IM@WORK FOR MY TOWN: BEST PRACTICES THROUGH THE INFORMATION LIFECYCLE

Information Management
Post Graduate Diploma
Program – Capstone 2023

About IM@Work For My Town

- This course is a partnership between the College of the North Atlantic (CNA) Information Management (IM) Post Diploma Program and the Professional Municipal Administrators (PMA), Newfoundland and Labrador
- This course is based on the Government of Newfoundland and Labrador's IM@Work: Making Information Management Work for You Available on the Office of the Chief Information Officer website
- **Completing this course will allow Town Users to:**
    - Demonstrate knowledge of IM and why it is important
    - Identify IM best practices through their lifecycle
    - Recognize IM roles and responsibilities

Background: CNA's IM Post-Diploma

- An interdisciplinary program combining records and information management with courses in business, project management, information technology, communications, and law.

- The IM Capstone is the final course of the program. Our CNA team includes:
  - *Lesley Halliday*
  - *Jason Mills*
  - *Lori Collins (instructor)*
  - *Kaitlyn Hilliard*
  - *Donna Leonard*

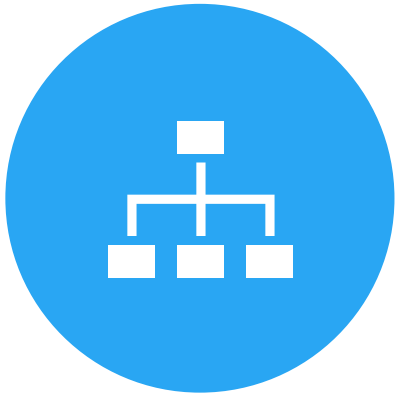
Capstone 2023: IM Toolkit for Municipalities

- **An IM toolkit, for distribution by the PMA to its membership, including:**
  - Records Management Policy template;
  - A standard Records Retention and Disposal Schedule (RRDS);
  - A plan to clear the backlog;
  - IM@Work for My Town – Best Practices Through the Information Lifecycle
- Target audience includes Towns under 1000 residents but can be useful to all

About This Course

MODULE 1: IM BASICS

MODULE 2: BEST PRACTICES



MODULE 3: ROLES AND RESPONSIBILITIES

About This Course

- This course will take approximately 2 hours to review
- There is a summary at the end of each section
- There are test questions at the end of each section that will help you to reinforce your learning
- There are references at the end of the course that will help you to build your knowledge of IM best practices

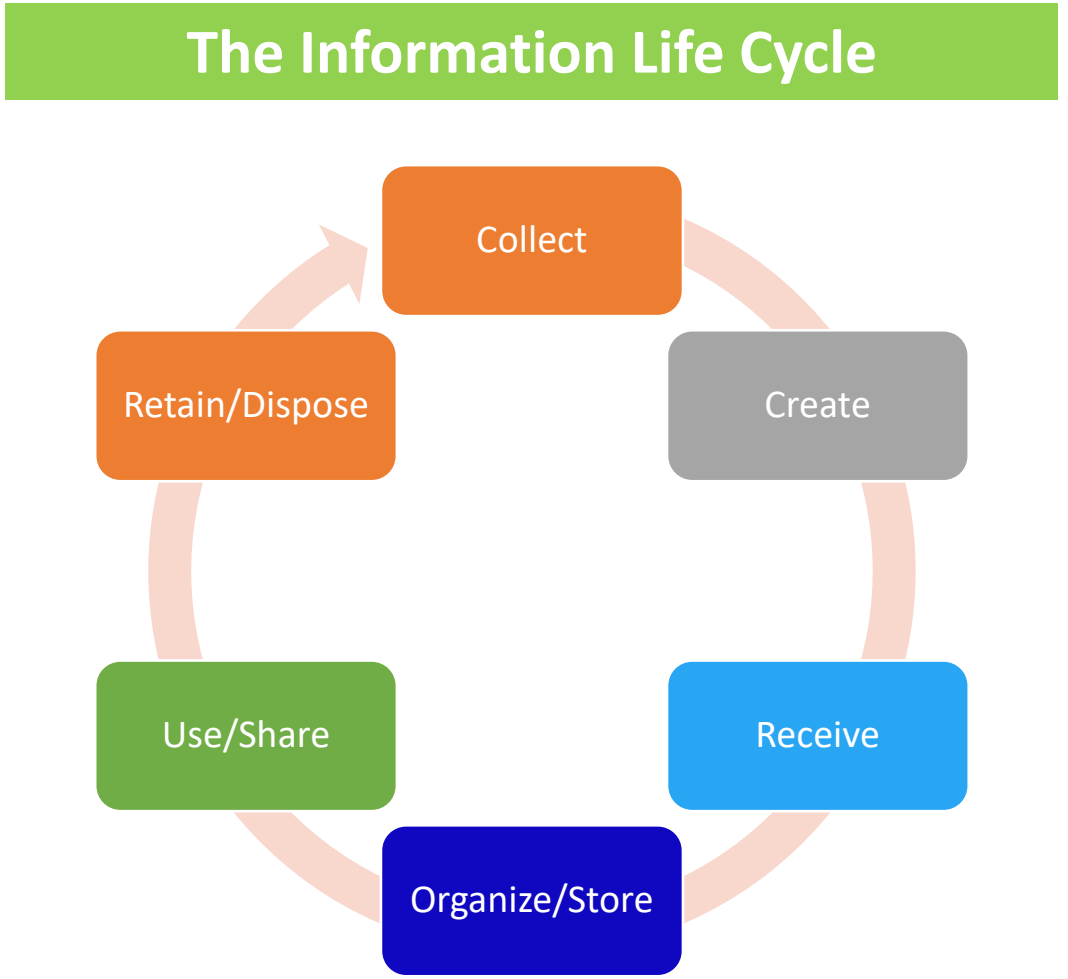
Welcome to Module 1: IM Basics

- **In Module 1, you will be able to:**
  - Define Information Management (IM)
  - Describe why IM is important
  - Identify what types of information must be managed
  - List who the stakeholders are in managing town information

What is Information Management (IM)?

IM is not adding a new task!

- Every time you handle town information, you already make decisions impacting how it is managed and protected
- For example, you complete templates, decide on a file name and location and choose who to share it with
- Each point of use - from collection to disposal - is referred to as the Information Life Cycle
- There are best practices you can apply along this path to improve IM



Town Work is Information Work

Council records including agendas, minutes and reports

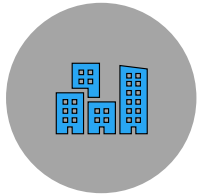
Election management including voter lists and polling information

Managing properties and collecting taxes

Providing permits and licenses

Managing services like organizing garbage collection and snow clearing

Completing projects on town roads, buildings and infrastructure



Hiring new employees, managing payroll, training, etc.

