IMPROVING ACCESS AND PRIVACY

WITH RECORDS AND INFORMATION MANAGEMENT

This guide provides general advice to public bodies on how to improve access and privacy with records and information management.

FEBRUARY 2022

Office of the
Saskatchewan Information
and Privacy Commissioner

ACKNOWLEDGEMENT

The Saskatchewan Information and Privacy Commissioner would like to acknowledge that this resource is based on the Information and Privacy Commissioner of Ontario resource *Improving Access and Privacy with Records and Information Management*.

CONTENTS

INTRODUCTION

Developing and implementing effective records and information management (RIM) practices and policies are key to compliance with *The Freedom of Information and Protection of Privacy Act* (FOIP) and *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP). The Office of the Saskatchewan Information and Privacy Commissioner (IPC) has prepared this guidance document to assist public bodies and their staff in understanding the direct relationship between good RIM practices and the public bodies' ability to meet their responsibilities under the acts. This guidance will also provide heads of public bodies with a basic understanding of RIM principles and best practices to facilitate conversations with information management professionals and staff.

WHERE RIM MEETS ACCESS AND PRIVACY

When a member of the public submits an access request, public bodies must respond thoroughly and within the required time frame. The public body's ability to do this, however, may be facilitated or hindered by its information management practices.

By implementing strong RIM practices, you:

- Can prevent records from being lost or inappropriately deleted.
- Ensure records remain legible and accessible.
- Reduce search times and fees associated with finding mishandled information.
- Reduce the risk of privacy breaches.

Poor RIM practices can negatively impact your ability to:

- Respond to requests.
- Be transparent and accountable.
- Implement and maintain Open Data and Open Information programs.
- Ensure confidentiality and privacy of personal information.
- Meet legislative requirements.

Our experience has shown that staff that process requests under the acts face situations where they are unable to locate responsive records or are burdened with extensive search times that return multiple copies of the same record and can result in excessive fees to the applicant.

In Review Report 075-2017 and 076-2017, the IPC found that the RM of Blaine Lake (the RM) did not have proper records management processes in place to respond to access to information requests. The lack of an organized filing system resulted in an unreasonable fee charged to the Applicant. In the report, the Commissioner commented that "the RM did not have proper records management processes in place to respond to access to information requests effectively." The Commissioner recommended that the RM establish a records retention and disposal schedule and records management policies and procedures.

In Review Report 078-2016 to 091-2016, the Applicant received a fee estimate totaling $111,842.50 from the Global Transportation Hub Authority (GTH). The IPC found that the fee estimate was inappropriate as it was largely based on searching email archives, which would not have been an issue with effective records management policies and procedures in place. The Commissioner recommended GTH establish records management policies and procedures to ensure it is better equipped to handle access to information requests.

In each of these cases, a significant misunderstanding of or a failure to apply good RIM practices directly impacted the public body's ability to meet its obligations under the acts.

In Investigation Report 072-2018, the Commissioner reviewed the Ministry of Central Services (the Ministry) use and management of backup tapes. In this report, the Commissioner found that the data residing on the backup tapes is not the "primary record," as the data is a copy of data that already exists elsewhere. As such, with some exceptions, backup tapes do not need to be included when conducting a search for responsive records related to an access to information request. The Commissioner made a number of recommendations to the Ministry on the management of the backup tapes, including recommending the Ministry establish an internal retention and disposal procedure for backup tapes.

For more information on searching for responsive records, consult our resources: *Checklist for Searching for Personal Health Information* and *Responsive Records Search Checklist*.

BASIC RIM CONCEPTS

Understanding records

For the purpose of this guide, we will use the term 'record' as it is defined in the acts:

> **Record** is defined at subsection 2(1)(i) of FOIP/2(j) of LA FOIP as "a record of information in any form and includes information that is written, photographed, recorded or stored in any manner, but does not include computer programs or other mechanisms that produce records."

Records can be emails, text messages, visual representations such as photographs, illustrations or maps, audio or video recordings, and data in any form. Consequently, RIM practices must address records in all their potential forms and media.

A challenge of introducing RIM practices to the public body is ensuring that staff understand the breadth of the term 'record.' Staff that deal solely with data, electronic files or other formats of materials must deal with their records in a similarly regimented way as staff dealing with traditional paper files.

Provincial government institutions must define a public record (also referred to as an official record) in accordance with *The Archives and Public Records Management Act* and manage it in compliance with this act.

