

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



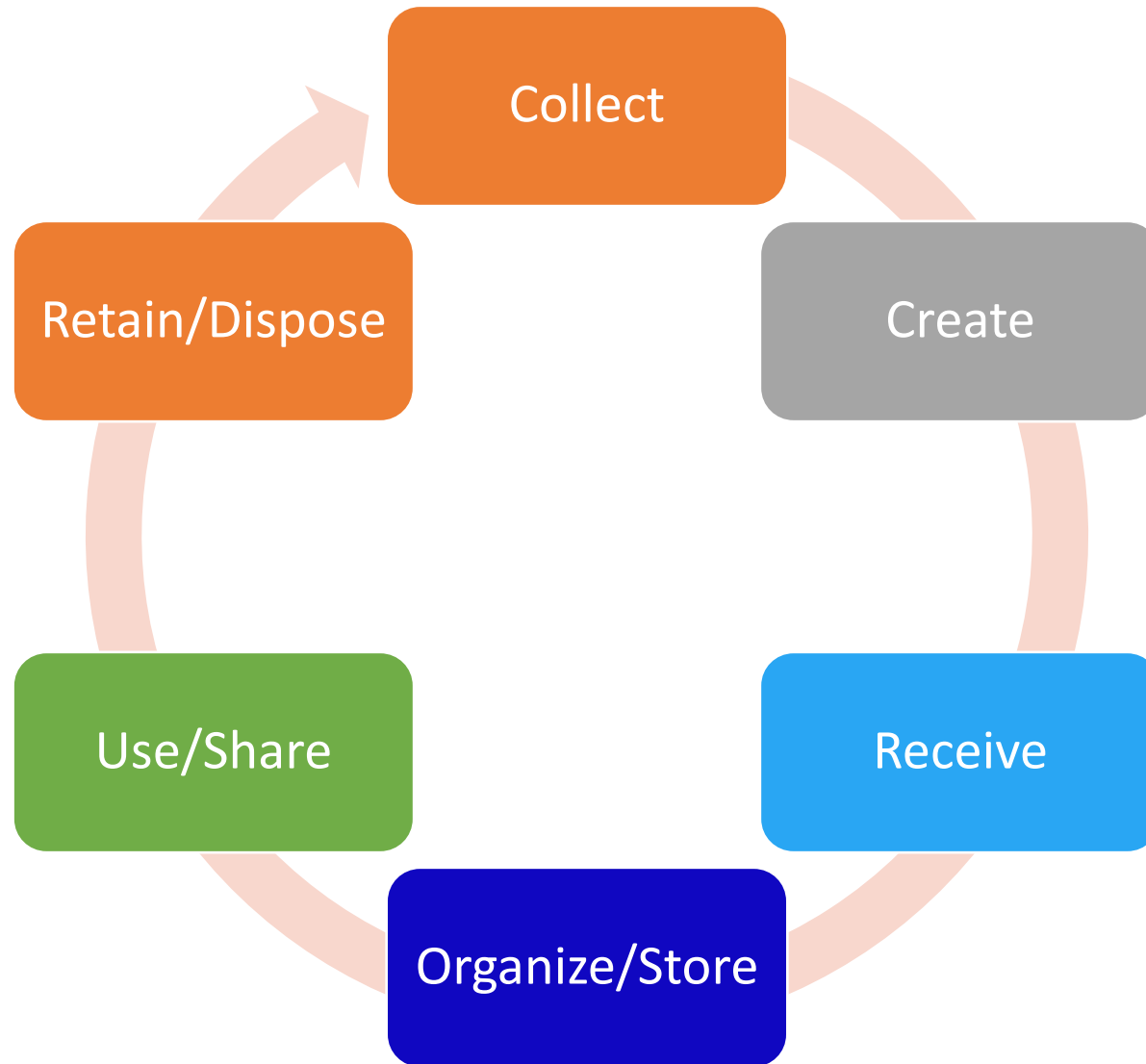
***Module 2.5: IM Best
Practices – Using and
Sharing***

Lori Collins,
Instructor, Information
Management Post Diploma

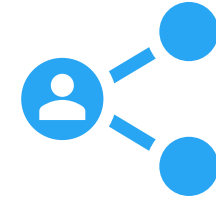
Welcome to Module 2.5: Using and Sharing

- **In Module 2.5 you will learn to:**
 - Recognize restrictions on how, when and to whom information can be shared
 - 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

The Information Life Cycle



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....
- Using or sharing Town information for reasons other than why it was collected may result in complaints, privacy breaches 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

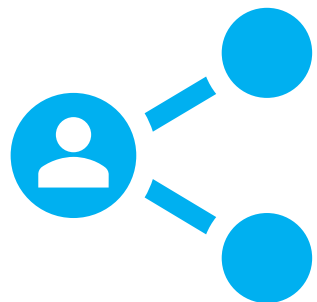


Town records are used and shared minimally in a manner consistent with the original purpose of collection/creation in accordance with the ATIPP Act, 2015.



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.