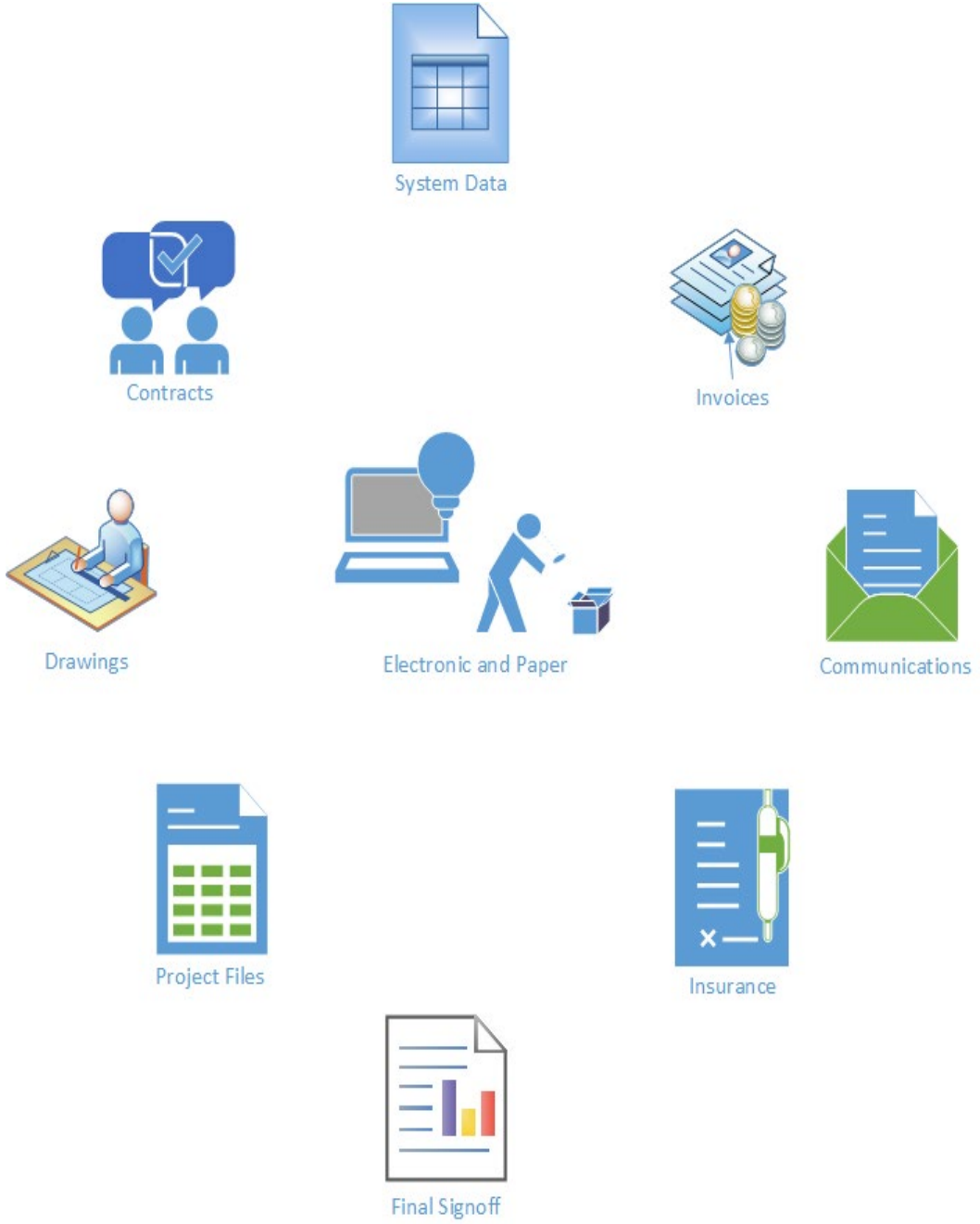
Managing budgets and funding

Why is IM Important?

- Imagine, a taxpayer emailed their councilor photos of damage to a bridge on a town road. You know that this bridge was recently rebuilt by a third party under contract with the town. Right now, you need to know:
  - What is the issue and how to fix it?
  - Who is responsible for fixing the bridge?
  - Does the vendor who was responsible for the work have responsibility?
  - How to let people in the town know about what is happening?

What Information Do You Need to Repair the Bridge?

- **You will need to access paper and electronic information quickly to:**
  - Assess risk to public safety & implement measures
  - Ensure communications to the public, council, the contractors, etc., are accurate and consistent with previous messages, reports, emails and posts, etc.
  - Protect the town from liability and reduce any expenses that may be recovered via the existing contract, insurance, funding partners, etc.
  - Provide information needed so that engineers, planners, construction can complete effective repairs quickly



Benefits of IM

Get More Done for Less

- Faster turnaround time as information is accessible
- Reduce stress and complaints from delays
- Reuse existing documents for new work
- Reduce time wasted looking for information
- Reduce storage of unnecessary information

Faster, Evidence-Based Decisions

- Have all the information you need to make decisions quickly
- Decisions are defensible when complete and accurate information is referenced
- Improve public confidence in the information and services you provide

Communicate Effectively

- Have confidence that you are accessing the most up to date version of information
- Be consistent in content that has been used in the past (e.g. do not provide one taxpayer with information that is different than what you told their neighbor a few months ago)

Benefits of IM

Demonstrate Compliance

- Good IM supports compliance with legislative and regulatory requirements
- Ability to respond to legal, audit or Access to Information requests within required turnaround is improved by good IM practices

Reduce Risk

- Reduce risk of privacy breach by following best practices
- Reduce risk of information loss in the event of a breach when only necessary information is retained
- Ability to demonstrate that good practices were consistently used in the event of an investigation

Evidence

- Good IM means that complete, accurate and unaltered records are created that act as evidence of how you provided programs and services
- Enables the Town to demonstrate transparency and accountability

Legal and Operational Requirements

- Operational Efficiency requires good IM
  - All lines of business have IM requirements

- Legislation including but not limited to *The Municipalities Act, The Municipal Conduct Act, The Emergency Services Act and Municipal Elections Act* have IM requirements.

- Legal commitments including things like contracts or funding agreements (e.g., capital works funding from federal government) may specify retention and access to information

- *The Access to Information and Protection of Privacy Act 2015 (ATIPPA 2015)* is closely related to how you manage your information

ATIPPA 2015

- An informed electorate is the foundation of democracy
- Towns need to be transparent and accountable to the public
- ATIPPA 2015 balances the need to provide access to information with the protection of privacy
- The Town has a duty to assist applicants by communicating what information it has.
- Response to information requests within turnaround period. Exemption of personal information as well as mandatory/discretionary exemptions

- IM best practices helps you comply with ATIPPA 2015:
  - Prevent privacy breach by use of information handling best practices
  - Ensure records exist and are complete and reliable
  - Ability to access records in a timely manner for processing
  - Eliminates unnecessary records from processing

What Kinds of Information Need to be Managed?


Email


Documents


Reports

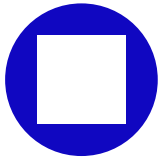

Drawings


Minutes


Phone


System Data


Text


Paper

What Kinds of Information Need to be Managed?

- Town information includes all formats, including physical (paper and hard copy), electronic records (including e-mail and instant messages), records in databases, datasets, or websites and any other technology in which information is created and managed.

- Some of the information the town uses needs to be kept confidential because it is either personal or sensitive

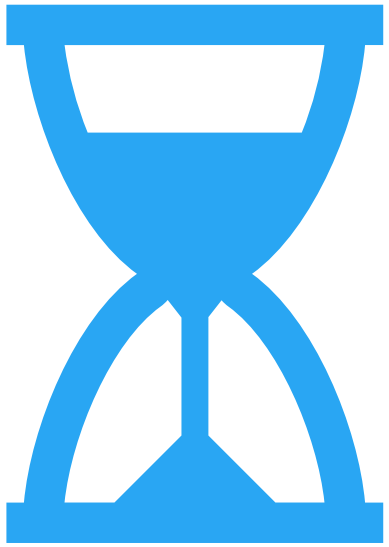
- All information is the property of the town and must be:
  - Managed as determined by the town
  - Returned to the town at the end of employment or term

What Kinds of Information Need to be Retained?

- There is a large volume of Town information that needs to be retained to provide evidence of how it met its mandate
- In today's workplace, there is also a great deal of information that is received/generated that does not need to be retained
- Focusing town resources on the information that needs to be kept to meet operational and legal requirements is a best practice that often relies on your own judgment

Records with Operational/Legal Value

- A Town record is any recorded information, regardless of medium or characteristics, made or received and retained by an organization in pursuance of legal obligations or in the transaction of business.
- Record disposal or destruction must be authorized by a disposal authority such as a Records Retention and Disposal Schedule (RRDS) that has been approved by the Town council. This will be discussed in more detail in Module 2.
- Prior to records disposal it is important to verify with the Town Clerk or ATRIPP coordinator that the records are not part of an expected or anticipated legal action, audit or request for information made under ATIPPA 2015
- Disposal of records must be documented



Transitory Records

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

Examples of Transitory Records

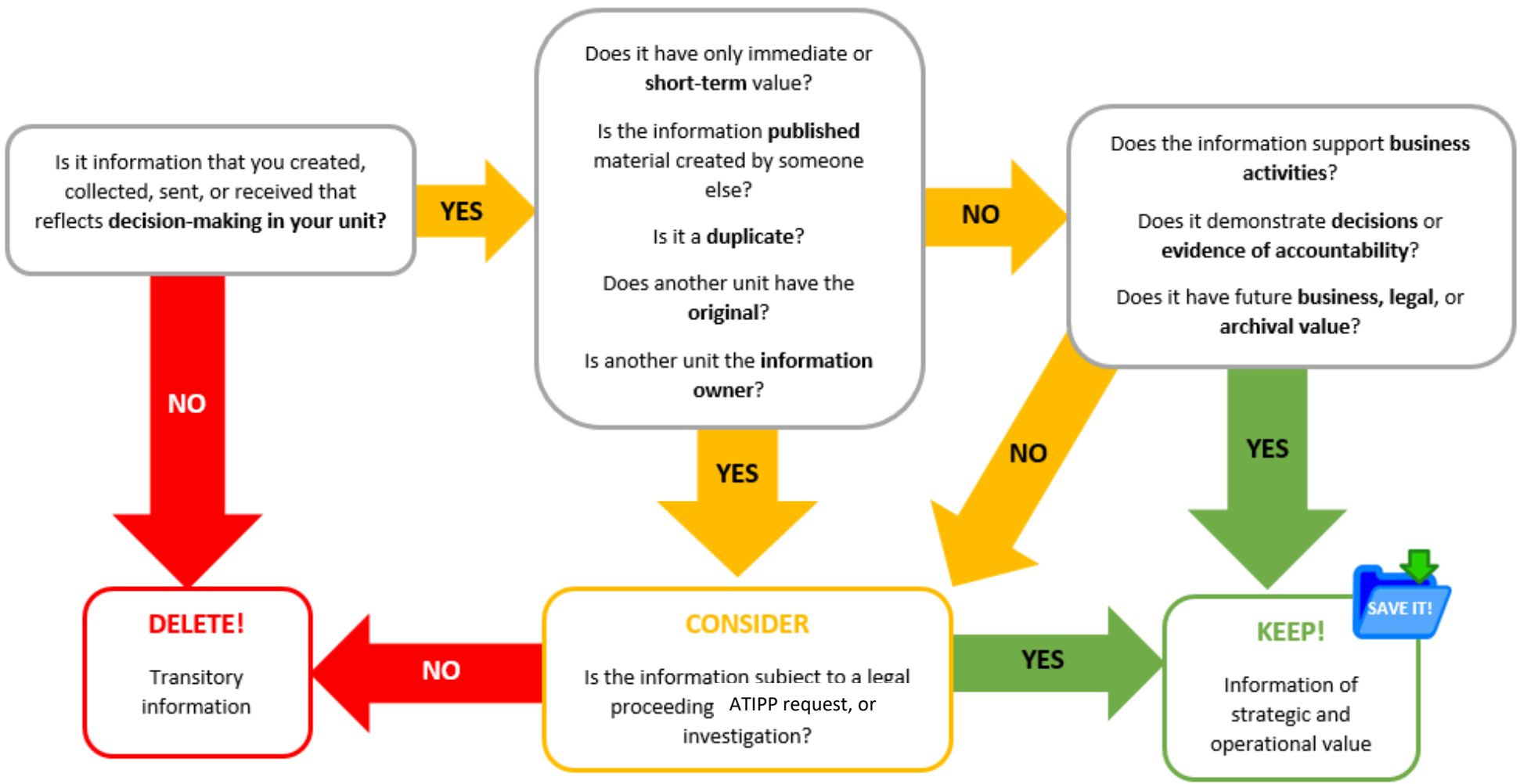
- Phone messages
- Appointment Calendars
- Convenience Copies
- Publications For Mass Distribution
- Drafts
- Working Copies
- Supporting Information
- Routing Slips