The information lifecycle

The **information lifecycle** refers to the various stages that records go through from their creation or acquisition to their final destruction or archiving. It is important to remember that access and privacy laws apply to records at any stage of their lifecycle. As a result, it is necessary to ensure that your RIM practices address each stage to protect and preserve valuable information.

Briefly, the information life cycle is:

1. **Creation and Collection:** This is the birth of a record. At this stage, a record is either created or collected. This can include several different types of records, such as drafts, research materials, and final versions of documents, data or analytics.

2. **Use and Maintenance:** Once a record has been created or collected, it enters this stage. Use and maintenance is typically focused on preserving records to ensure they remain

accessible, legible and searchable. Their authenticity and integrity are preserved until they are approved for disposition.

3. **Disposition:** When a record is no longer useful, it will either be retained permanently (archived) or destroyed. The decision to archive or destroy the record will be based on historical assessment and evaluation of the record.

Generally speaking, records with a short-term value will be saved for a defined period of time before being destroyed, while records with a long-term value will be retained for a longer period and may be archived. Records that are deemed to be of no lasting value, such as transitory records, will be destroyed.

The method of destruction will vary depending on the sensitivity of the information contained within the record. For example, a publicly available newsletter may simply be recycled, whereas a document containing personal information or personal health information would require a secure destruction in accordance with records disposal policies.

The Provincial Archives of Saskatchewan produced the document *Saskatchewan Records Disposal System*, which outlines the disposal process for official government records. Local authorities may want to consult the Ministry of Government Relations' document, *Records Retention and Disposal Guide*, for more information on retention, disposal and secure destruction of files.

RIM BEST PRACTICES

The following RIM practices are commonly accepted best practices but are not exhaustive. The intention of this section is to provide public bodies with a high-level overview, rather than a detailed description of how to implement different RIM practices.

It must also be noted that no single approach will be appropriate for every public body. Some of these practices will need to be modified to meet specific needs, and some may not be appropriate at all.

The IPC recommends that you work closely with your public body's RIM staff in the development of practices that meet your public body's unique needs and situation. Provincial government institutions should consult the Provincial Archives of Saskatchewan to ensure compliance with provincial government RIM requirements. If your public body does not have dedicated RIM staff, consider designating a team or engaging with external consultants to investigate these options and develop an implementation plan.

Review and understand your public body's requirements

It is important to fully understand the recordkeeping rules that currently apply to your public body. Public bodies should ensure they consider any legislative requirements, bylaws, policies or procedures related to records management or retention. For example, government institutions, as defined by FOIP, are required to meet the obligations of *The Archives and Public Records Management Act*. For additional guidance on records management practices, government institutions can also refer to the Provincial Archives of Saskatchewan resource *Basic Records Management Practices for Saskatchewan Government*. Another example is *The Municipalities Act*, which requires that municipalities - considered local authorities pursuant to LA FOIP - establish a records retention schedule.

Implementing records retention schedules, policies and procedures are important to ensure the access to information and privacy rights of individuals are met. In consultation with your legal and RIM staff, review all existing requirements and how they have been implemented within your institution before considering new plans and RIM activities.

Develop safeguards

The information maintained within records will vary significantly, and as a result, not all records will require the same degree of protection. For example, personal information or personal health information must be protected from any unauthorized collection, use or disclosure. As a result of the requirements to protect personal information and personal health information, records that contain such information may require greater safeguards than others.

Personal information, however, is only one form of information that may require special measures. The public body may maintain records that are sensitive for other reasons. Consider, for example, law enforcement records that form part of an active investigation. The disclosure of this information may impede an investigation. Another example is location information for species at risk. The disclosure of this information could result in harm to an endangered species.

In order to effectively protect sensitive information, the public body must know where that information is held, who may access it and under what circumstances. You can start by developing sensitivity classifications for your records and assign appropriate safeguards for each sensitivity level.

When implementing RIM practices and policies, it is essential to develop accompanying safeguard requirements. Records that contain personal information or personal health information require several security controls. The acts require that public bodies have administrative, technical and physical safeguards in place to protect personal information or personal health information:

- **Administrative:** policies that reflect who is permitted access to sensitive records and what they may or may not do with that information. For example, information that is highly sensitive may only be viewed by specific individuals who need the information to conduct their work. Alternatively, information that is deemed non-sensitive may be accessed and used broadly.
- **Technical:** access controls that can be built into information systems. Some examples of technical access controls are password protection, encryption and secured shared drives.
- **Physical:** physical controls that can be implemented to protect records. These controls may be as simple as maintaining locks on file cabinets containing sensitive information, or more complex measures, such as key card access to specific locations within your office.

