returned to the office for secure disposal

Storing Information

Information is stored in many locations and IM best practices help keep it accessible and protected.

Storing Information



- Ensure that Email is organized and that transitory email records are removed on a regular basis
- Employees are sometimes provided with a Personal Network Drive to store information related to an employee's specific job duties
- A Shared Drive is used by public bodies to store information that needs to be accessed by multiple employees
- If information is personal or confidential, it may not be appropriate for this information to be stored on a Shared Drive. Verify with your manager, or IM division, to confirm where this information should be stored
- Be familiar with your organization's backup protocols

Never save records to your local drive
(e.g. "C" drive, My Documents, Desktop)

Storing Information

- Portable Storage Devices (PSDs) include USB flash drives and CDs. PSDs are intended for temporary storage of information that is, or will be, backed up on the organization's network
- There are significant risks involved in using PSDs. Caution and diligence are required when using portable storage:
  - When working outside the office, only use an encrypted PSD to transport and store needed information. Upon returning to the office, transfer the information contained on the PSD back to the network, then delete the files from the PSD
  - Report misplaced or stolen PSDs to your Manager/Director

Storing Information

Personal Work Station

File Cabinets

File Room Registry

- Personal Work Stations such as cubicles need to be kept clean and organized in order to find information quickly and prevent access to sensitive information by those without a business need to see it
- Ensure established procedures for the File Room Registry are followed, including the sign in and out of records
- Lock File Cabinets when you are not at your desk
- Ensure that File Cabinets, located in common areas, are locked after use, and that the keys returned to the person responsible for their safe keeping

Disposing of Information

When a document, e-mail, paper record, etc. is no longer needed to support business and legislated retention requirements, this record or information is ready for disposal.

There are two ways to dispose of public body records:

SECURE DESTRUCTION

TRANSFER TO THE ROOMS PROVINCIAL ARCHIVES

The Rooms
ARCHIVES · ART GALLERY · MUSEUM

Disposing of Information

- Records of historical value are transferable to The Rooms
- Part of the mandate of The Rooms, as outlined in The Rooms Act, is to:
  - Collect, preserve, present and make available for research the historic artifacts, natural history specimens and archival records that represent and illustrate the natural heritage of the Province
- The *Management of Information Act* must be followed before any records are legally destroyed
- When a document, e-mail, paper record, etc. is no longer needed to support business activities, and legislated retention requirements are met, this record or information is ready for disposal
- In order to destroy records, the public body's legal time limit for keeping them must have expired

Disposing of Transitory Information

Transitory records are disposed of anywhere in an organization's information flow when they are no longer required, and include the following:

- Paper records in secure shredding bins, or via desktop shredder.
- Published materials placed in recycling bins, such as magazines .
- Electronic records such as email and electronic documents.
- CDs, DVDs, Portable Storage Devices, Tapes, etc. Contact the organization's IM division to dispose of these.

In the event of an ATIPP request or legal proceedings, all transitory records on that issue must be accessible. Deleting transitory records as a regular practice is the first step to effective information management.

Section Highlights:

- ✓ Sharing an application such as a new driver's license with only those with the business need for the information is IM best practice.
- ✓ A copy of the original information already in an electronic records management system is considered transitory and can be securely destroyed.
- ✓ If an email has no ongoing value beyond an immediate and minor transaction or the preparation of a subsequent record, it is considered transitory and may be deleted.

Employees should not respond to or click on any links from a suspected phishing email. Such emails should be deleted.

Summary

- In this section, you learned how information flows through the organization from the time it is collected, received and created until disposed.

- The next section will focus on the roles and responsibilities of those managing and protecting information. As you explore these further, think about the flow of information and IM best practices.

Roles and Responsibilities

Section Outline

SECTION 1: Introduction to Information Management (IM)
SECTION 2: Best Practices for Managing Information
SECTION 3: Information Management Roles and Responsibilities

Section 3 will:

- Explore the roles and responsibilities of those managing and protecting information

Who Is Responsible for IM?

Newfoundland Labrador

EVERYONE

According to the Management of Information Act, all employees and contractors have a legal obligation to manage and protect the information they maintain on behalf of the public body.

Who Is Responsible for IM?

Information Management has always been a responsibility of public service employees.

The *Management of Information Act* was proclaimed in 2005 and requires all public bodies, including departments, to implement an IM program.

Organization | Public Bodies | Employees | OCIO

Who Is Responsible for IM?