Transitory Records

- The definition of the transitory record is critical in helping an organization eliminate large volumes of information that do not contribute to the evidentiary or operational requirement for records retention.

- *The elimination of transitory record is important because:*
  - Just because something is transitory does not mean it does not contain personal or sensitive information. Eliminating copies or drafts of personal or sensitive information mitigates risk.
  - Transitory records are discoverable in the event of an ATIPPA request, audit or legal information request. They need to be processed in the same manner as all other information. Retaining transitory records potentially compounds the resources required to respond to information requests.
  - Transitory records are an unnecessary use of space and other resources (e.g., offsite storage, backup and recovery) when determining what records need to be retained.

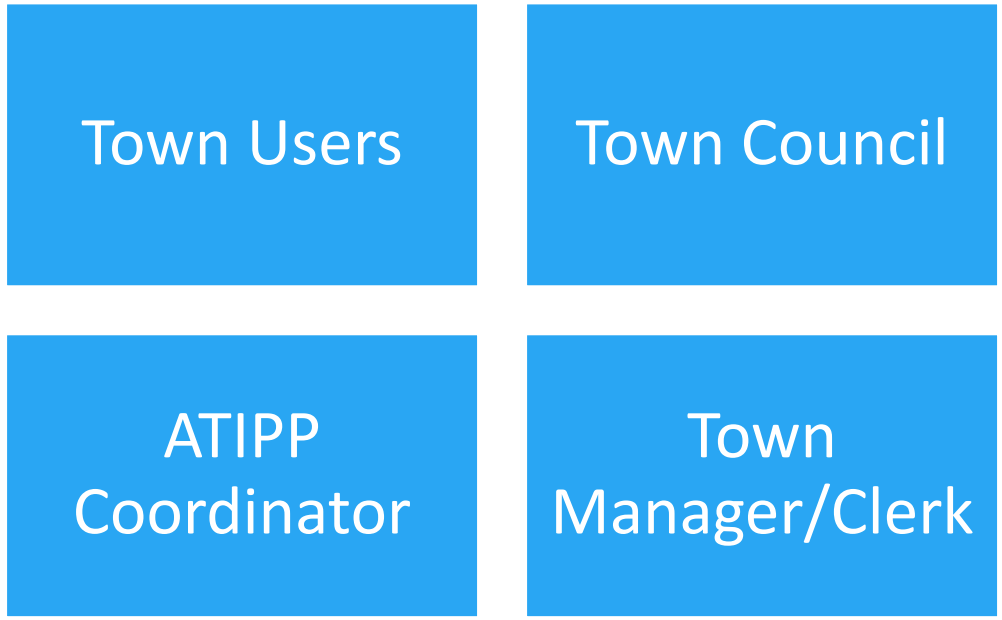
Transitory Records



College of the North Atlantic

Who Needs to Manage Information?

- Town users include anyone who handles information on behalf of the town:
  - Employees
  - Council
  - Volunteers
  - Contractors
- Other individuals/groups have additional responsibilities
  - How IM tasks are assigned vary depending on the size of the town
- Module 3 will provide more detail on roles and responsibilities



Module 1: Summary

- IM involves the handling of information throughout its lifecycle
- Implementing IM best practices ensures effective responses to access requests, compliance standards can be met and help to limit the retention of unnecessary information
- All information, regardless of media type needs to be managed and protected
- Transitory records are discoverable in the event of an ATIPPA request, audit or legal information request. It is important to dispose of these records on a regular basis to avoid limit the associated legal risks

Module 1: Test Your Knowledge

Q: You have several drafts of the council minutes with minor edits for formatting and spelling errors. The final minutes have been posted to your town site, would these drafts now be considered transitory?

Q: Who are the stakeholders in managing town information?

Q: What are three examples of information types that need to be managed?

Module 1: Answers

A: Yes. The drafts can now be securely destroyed.

A: Town users, town council, ATIPP coordinator and the town manager/clerk. Town users also include employees, volunteers and contractors.

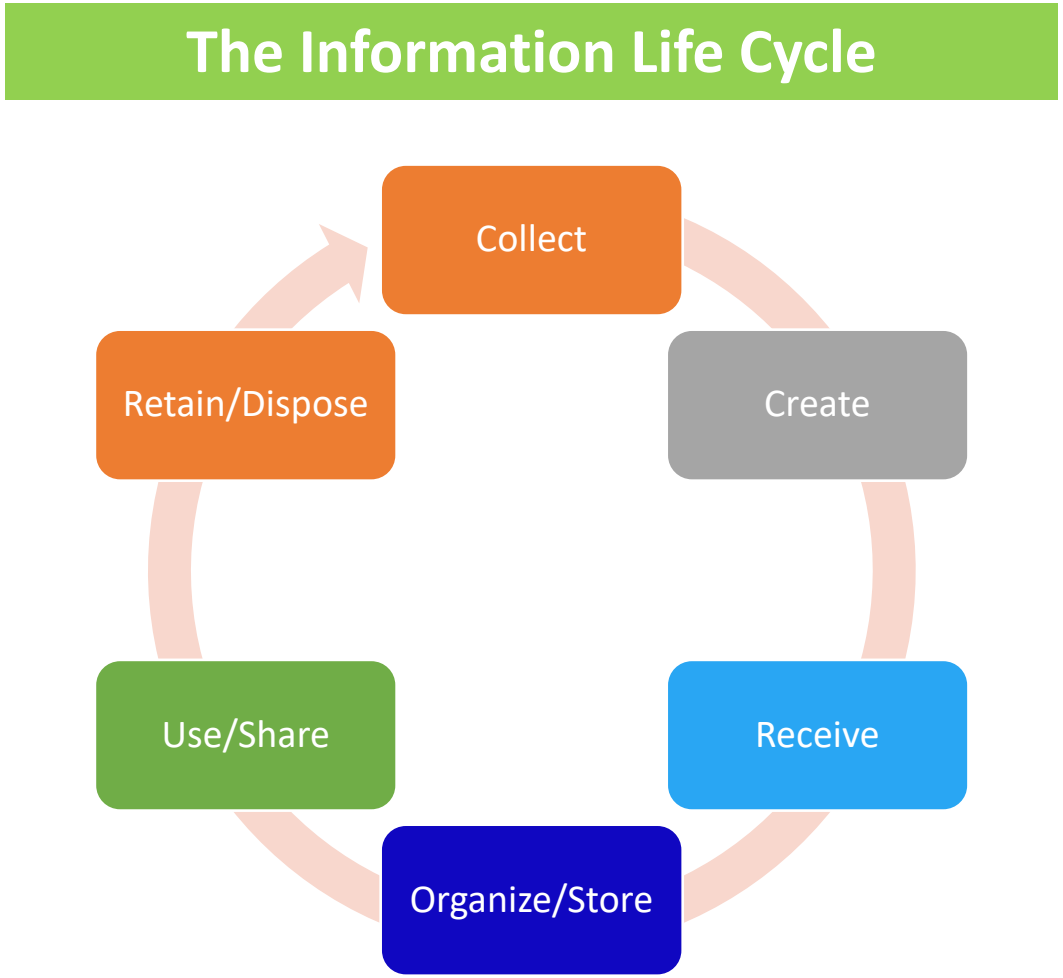
A: Information type examples include, e-mails, documents, reports, drawings, meeting minutes, phone recordings/voice mails, text messages, paper and system data.