In addition to safeguards, consider data minimization and need-to-know at all stages of sensitive information handling. **Data minimization** refers to the practice of limiting the collection, use or disclosure of personal information and personal health information to only what is necessary. **Need-to-know** refers to the practice of making personal information and personal health information available only to those individuals in an organization that have a legitimate need-to-know that information for the purpose of a program or activity of an organization. These practices can greatly assist public bodies when responding to access requests. Where possible, the public body should avoid the unnecessary collection of any personal information and personal health information.

However, if it is necessary to collect or create records containing personal information and personal health information, design your records to ensure the specific information is easy to remove. For example, where feasible and appropriate, personal information being collected should have a designated section on the application form. Personal information or personal health information in databases can be kept in separate tables from other data, or documents that include personal information. This will make it easy to redact information should it be exempt from disclosure under the acts. This approach can be applied to any record containing personal information or personal health information or other information that the public body deems as sensitive or confidential in nature.

Design with access and privacy in mind

When public bodies implement or plan to implement new information systems or technologies, it is essential that these tools be capable of functions that support access and privacy obligations under the acts. When a system is not capable of simple extraction, the costs associated with an access or correction request may ultimately come at the expense of the public body. Likewise, the lack of extraction capability could prevent the appropriate destruction or archiving of records, leading to potential privacy and access issues.

In Investigation Report 262-2017, my office was prevented from conducting a full investigation and reviewing relevant records. The Ministry of Social Services (Social Services) advised my office that they believed the Ministry of Central Services (Central Services) was keeping their official records on back up tapes, so they did not appropriately retain and store official records within their own records management system. After consulting with Central Services, Social Services determined that retrieving the email records from the backup tapes would be too costly and time-consuming; therefore, they were unable to provide my office with the pertinent records. The Commissioner recommended that Social Services develop an email management policy or procedure and work with the Provincial Archives of Saskatchewan to develop a records retention schedule to ensure compliance with *The Archives and Public Records Management Act* and ensure records are accessible for the purposes of FOIP.

Consult with access and privacy staff, records management, legal and information technology staff before implementing a new system. The following may be taken into consideration when implementing a new system or technology:

- Conduct a privacy impact assessment (PIA) to determine whether the risks outweigh the benefits and if all access and privacy legislation is being met. For more information on PIAs, consult our resource, *Privacy Impact Assessment: A Guidance Document*.
- Determine if the system is compliant with your jurisdictional RIM requirements.
- Determine goals and objectives of the system or technology. Determine what needs to be collected to reach the desired outcome.
- Determine the structure and format of the data. For example, structured or unstructured fields.
- Determine if training will need to be done. Will the vendor demonstrate to the staff, or will simple on-site training be done?

- Following implementation, test the system. Are all access and privacy expectations being met?
- Determine when updates and maintenance should be completed.

Systems or databases that contain personal information or personal health information must be capable of allowing users to access and correct that information or add a notation where a correction request is denied to enable compliance with the acts. Systems and technology must allow users to access, extract and correct the information within the system. The systems also have to ensure that records are retained in a manner that protects their integrity and authenticity and that RIM practices including disposal procedures compliant with jurisdictional RIM requirements, can be implemented.

Failure to address access and privacy issues at the system design stage may result in greater costs, in both time and resources. Information technology professionals, as well as procurement professionals involved in the acquisition of information technologies, must understand the RIM, access and privacy requirements for any new system.

Designate staff as records management personnel

In large offices where many staff perform a variety of functions, it can be challenging to determine who is responsible for individual records. This challenge may grow over time, as staff change positions or leave the public body. This can become especially problematic when access requests are received. If records have been abandoned, it can be extremely difficult for staff to identify the appropriate individuals and offices to conduct a search. Designating staff as records management personnel can help to address this issue.

Records management personnel are individuals or a group that is responsible for maintaining specific records or types of records. Depending on the nature of the records and the size of the organization, records management personnel may be an individual, a work unit, or even a large branch. However, it is a best practice to identify a specific position or group that is most familiar with the records to be responsible for carrying out maintenance actions and responding to requests regarding the records.

When records management personnel for the public body have been identified, document the designation and make the document accessible to others in the public body that may need to know. This can be done in several ways, depending on the types of record. For example, consider using metadata. Metadata is descriptive information about a data set or record which can easily include contact information for the responsible records management personnel. For some types of records, it may be appropriate to designate records management personnel in job descriptions, file plan documentation or simply as a note on a shared drive. It is important to remember to keep this information up to date, changing designations and contact information as necessary. The key point in designating records management personnel is to ensure that records are appropriately managed and maintained over time to prevent records from being mishandled, lost or forgotten.