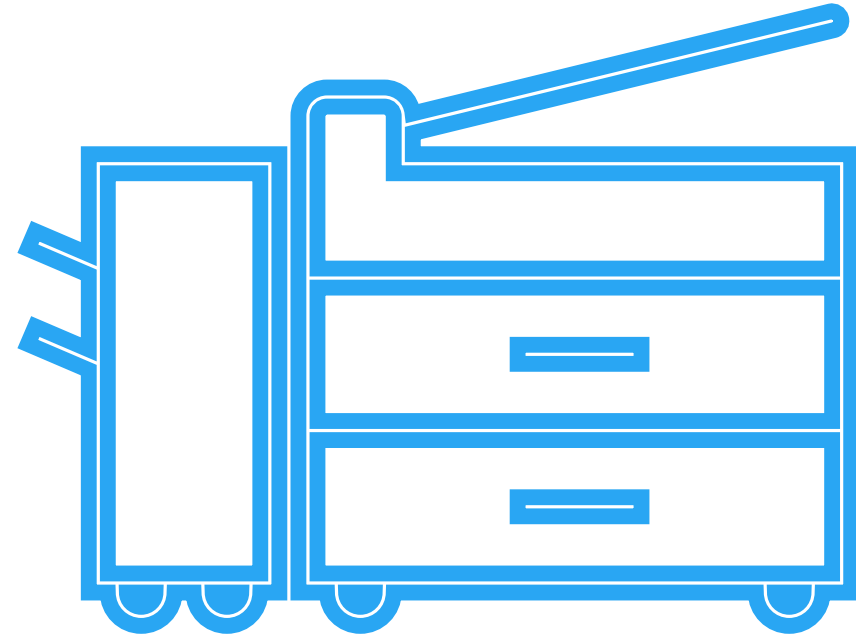
Best Practices:



- Consult with your Town Clerk or manager, if you need to clarify whether personal or confidential information can be accessed.
- 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
- Use encrypted removable media/flash drives

Using/Sharing

- Printing
 - Documents left on a printer can lead to information loss or a breach
 - Learn about the security features of your shared printer
 - Use a password
 - Do not leave documents with personal or confidential information on a printer
 - Pickup your print jobs immediately



Using/Sharing

- Faxing:
 - Do not fax personal or confidential information unless there is no other option
 - Verify with the recipient you have the right number
 - Double Check fax numbers
 - Use programmed numbers for frequently faxed #s
 - Notify the recipient that the fax is being sent
 - Verify with the recipient the fax has been received
 - If you receive a fax that is not intended for you:
 - If possible, contact the sender by phone or Email to notify them of the error
 - Securely destroy the information



Using/Sharing

- Meetings:
 - Book meeting rooms to discuss sensitive content or issues
 - Verify all participants are authorized to be included in the discussion
 - When using an online meeting platform:
 - Verify participants identities
 - Learn about the security options for the meeting platform
 - Notify participants prior to recording
 - Close room doors especially when using external locations (e.g., hotels)
 - Pause discussion when a non-participant enters the room (e.g., catering or IT support)
 - Before you leave the room:
 - Erase all whiteboard content
 - Retrieve all agendas and handouts
 - If used, eject your removable media



About IM@Work For My Town

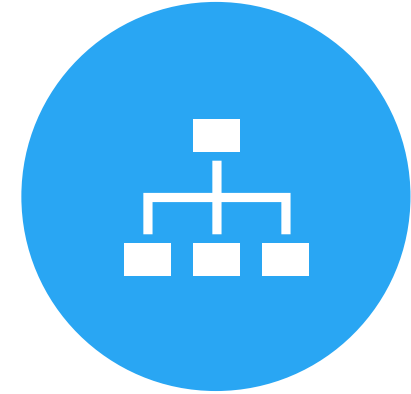


MODULE 1: IM BASICS



MODULE 2: BEST PRACTICES

- 2.1: COLLECTION
- 2.2: CREATION
- 2.3 RECEIVING
- 2.4: ORGANIZE/STORE
- 2.5: USE/SHARE
- 2.6: RETAIN/DISPOSE



MODULE 3: ROLES AND RESPONSIBILITIES



References

- *Creating and Capturing Records*, Archives of Manitoba Government Records Office:
https://www.gov.mb.ca/chc/archives/gro/recordkeeping/docs/creating_records.pdf
- Naming Conventions for Electronic Files and Folders, York University:
<https://ipo.info.yorku.ca/tool-and-tips/tip-sheet-6-naming-conventions-for-electronic-files-and-folders/>
- Version Control Guidance, University of Glasgow:
https://www.abdn.ac.uk/staffnet/documents/policy-zone-information-policies/UoA_Version%20Control_July%202017.pdf
- How to Effectively Manage Removable Media, Stanfield IT:
<https://www.stanfieldit.com/how-to-effectively-manage-removable-media/#:~:text=Data%20breaches%20are%20one%20of,data%20security%20a%20major%20concern.>

CONTACT US

Ashley Sheppard
Communications
Coordinator, PMA

Email: Ashley@pmanl.ca

Tel: 709-726-6405

Lori Collins
Instructor, Information
Management Post Diploma

E-mail: Lori.collins@cna.nl.ca

Tel: 709.728-6726

Rod Hynes
Municipal Access and Privacy
Analyst, ATIPP Office, Department
of Justice and Public Safety,

Rhynes@gov.nl.ca

E-mail: name@cna.nl.ca

Tel: 709.123.4567