Welcome to Module 2: IM Best Practices

- **In Module 2, you will learn to:**
  - Apply best practices to manage and protect information through the life cycle
  - Understand what phishing is and how to identify/manage it
  - Make decisions regarding information value of transitory records versus records that must be retained
  - Use tools like records retention and disposal schedules

Stages of the IM Lifecycle

- IM is the things you do daily when you are working with town information as a part of your job.
- The way information flows through the town is sometimes called its lifecycle. It is how information is:
  - Collected, created or received as part of daily work
  - Organized and stored to ensure it is safe and easily retrieved
  - Used by Town Users or shared with others
  - Disposed of when the Town no longer needs it



Collection



- Occurs whenever the town actively seeks, acquires, receives, obtains, gathers, or compiles information
- Often is driven or flows from an external source (e.g., taxpayer)
- Can happen via telephone, email, correspondence, form, interview, etc.
- Initiates a process or service and creation of new records (e.g., new permit)
- Some information the town collects is personal or confidential. This means that it needs to be protected at all stages
- The collection point is where there are many potential risks!

Collection

Risks to information collection include:

- Town users are unaware which types of information includes PII or confidential content
- Failure to obtain consent for the collection of personal information
- Collecting information beyond what is needed to provide the program or service
- Information is not collected in a secure manner – e.g., at the counter where others may overhear

Collection

- **Personal Identifiable Information (PII)** means recorded information about an identifiable individual

- **Confidential information** is information that is prohibited from disclosure because of legislation or court order or any other information that pertains to the business of the Town generally considered to be of a confidential nature,
  - All municipalities must comply with the ATIPPA 2015 so using the definitions in that Act is an easy way to identify what information needs to have extra protection

- All employees need to understand whether the information they are working with is personal or confidential and apply safeguards

What is Personal Information?

Contact Information (e.g., name)

Race/Religion/ Political (e.g., Indigenous status)

Physical Descriptors (e.g., age)

Health Information (e.g., sick leave note)

Anatomical (e.g., biometrics)

Unique Identifier (e.g., account number)

Social, Educational or Financial (e.g., bankruptcy)

Opinions (e.g., reflects personal relationship or assessments)

What is Confidential Information?

- Cabinet confidences
- Local public body confidences
- Policy advice or recommendations
- Legal advice
- Disclosure harmful to law enforcement
- Confidential evaluations

What is Confidential Information?

Disclosure harmful to the financial or economic interests of a public body

Disclosure harmful to conservation

Disclosure harmful to individual or public safety

Disclosure harmful to business interests of a third party

Disclosure harmful to personal privacy

Disclosure harmful to intergovernmental relations or negotiations

Collection

- Should be limited only to that which is necessary to provide a program or service.
- Requires a privacy notice, as set out in s. 62(2) of the *ATIPP Act, 2015,* to be given either verbally or in writing prior to collection.
- Town users must collect only information that the Town is authorized to collect.
- Be mindful of your surroundings during collection and ask yourself the following question: what would the impact or risk be if this information was accidentally seen by clients, colleagues, or bystanders?

Collection

- Do not leave confidential or sensitive information on a desk or displayed on a screen while you deal with another client, colleague, etc.
- Use the most up to date form or template
- Verify that information/records are complete and accurate
- Organize and label information as soon as it is collected

Collection Summary

- Collection occurs whenever information is obtained
- Information can be collected from many sources in varying formats
- The collection point of information can pose many risks. This includes unidentified personal information, failure to obtain appropriate consents, over/unnecessary collection and unsecure collection.
- Personal and confidential information acquired by the town requires additional protection in order to comply with ATIPP legislative standards

Collection: Test your Knowledge

Q: What are some examples of personal information?

Q: What are some examples of confidential information?

Q: What are some best practices related to information collection?

Collection: Answers

A: Contact information, race/religion/political views, physical descriptors, health information, anatomical data, unique identifiers, social/educational/financial information, and opinions.

A: Local public body confidences, legal advice, policy advice/recommendations, disclosure harmful to individual/public safety, disclosure harmful to personal privacy, and disclosure harmful to business interests of a third party.

A: Ensure forms and templates are up to date, collect only what is necessary and authorized, organize and label information upon collection, verify accuracy and provide notices of collection.

Creation

- Have you ever been asked about a meeting, property, building or project that occurred before you started with the Town?
  - 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.

Creation

- Everyday you create information to document events, business functions or activities using:
  - Software like Microsoft Word, Excel or PowerPoint
  - E-mail
  - Business applications including databases or systems designed to support your processes (e.g., Townsuite or accounting software)
  - Pen and paper
- Your goal is to create information that accurately reflects the activity or business function you are documenting.

Creation

- Creation is when the town uses information at its disposal to create a new information product
- Creation is often driven or flows from an internal requirement (e.g., new funding grant, council minutes)
- Typically will use internal desktop tool like word processing, spreadsheets, email
- Responds to an assigned task (e.g., monthly council meeting agenda)
- May contain personal or confidential information depending on the nature of the document. This means that it needs to be protected at all stages

Think about our damaged bridge….
One issue or event may result in many types of information being created as the problem is resolved

Taxpayer Identifies Safety Concern

Email Photos to Councilor

Councilor Raises Awareness

Assessment and Response

Multiple types

These are some types of information may result from one event or issue

Communicate to Stakeholders

Media Inquiries and Responses

Website and Social Media Notices

Assessment Records

Legal Action

Designs

Meetings and Council Approval

Tender and Contracts

Construction

Invoices & Payments

Creating Good Records

When creating a record, it is important to ensure the record is:

Comprehensive: contains all elements required to document a complete decision, transaction, process etc.

Accurate: the information contained in the record, correctly reflects the decision, transaction, process etc.

Complete: in addition to the content of the record, it contains the structure and context required to understand the decision, transaction, process etc. being recorded

Documents the regular course of business/operations: activities necessary, normal and incidental to the business are followed when a record is created

Created within a reasonable time period: aids in the development of clear, accurate content

Qualities of Good Records

Authenticity: An authentic record is one that can be proven to be what it purports to be, to have been created or sent by the person purported to have created or sent it, and to have been created or sent at the time purported. (Source: ISO 15489-1: 2016)

Integrity: The assurance that information is accurate, correct, and authentic by using consistent methods to create, retain, preserve, distribute, and track information (Source: ARMA).

Usability: means that the record can be found and used effectively when needed. Records are to remain accessible and legible throughout the duration of their lifecycle.

Creation

- Know the intended audience and how information will be used to focus on the appropriate detail, language and content
- Choose the right tool to communicate the information:
  - Don’t write a short e-mail when what is really needed is a full decision document or position paper
  - Do you need to create a new piece of information, or would a meeting or quick phone call be a better way to communicate?
- Have a consistent approach to managing drafts or versions

Creation

- Use the most up to date form or template
- Review information to ensure that it is clear and accurate
- Use departmental naming conventions to label documents and files
- Remember that working papers that are used in the preparation of a subsequent record may be considered transitory in which case they can be securely deleted or destroyed when no longer required

Creation

- Under the Municipalities Act, Section 215, the following types of documents must be available for inspection by the public
- Do not include any personal or confidential information when you create these records

Adopted Minutes of the Council	Assessment rolls	Regulations
Municipal Plans	Opened Public Tenders	Financial Statements
Auditor's reports	Adopted Budgets	Contracts
Orders	Permits	All documents tabled/adopted by Council at a public meeting

Creation

When composing an e-mail:

- 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
- Double check data entered into a business application or system

Creation Summary

- Records require sufficient detail and context in order to accurately represent business functions
- Personal and confidential information must be protected during creation
- Good records are those that are authentic, have integrity and are useable
- When creating records, be mindful of their intended audience and maintain a consistent approach
- Follow best practices when composing e-mail messages

Creation: Test your Knowledge

Q: What are 5 things to consider when creating records?

Q: What are some best practices when creating e-mails?

Q: What are some best practices related to creating records?

Creation: Answers

A: Ensure records are: Comprehensive (contain all of the process elements), Accurate (correctly reflect process), Complete (contain context for understanding process), Documented in the regular course of business, and created within a reasonable time period.

A: Detailed subject line, includes sufficient information, copy only those that the e-mail is intended for, and ensure accurate information.

A: Use up to date forms and templates, review information for accuracy, apply naming conventions to files, identify whether newly created records are transitory

Receiving Information

- We receive information as a regular part of our day-to-day work. This information can come from many different sources and in many different structures.
- When information is received it should be quickly analyzed to decide the best way to use and store it.
- When information is received it should be analyzed to identify if it is considered transitory and if it should/can be disposed of.

What is a Transitory Record?

- 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.

A document or piece of information that is considered temporary and has a short-term value for an organization or individual.