Develop and implement records schedules

Records schedules are tools that assist public bodies in classifying, managing and disposing of their records. Schedules consist of a classification system to facilitate the systematic organization of records and a retention portion which establishes time periods for which records must be kept to meet all requirements. The retention portion also facilitates the disposition process.

These schedules are an essential component of any RIM strategy and must form part of the policies and procedures used to implement that strategy.

FOIP and LA FOIP do not specify retention and destruction periods. Therefore, public bodies that do not have a records retention schedule implemented or are unsure if they have any legislative requirements related to records retention, should consult with their RIM and/or legal staff. Some considerations for public bodies when implementing records retention and disposal schedules include:

Government Institutions (within the meaning of FOIP)

- *The Archives and Public Records Management Act*, section 21, states that the Legislative Assembly, Legislative Assembly Service, every Officer of the Legislative Assembly, government institutions and the courts must preserve records in their possession until transferred to the Provincial Archives of Saskatchewan or destroyed based on an approved records schedule.
- Check out the Provincial Archives of Saskatchewan's resource, *Records Retention and Classification Schedule Development Guide* for information regarding the schedule development process.

Local Authorities (within the meaning of LA FOIP)

- *The Municipalities Act*, section 116, and *The Cities Act*, section 90, state that the municipal council must establish a records retention and disposal schedule for all public documents. These acts also state which public documents must be kept permanently such as meeting minutes, bylaws, cemetery records and annual financial statements.

- *The Education Act*, section 369, obligates the board of education to preserve all public documents of a school division or school community council until the disposition of the records is determined by the board of education or the minister.
- Municipalities, school boards and some other local authorities can contact the Provincial Archives of Saskatchewan to request historical appraisal of material prior to its disposal to select historically valuable records for transfer to the Archives.

Keep up with retention schedules

Establishing records retention schedules is an excellent first step in developing a RIM strategy, but to be fully effective, the schedules must be implemented and followed. As a starting point, train all staff on how to apply retention schedules to their records. This is particularly important for records management personnel who will be responsible for maintaining the records and ensuring that they are appropriately handled at the end of their lifecycle.

Once implemented, staff will need to periodically review holdings to find records that have exceeded their retention period and can be disposed of. Any records that are not accessed regularly can be moved to offsite storage where they are retained until they are eligible for disposal. Detailed inventories of records must be maintained. Records must be disposed of in accordance with the applicable records retention schedule following a well-established and well-documented disposal process.

The following tips can help your public body keep up with retention schedules and ensure that records are destroyed or archived properly. Provincial government institutions should refer to the Provincial Archives of Saskatchewan website for further information concerning schedule implementation and records disposal.

1. Maintain detailed records inventories that include the dates the records are eligible for disposal and the appropriate schedule designations. This will allow records management personnel to quickly see which records have exceeded their retention period and what the next steps will be.

2. When large volumes of records are meeting their retention period at the same time, schedule reminders for staff.

3. Schedule regular record clean-up. This could be a large annual event or a smaller weekly task. Determine what kind of schedule works best and ensure that you keep up with the required schedule.

4. Identify transitory records and non-records and ensure they are destroyed in a consistent and regular manner.

Remember that records may be responsive to access requests if they are in the possession/custody or control of the public body. When staff are conducting reviews, it is important to remember that any records that are responsive to a request or subject to a litigation hold must not be destroyed. Ensure that staff consult with your public body RIM, legal and access to information departments and the Provincial Archives of Saskatchewan before destroying records.

Transitory records

Public bodies create and collect a large variety of records, but not all these records have ongoing value. Consider, for example, emails or posters about internal social events, or multiple copies of a report. While these records serve a short-term purpose, such as informing staff of a bake sale, or distributing copies of a report to many people, they do not serve any significant business purpose to the public body or to the public. Records such as these are called 'transitory' meaning that they are only useful for a short and temporary amount of time. These types of records may be used for simple tasks and have their own records retention schedule that allows them to be destroyed.

In developing and implementing RIM practices, it is vital that public bodies clearly define the difference between transitory records and non-transitory records and establish protocols for deleting transitory records. When an access request is received, staff may need to search through a multitude of record holdings. This task can be made significantly easier if transitory records are destroyed appropriately.