Being responsible as an **organization** for all information, is part of daily business. This responsibility is driven by information used to initiate, process and finalize:

- Developing programs or policies
- Delivering services
- Managing Projects
- Managing and planning

Who Is Responsible for IM?

Public bodies, including departments and central agencies, are responsible for the information collected as part of their business and legal obligations. They must:

- Authorize the collection and use of personal and confidential information
- Authorize the sharing of the information they maintain
- Limit access to personal and confidential information to those who need it to do their job
- Disclose the minimum amount of information needed to provide a service or complete a transaction

The Office of the Chief Information Officer (OCIO) administers the *Management of Information Act* and establishes policies, directives, standards, guidelines and best practices for all employees in a public body.

Who Is Responsible for IM?

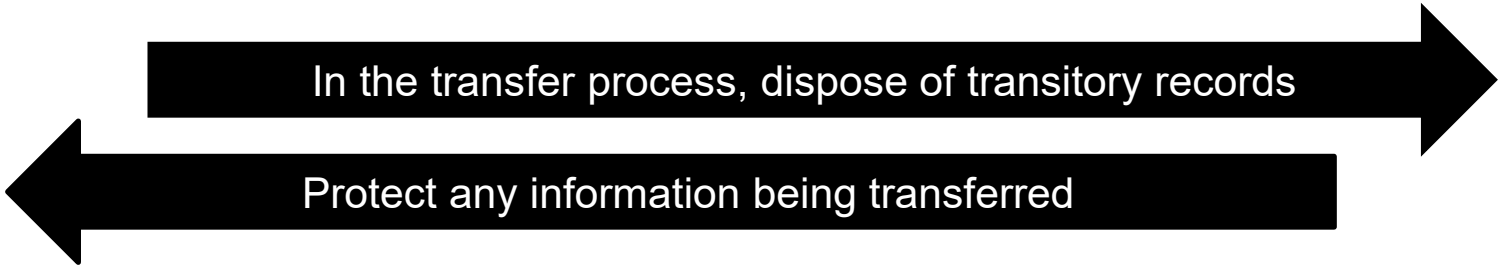
Newfoundland Labrador

Employees are responsible for managing and protecting the information associated with their day to day job duties, including:

- Understanding how IM Best Practices apply to their job
- Protecting sensitive information
- Accessing information only to do their job
- Ensuring that records are accurate and up to date

Employee Responsibilities

When you transfer to a new position, change roles, or leave the organization, all information is retained by the organization. Paper, electronic records, and e-mail are transferred to an internal resource, as assigned by your manager and the director of Information Management.



A work computer and email are the property of the public body, not the individual. The information on the computer is also the property of the public body, not the individual. Read the Equipment and Resources Usage Policy, from the Human Resource Secretariat for more details on using information technology assets and other equipment in your job.

Who Is Responsible for IM?

The Office of the Chief Information Officer (OCIO) administers the Management of Information Act and establishes policies, directives, standards, guidelines and best practices for all employees in a public body.

Information related to the administration of the act can be found on the OCIO website, including:

- Information Management and Protection Policy
- Acceptable Use Directive - Government Network and Information Technology Assets
- E-Mail Policy

Section Highlights:

- ✓ The public body is responsible for the information it collects, receives, and creates as part of conducting public service work.
- ✓ Public bodies are responsible for records they maintain and must only disclose the minimum amount of information needed to provide a service or complete a transaction.
- ✓ Information regarding using and protecting your account can be found on the OCIO website, including acceptable use of the network and technology assets.
- ✓ When you transfer to a new position or leave a public body position, all information is retained by the organization. Paper, electronic records, and e-mail must be transferred to an internal resource, as advised by your manager or IM Division.
- ✓ Employees must responsibly manage information in their care and control.

Summary

In this section you learned that all employees of a public body have a responsibility to manage and protect the information they use to do their work.

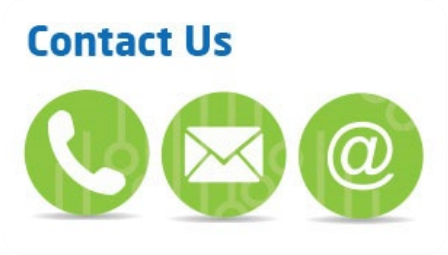
You also learned about IM best practice when an employee transfers within and/or out of the organization.

Summary

Remember!

Everyone is involved in the Management and Protection of Information.

Summary



Questions and inquiries can be sent to im@gov.nl.ca

More information is available at the OCIO Website:
WWW.OCIO.GOV.NL.CA