Transitory records are typically of temporary or fleeting importance and are not meant to be retained for the long-term.

They may include draft documents, emails, informal communications, or other similar materials that are used for reference or convenience but are not considered permanent or official records.

Receiving

Information is received by the Town through a variety of channels including regular mail, courier, email, text messages or other messaging technologies

Information may be provided verbally in person or via phone or other technologies (e.g., Skype or Microsoft Teams)

Often is driven or flows from an external source (e.g., taxpayer)

May initiates a process or service and creation of new records (e.g., new permit)

Some information the town collects is personal or confidential. This means that it needs to be protected at all stages

There are many potential risks when receiving information!

College of the North Atlantic

Receiving

Risks to receiving information include:

- Information may be unsolicited and waste time
- Information received electronically via email, text or other messaging technologies may contain malware or viruses that risk information loss, cyber attacks or ransomware
- Information may not be sent to the right person to deal with an issue, complaint or request

Receiving Information

- Records received by Town users will apply best practices for the protection of information.
- Ensure records are routed to the authorized and intended person
- Classify and store records as soon as they are received
- Follow established practices for receiving (e.g., date and time stamp physical records if this is your practice)
- Town users should verify that sources of information are trusted:
  - Go back to a previous email
  - Visit an official website
  - Person to person contact (e.g., phone or direct messaging to known accounts) as needed.

Phishing

When receiving or collecting electronic 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.

Never click on links or attachments in e-mails from unknown sources

Never disclose your work usernames and/or passwords

Never use your work e-mail for personal use

Phishing

- Perpetrators profile victims then send a message that the victim may assume to be legitimate
- This information may have been obtained through another breach or through social media
- It may be because they know where you bank, an online store where you shopped or even because they know your kids play a sport
  - Open your discount from xyz…
  - There is a problem with your account
  - You have been chosen to receive a reduced rate on your insurance
- **“Spear phishing”** is an email targeted at a specific individual or department within an organization that appears to be from a trusted source

Phishing: How to Recognize it?

- Only click on email links and attachments from known, trusted and verified sources
- Verify the authenticity of the link/website address before you select it. You can do this by moving your mouse over the link to reveal the actual address

Phishing: How to Recognize it?

- Check the spelling and other characteristics in the address itself

Correct Address	Example of a Phishing Address
www.royalbank.com	www.rbcc.com
www.facebook.com	www.facebokk.com
www.visa.com	www.vsa.com
www.mun.ca	www.mmun.ca

- Use your search engine to research an unfamiliar website

Phishing: Examples

- **Phishing**:
  - *"We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity…"*
  - *"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information…"*
  - *"You have won a prize, contest, etc. please respond…"*
  - *"Someone you know needs a transfer of funds immediately because they are stranded…"*

Receiving: Summary

- Information is received through a variety of channels and may initiate the service or the creation of new records
- Records you receive may contain personal or confidential information, this sensitive information must be identified and handled appropriately
- Electronically received messages may contain malware, viruses or phishing schemes which could lead to information loss or privacy breaches
- Following best practices to identify phishing e-mails helps to mitigate their adverse effects
- Records should be identified as transitory upon receipt to limit storage, and improve organization and retrievability

Receiving: Test your Knowledge

Q: Identify the channels through which records can be received.

Q: What is Phishing?

Q: You receive an e-mail from Microsoft regarding a software update which includes a clickable link. What are some steps you can take to ensure this e-mail is legitimate?

Receiving: Answers

A: E-mail, regular mail, courier, instant messaging, text messaging, verbally via phone/video conferencing software.

A: A type of fraud that uses deceptive e-mails, websites and/or text messages to gather personal, financial and confidential information or fraudulent and/or unauthorized purposes. Oftentimes scammers will peruse personal social media accounts to create a personalized/targeted phishing e-mail, making it appear more legitimate.

A: Hover your mouse over the link to verify its source, check for spelling, font consistency and grammatical errors within the e-mail. Search your web browser to confirm the legitimacy of the website address and e-mail content. Refrain from clicking links until you seek further verification (i.e., ask a co-worker). Refrain from using your work e-mail for personal use to manage expectations on who/which companies would be e-mailing you.

Organize/Store

- Imagine there is an ATIPP request that asks for all the records related to the purchase and renovation of the recreation facility which has been around since 1988!

- The town has a limited time to complete a search of all its information holdings. If the town does not respond within the time limit, the requestor has the ability to file a formal complaint.

Organize/Store

- Organization occurs when a Town user classifies information for the purpose of storage
- Follows collection, creation or receipt
- Is essential to:
  - Linking the information to the business process
  - Applying access controls to minimize unauthorized access
  - Aiding future retrieval

- Using the RRDS as a basis for organizing information is a best practice that aids retrieval and minimizes retention of unnecessary information
- The organization point is where there are many potential risks!

Organize/Store

- **Risks to information organization/storage include:**
  - Mislabelled or filed information may be lost forever
  - Delayed access to information
  - Wasted time spent locating poorly organized information
  - Unauthorised access to information that is not organized properly

Organize/Store

- Every process, service or program you provide results in a record or a group of records
  - *IM calls this a record series*
- Record series have the same management requirements as access control, retention period, etc.
- There is often a file for each time the process occurs
- This is where the record series requirements are applied

Organize/Store

- Understand the business process – how does information flow through the town?
- What records are generated to support the business
  - Paper
  - Systems
  - Electronic
- Who creates, uses and shares these records?
- What is the best way to organize these records to support operations and ongoing access?
- What triggers disposal – time or event based?

Organize/Store

- Use the Town's approved records retention schedule
- Reorganization of any existing records series or the application of the records retention, shall be consulted with the Town Clerk
- Organizing information can make it easy to find and secure access to information
- A naming convention is a generally agreed structure for naming records/files in such manner that describes what they contain and how they relate to other files
- They help to stay organized, identify records and retrieve a record when necessary

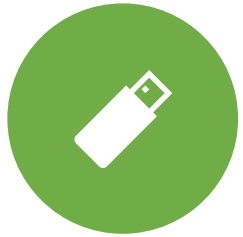
Organize/Store

TOWN RECORDS ARE ORGANIZED ACCORDING TO DIRECTION OF THE TOWN CLERK.

TOWN RECORDS ARE STORED IN SECURED STORAGE LOCATIONS AS DIRECTED BY THE TOWN CLERK.

REASONABLE SECURITY MEASURES MUST BE USED TO TRANSPORT AND STORE REMOVABLE MEDIA.

REMOVABLE MEDIA IS PASSWORD PROTECTED AND/OR ENCRYPTED.



RECORDS STORED ON REMOVABLE MEDIA ARE RETURNED TO THE TOWN'S STORAGE LOCATION AS SOON AS POSSIBLE.

Organize/Store

Best Practices:

- *Passwords* – ensure they contain a combination of letters, numbers and symbols and refrain from using the same password across multiple accounts
- *Backups* – complete them often and routinely to ensure information is protected
- *Access Control* – only give access to authorized personnel
- *Naming Conventions* – ensure they are uniformly applied by everyone
- *Version Control* – ensure reference documents are kept up to date and employees do not use outdated information

Organize/Store: Summary

- Proper organization ensures information is available in a timely manner and mitigates loss
- Access control protocols prevents unauthorized access to information and assists in privacy breach prevention
- Classification guides the records retention and disposal schedule
- Naming conventions improve searchability and retrievability of information and mitigates loss
- Regular backups of information support its availability and access
- Version control allows users access to the most up to date information and allows them to compare current versions with older versions and review changes

Organize/Store : Test your Knowledge

Q: Why is organization and classification of information essential?

Q: What are some risks associated with improper storage of information?

Q: What are some best practices to information organization/storage?

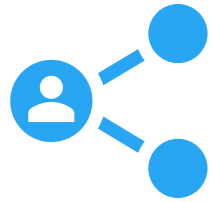
Organize/Store: Answers

A: Linking the information to the business process, applying access controls to minimize unauthorized access and aiding future retrieval

A: Information may take a long time to find or may be lost altogether, unauthorized access may occur, and retention and disposal requirements may not be met

A: Passwords, backups, access control, naming conventions, version control, classification procedures and adherence to the RRDS

Using/Sharing



- Imagine your aunt, who lives out of province, asks you for an address of someone who lives in the town because she wants to send them a Christmas card
- What's the big deal? When using and sharing town information you need to think like a Town User and not a neighbor, relative or friend.
- It can be challenging, especially when living in a small community where many people seem to already know everyone like:
  - Where they live
  - Where they work
  - Who sold them their land
  - What local company will bid on work
  - And more….
- But using or sharing Town information for reasons other than why it was collected may result in complaints and/or legal issues

Using/Sharing

- Following collection, creation or receipt, information may:
    - Require action
    - Start a new process
    - Need to be routed to another Town User or authorized work connection to make things happen
    - Need to be released to the public or available for inspection
    - Need to be updated, modified and/or signed off
- Under various legislation including *The Municipalities Act* and *ATIPPA 2015*
- There are risks associated with using and sharing information

Using/Sharing

Risks to sharing and using information include:

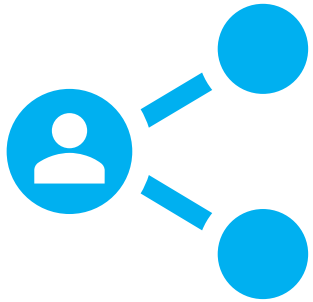
- Information that includes PII or confidential content is shared:
  - With those who are not authorized to access it
  - Used or shared for purposes other than it was collected
- Accidental disclosure due to human error or unsafe handling practices
- Poor document and/or version control resulting in inability to locate most up to date information
- Lack of collaboration resulting in too many transitory record copies retained

Using/Sharing

Town records are used and shared minimally in a manner consistent with the original purpose of collection/creation in accordance with the ATIPP Act, 2015.