The following considerations can help public bodies define transitory records:

1. Was the record produced by your public body?

2. Does the record document your public body's business? If the record contains information pertaining to your work, it is more likely to be a record that should be kept. If, however, the record pertains to internal social events, or external news clippings, it may not have a lasting value.

3. Are there multiple copies of the same record? It is important to save the official copy of a record, but duplicates may not be needed.

Transitory records should be kept only for as long as they are needed. Destruction of transitory records that no longer have value reduces the amount of material being stored and the resources associated with storing and searching through unnecessary records. In addition, transitory records are subject to access to information requests and legal holds. For these reasons, public bodies should destroy transitory records on a regular basis. For more information on transitory records, check out the Provincial Archives of Saskatchewan's *Guidelines for the Management of Transitory Records*.

Email management

As described above, records can be in any format. Even though email is one of the main forms of business communication, many people see emails as inherently transitory. However, business decisions, key communications, and important information are regularly shared by email, and as a result, emails must be managed as any other record in accordance with the public body's policies, legislative requirements and records retention schedules.

Managing email records can be challenging, especially given the volume of emails received and sent. The following tips can help public bodies and their staff organize and manage their email records:

1. Email messages that qualify as business records should be saved to shared repositories or other storage associated with the file in the institution's internal records keeping system. Determine what format will best suit your access and privacy needs and meets your RIM requirements and ensure that the format is stable and difficult to alter.

2. When possible, avoid sending attachments. Rather, send hyperlinks to records in shared repositories to ensure that recipients have the most up-to-date version and to prevent potential inadvertent disclosure.

3. Create folders within your email to organize emails into relevant subjects for your reference purposes. This can help keep inboxes manageable and may assist with workflow. Emails that are official records should be transferred and captured in your institution's internal records keeping system, ideally along with records they relate to, where they are retained in accordance with an approved records schedule.

4. Keep subject lines short and clear, using consistent naming conventions when possible. This will help both you and the recipient find information and quickly identify relevant emails.

Consult the Provincial Archives of Saskatchewan's *Email Management Guidelines* for more information and best practices for managing business emails. The IPC has also created a guide for the management and best practices of emails called *Best Practices for Managing the Use of Personal Email Accounts, Text Messaging and Other Instant Messaging Tools*.

The following are examples of IPC reports issued on email management:

In Review Report 301-2017, 302-2017, 303-2017, 304-2017, 003-2018, the Commissioner found that the Ministry of Central Services (the Ministry) did not have an electronic filing system for the storage and organization of emails. The Commissioner recommended the Ministry develop an email management policy or procedure to ensure emails are managed in the same manner as any other records.

In Review Report 035-2018, the Commissioner found the RM of Manitou Lake (the RM) had not made a reasonable effort to search for email records. The Commissioner made several recommendations regarding the management of email records including undertaking a records management project to ensure emails stored in council members' email accounts are saved into the RM's central records management system and recommending the RM implement an email management policy.

Storage of electronic records

While records are in active use, they should be stored in a secure manner that allows for ease of access by authorized individuals. This is essential for responding to access requests as it can significantly reduce search time and resources. Shared drives, electronic records management systems or other shared organization storage resources are recommended, as they allow public bodies to set access controls and limit access to authorized individuals. When individuals save records on their assigned work computers or within their email or text messages, it is easy for those records to be lost should the computer break down, become lost or stolen or individuals leave the public body.

Shared storage resources should have automatic back-up to prevent inadvertent loss of information. In addition, they should have security controls that allow only authorized individuals to access information. For example, access to a shared drive may be appropriate for members of a work unit or department but not for other members of the public body. Alternatively, sensitive or personal information or personal health information may require that only specific individuals or management have access.

File naming

File names are an important tool to help staff find information, especially in the context of an access request. However, when working on materials that are familiar to us, we tend to use vague titles. While one staff member may easily recognize what "letter.doc" is, other staff will have to open the file to determine what the file actually is. In the context of an access request, this can result in significant search time and associated fees.

Implementing file naming conventions throughout a public body can standardize the way that staff save and file records and help ensure that materials can be easily searched for and accessed. File naming conventions do not need to be complicated to be effective. Rather, they should capture the minimum amount of information necessary for staff unfamiliar with the file to access it using a standard search.

Public bodies will need to consider the types of information that is necessary to easily identify records, but there are a few elements that are recommended:

- The date the record was prepared.
- A descriptive title. For example, rather than simply naming a document "New Practices," a more descriptive title could be "RIM Practice Guidelines."
- A version number as it can be easy to become confused when there are many versions of a record. Adding a version number can help ensure that staff are accessing the most current materials.
- Volume numbers if multiple files for a particular subject exist.