Town users do not disclose confidential information obtained in the course of their duties, except as required by law or as authorized by the town to do so.

Best Practices:



- A “clean desk” practice can limit unauthorized/accidental access to information
- Information should be viewed in a secure location, away from unauthorized individuals
- Always double check that you do not leave information behind when exiting a car, taxi, boardroom, conference room etc.
- Use a brief case or secure folder to transport sensitive files and documents
- Consult with your Information Management division, if you need to clarify whether personal or confidential information can be accessed.

Using/Sharing: Summary

- Using or sharing town information for reasons other than why it was collected may result in complaints and/or legal issues
- Risks to sharing and using information include the mishandling of personal information/accidental disclosure, poor version control that leads to inaccurate/stale dated information and a surplus of transitory records
- Records should be used and shared in accordance with ATIPPA 2015
- Best practices should be followed in the use/sharing of information

Using/Sharing: Test Your Knowledge

Q: What are some risks associated with using and sharing information?

Q: What are some best practices of using/sharing information?

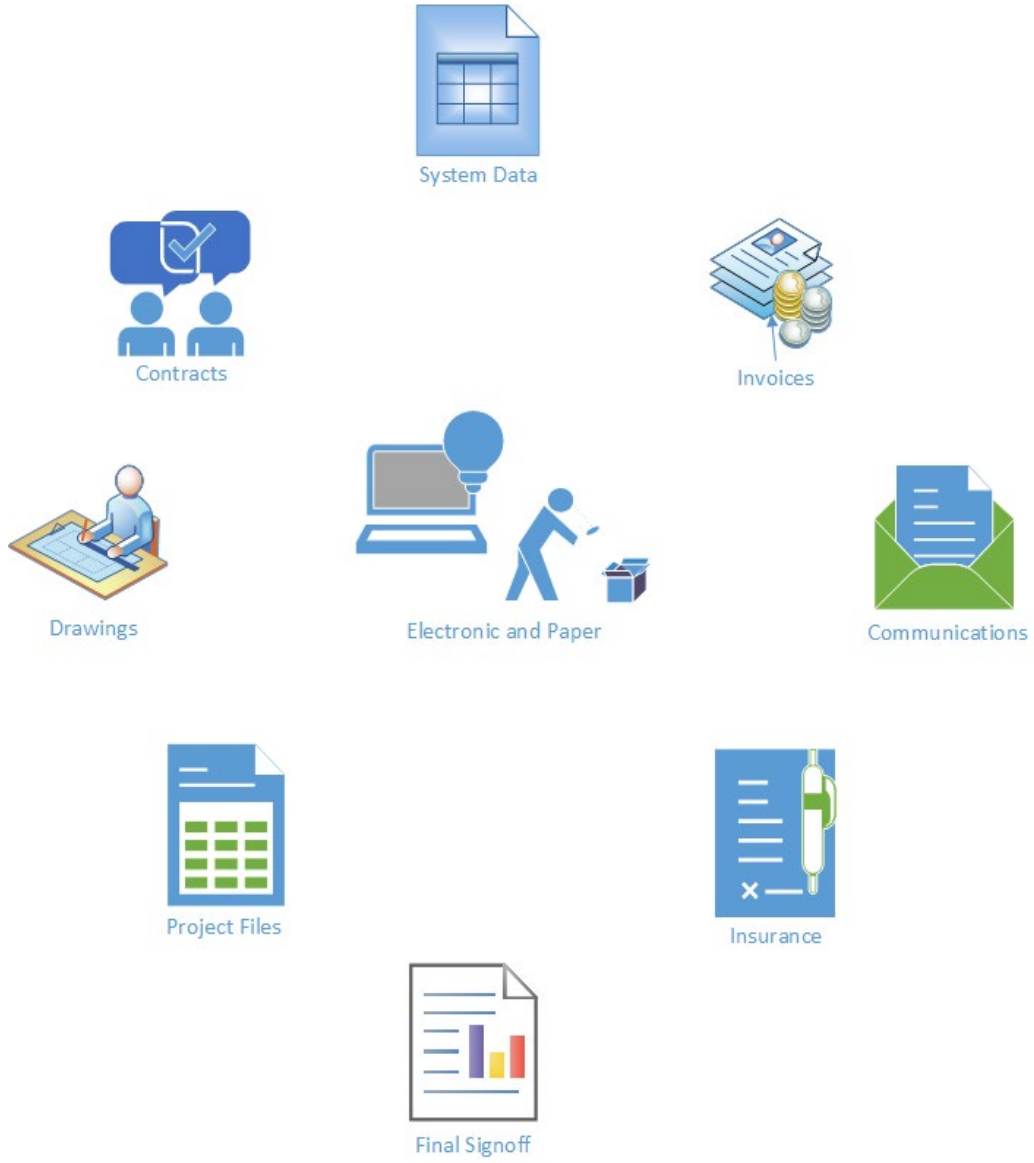
Using/Sharing: Answers

A: Personal identifiable information or confidential information could be authorized, used or shared inappropriately, lack of version control may result in decisions guided by outdated information, and an excess of transitory records that result from a lack of collaboration

A: Use information sharing agreements where required. Consider using links instead of attachments when sending e-mails. Work in an organized environment and limit loose files/papers. View information in a secure location. Be careful not to leave information in an unsecure location. Transport sensitive information in a protected manner. Consider encryption when sharing sensitive/personal information.

Retain/Dispose

- Remember the damaged Bridge? One of the vendors who had been outbid made an ATIPP request for all records related its construction and repair
- Your search finds no responsive records.
- The applicant makes a complaint. This initiates an investigation and public report.
- Retention means information needed for operational and legal requirements is maintained and accessible
- Disposal means that when legal retention requirements are met, information is:
  - Securely destroyed
  - Transferred (e.g., local archives or museum)



Retain/Dispose

- *Risks associated with retention and disposal include:*
  - Records are not retained and/or accessible
  - Extensive transitory records are retained wasting search and processing time and storage resources
  - Records are not securely disposed of risking loss or breach

Records Disposal

- Town users dispose of transitory records as a regular course of business.
- The RRDS authorizes the retention and disposition of the town's records.
- Town records may be transferred to a third party as approved by the Town Clerk.
- Town records will be destroyed securely and completely, without possibility of reconstruction.

What is a Retention and Disposal Schedule?

A policy/procedural document that identifies how long different types of information assets are to be held, and how they will be archived or disposed of at the end of their lifecycle.

What is a RRDS?

Records generated **from** an **event, activity or process are called record series**

These records typically **have the access, retention and disposal** requirements

Identifies how long records need to be kept for legal purposes

Description is detailed enough to allow an employee to retrieve the right records

Will records be retained permanently or archived or securely destroyed

Elements of a RRDS

Code

Record Series Description

Retention Period

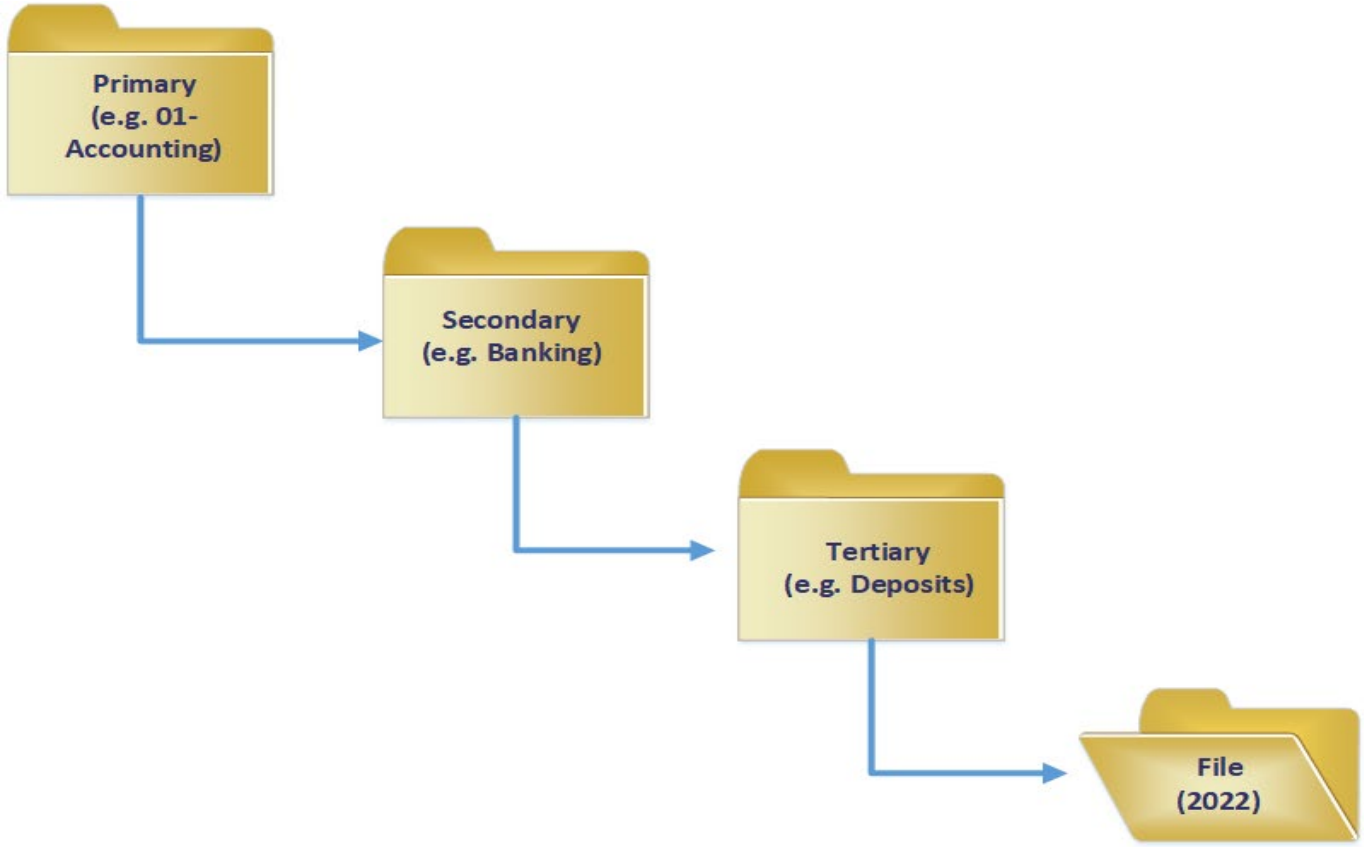
Disposal – Destroy or **Archive**

RRDS Template: Primary Record Series

- 01 - Accounting
- 02 - Buildings, Facilities and Properties
- 03 - Engineering and Public Works
- 04 - Human Resources
- 05 - Legal Services
- 06 - Legislative and Regulatory

Record Series	Description	Retention	Disposition
Banking			
Account Information	Includes account details, agreements and requirements resulting from the establishment and maintenance of bank accounts held by the municipality.	Permanent	Permanent
Signing Authorities	Includes policies, procedures, completed forms and signature cards that document the individuals that have signing authority for bank accounts held by the municipality.	Permanent	Permanent
Bank Statements	Includes periodic bank statements issued by financial institutions for accounts held by the municipality.	7 Years	Destroy
Deposits	Includes all records related to regular deposits made to municipal accounts by approved signing authorities. Includes deposit books.	7 Years	Destroy
Cheques	Includes records relating to the issuance and management of cheques, including cheque vouchers, journal vouchers, returned cheques, cheque lists, cancelled cheques, etc	7 Years	Destroy

Secondary and Tertiary Series



- Close the File at the end of the fiscal year
- Based on the RRDS, these records are securely destroyed after 7 years

Retain/Dispose: Summary

- Information must be retained both for operational and legal requirements.
- Transitory should be destroyed/deleted to reduce search times.
- Records must be disposed of in a secure manner to prevent breaches.
- An RRDS (Records Retention and Disposal Schedule) dictates how long records must be kept for legal purposes, works with classification to allow for organization and retrieval, and determines destruction or archiving. It includes a code, record series description, retention period, and destroy/archive status.
- An RRDS consists of a Primary, Secondary, and Tertiary Record Series as a means of classifying categorically down to specific files.

Retain/Dispose: Test your Knowledge

Q: What are some risks associated with retention and disposal schedules?

Q: What are some examples of a primary record series?

Q: What are the elements of a Records Retention and Disposal Schedule?

Retain/Dispose: Answers

A: Records become difficult to locate, too many transitory records can prolong the search process, legally required to retain certain records, risk of loss or breach from improper disposal.

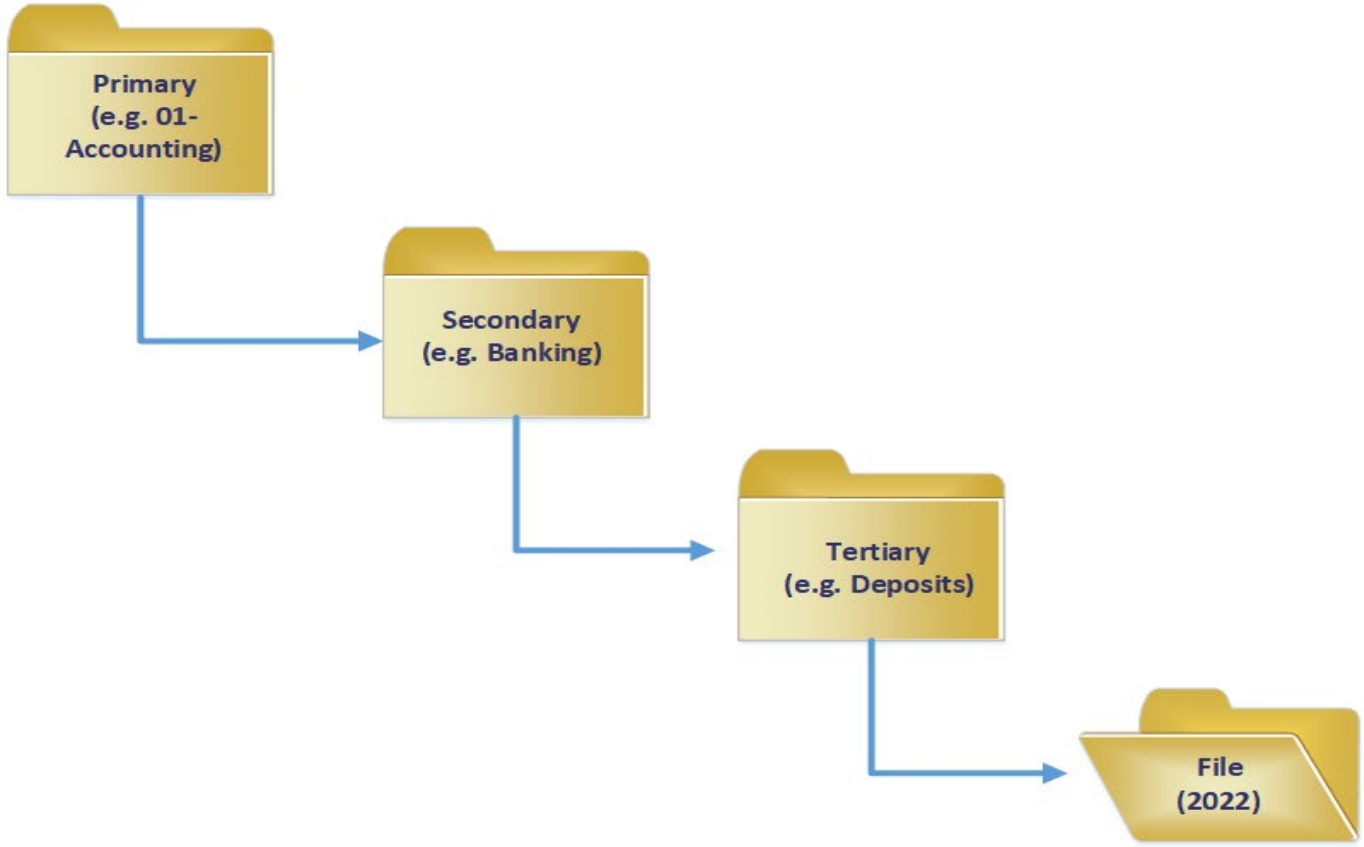
A: Accounting; Buildings, Facilities, and Properties; Engineering and Public Works; Human Resources; Legal Services; Legislative and Regulatory.

A: A code, the retention period, a records series description, and whether to destroy or archive a particular record series based on its classification.

Welcome to Module 3: Roles and Responsibilities

- **In Module 3, you will be able to:**
  - Define Information Management (IM)
  - Describe why IM is important
  - Identify what types of information must be managed
  - List who the stakeholders are in managing town information

Secondary and Tertiary Series



- Close the File at the end of the fiscal year
- Based on the RRDS, these records are securely destroyed after 7 years

Welcome to Module 3: Roles and Responsibilities

- **In Module 3, you will be able to:**
  - Understand roles and responsibilities related to Town IM
  - Describe best practices for managing Town information through the employment cycle

Roles and Responsibilities

While everyone is a Town User, there are additional responsibilities associated with different roles.

These may vary depending on your Town's policies or staffing arrangements

- Town Users
- Town Clerk/Manager
- ATIPP Coordinator
- Council
- Head of the Public Body

Roles and Responsibilities

- Town Users include all employees, elected officials, contractors, consultants, partners, students, temporary workers, volunteers, vendors, agents, third parties and other persons working on behalf of the town
- Town users are responsible to the creation, use and management of records as defined by the Town's internal policy and directives. Following the best practices outlined in this training supports compliance!

Roles and Responsibilities

- The role of the Town Clerk and the Town Manager (or CAO) are defined in *The Municipalities Act*. In small municipalities these roles are typically combined.

✓ Overall management of the Town's records.	✓ Control access to Town records and storage locations.
✓ Organize orientation and training for Town Users on their records management responsibilities.	✓ Retrieve and catalogue all records returned to the Town by the Town Users at the end of their term or employment.
✓ Provide tools and resources to Town Users to support compliance with this policy.	✓ Support ongoing disposal of records as per the RRDS.
✓ Authorize/issue equipment and tools to Town Users for the production/storage of town records (e.g., Town network and/or email account, computing devices, cellular phone, etc.).	✓ Identify/approve record storage locations either onsite (e.g., town hall) or offsite (e.g., approve secure storage at a Town User's home office).
✓ Identify alternative storage locations for Town records including third party storage or archives.	✓ Advise Town Council of any risks associated with non-compliance.

Roles and Responsibilities

- The ATIPP Coordinator is mandated by ATIPPA 2015:

✓ Receiving and processing requests made under the ATIPP Act, 2015.	✓ Educating town users of the public body about the applicable provisions of ATIPP Act, 2015.
✓ Coordinating responses to requests for approval by the head of the public body (as designated under s. 109 of the ATIPP Act, 2015).	✓ Tracking requests made under ATIPP Act, 2015 and the outcome of the request.
✓ Communicating, on behalf of the town, with applicants and third parties to requests throughout the process including the final response.	✓ Preparing statistical reports on requests for the head of the public body.

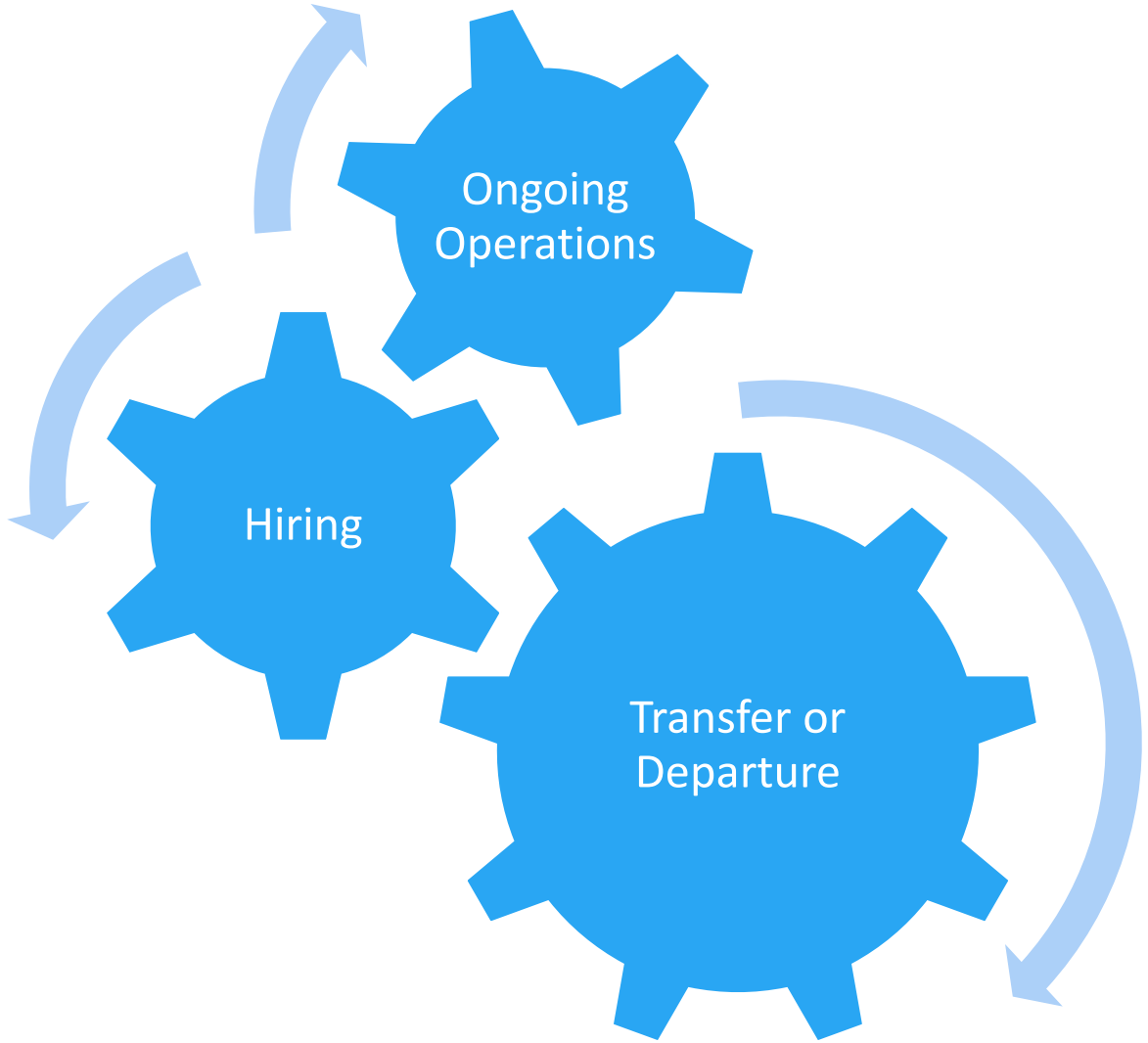
Roles and Responsibilities

- Town Council is responsible for:

✓ Control access to Town records and storage locations.
✓ Retrieve and catalogue all records returned to the Town by the Town Users at the end of their term or employment.
✓ Support ongoing disposal of records as per the RRDS.
✓ Identify/approve record storage locations either onsite (e.g., town hall) or offsite (e.g., approve secure storage at a Town User's home office).
✓ Advise Town Council of any risks associated with non-compliance.

Managing Town Information Through the Employment Cycle

If you are responsible for managing town users, using best practices through the employment cycle ensures compliance, efficiency and that Town information is retained and disposed of properly



College of the North Atlantic

Hiring

- Having employees apply IM best practices may start even before they start work:
  - Create position descriptions that include IM
  - Restrict user access to information and systems they need to do their job
- Provide Orientation for new employees
  - Know whether information is personal or sensitive
  - Understand rules for managing and protecting information
  - Tools and resources your work group uses
- Retain all onboarding and training records

Ongoing Operations

- Have rules on where to store physical and electronic information:
  - Establish one way to classify both electronic and physical records storage
  - Retention and Disposal Schedule
  - Store information in a safe location where risk of damage is low
- Give users tools
  - Boxes and pre-labeled folders with guidance on the inside lid
  - Pre-made electronic folder structures
  - Have rules that direct how to organize information in physical and electronic format and make sure everyone follows them
- Protect information
  - Ensure information is stored in accessible locations
  - Restrict access to storage to those who need it – physical and electronic

Ongoing Operations

- Continue to communicate IM best practices
- Monitor compliance with the rules
- Do periodic random check to ensure quality information and compliance
- Allow employees time to perform IM tasks like closing files, cleaning up email, deleting or shredding transitory records
- Update tools and resources when there are new technologies or requirements

Transfer or Departure

- All information generated or used to complete assigned work on behalf of the town is the property of the town
- When an employee transfers to another role within the town it may not be appropriate for them to have continued to access to information and systems in their new role
  - e.g., an administrative employee move from the engineering to the finance department
- Town information must be retained internally prior to the employee's departure as a result of change in

Transfer or Departure

- As soon as a departure date is known, meet with the employee to review the information they may have stored in their email or workstation
- Develop a plan to ensure all information is retained internally
  - Information stored on the computer hard drive, shared drives or personal network drive
  - Information stored in e-mail mailbox (both inbox and sent mail)
  - Physical records retained at a workstation or in an office
  - Business applications to which the employee has access
  - Storage media including CD’s, DVD’s, etc.

Transfer or Departure

- In the event there is no notice of an employee departure:
  - It may be necessary to notify the IT service desk to modify access to the departed employee's email, network drives or business applications.
  - Complete an inventory of what the employee has in their office and work with your team to identify how/what to transfer to another employee(s).
  - Request access to the employee's e-mail account and personal drive by submitting the appropriate form through the IT service desk.

Contacts

College of the North Atlantic