For more information concerning naming conventions, refer to the Provincial Archives of Saskatchewan resource *Naming Conventions*.

Entry and exit protocols

As staff move between positions and public bodies, it is easy for records to be lost, mishandled or destroyed inappropriately. Developing protocols for when staff start or leave positions can help prevent the loss of valuable information, as well as protect your public body from privacy breaches.

For staff entering a new position, ensure that they are made aware of the following:

- What records their position is responsible for maintaining.
- The RIM standards in place and how to apply them.
- Any mandatory or voluntary RIM training that is available.

- How to access and use shared organization storage resources.
- Who the contact is for questions about RIM.

For staff exiting a position, it is important to ensure that records created or maintained during the individual's tenure are appropriately saved, securely destroyed or transferred to a replacement. Have the departing staff member or assigned staff member verify that the following is completed prior to their departure:

- Records have been stored, transferred to an archive or destroyed based on their retention schedules following required disposal procedures.
- Personal non-work-related information that may have been stored on a computer or in paper files has been destroyed.
- Email records and text and picture messages have been appropriately saved in your institution's records keeping system or destroyed as per your public body's disposal requirements.
- A list of all records that the individual is responsible for maintaining has been prepared for transfer to the new records management personnel.
- Passwords for protected files or storage media have been reset and transferred to the new records management personnel.

Managers are responsible for ensuring that departing staff have completed all RIM requirements and should take steps to verify their completion.

Create a duty to document

As was seen above, records can be in any format. However, in some cases, important information is conveyed without the creation of a record. Business or policy decisions are sometimes made in meetings, over the telephone or in other settings that do not automatically create a lasting record (such as over instant messaging programs). When these decisions or actions are not recorded, public bodies may not be able to meet their access and privacy requirements. As such, public bodies should develop a policy requiring staff to document business or health service-related activities, including a duty to accurately document key decisions and actions.

In addition, it is important to ensure that staff use appropriate communication tools for business information. In our resource, *Best Practices for Managing the Use of Personal Email Accounts, Text Messaging and Other Instant Messaging Tools*, we also recommend that public bodies prohibit the use of non-public body email accounts or instant messaging for conducting business or health services.

Implementing a requirement to document decisions and actions requires the development of policies and training for staff so that they will fully understand what information should be recorded and how to manage it.

Consider developing templates for use in specific situations, such as meeting notes or pre-developed nursing forms. Training on how and when to appropriately use these templates may help ease the transition for staff accustomed to making informal and undocumented decisions.

Ongoing training

Initial training on RIM practices is essential. It will provide your staff with a strong basis upon which to build additional knowledge and skills. However, for long-term practice changes to take root, the lessons must be regularly refreshed and reinforced. Invest in a training program that allows staff to re-visit training materials and help them to understand RIM concepts and implement changes in their own work. Remember that the success of your RIM program is in the hands of your staff. Make sure that they have the resources and assistance that they need.

Review and audit

Implementing strong RIM practices should be a long-term goal. Do not expect quick and easy fixes. Staff are accustomed to their own filing and RIM practices, so changing habits can take a long time. As with any change, it will take time, patience and regular reinforcement.

To help keep staff accountable for maintaining RIM practices, it is highly recommended that public bodies include regular review and monitoring of RIM practices in their ongoing plans. In addition, including RIM actions and targets in annual performance plans will help keep staff engaged and accountable.

CONCLUSION

By implementing RIM best practices, public bodies can vastly improve conditions for accessing information. Information that is appropriately created, managed and stored is eminently easier to find and use. In addition, following a well-documented disposal process regularly provides accountability for disposed information and reduces volume of information to search. Access requests can be processed with greater ease and efficiency. Staff time associated with record searches can be significantly reduced. Risks associated with failure to provide responsive records or with failing to meet the required response timelines can be avoided. Ultimately, a comprehensive RIM plan can help public bodies to be more agile, efficient and accountable to the public.

Implementing RIM policies and practices can be challenging. Institutions, departments, and individuals in a public body should establish effective procedures to manage their records over time, to engage staff and change ingrained habits. When preparing to develop and implement new or improved RIM practices, remember the following:

1. **Compliance**: Make sure you follow RIM legislative requirements applicable to your public body.
2. **Be engaged**: Senior management should understand the importance of RIM practices to the legislated obligations of the acts and actively support the efforts to introduce or update RIM practices in your institution.
3. **Communicate often**: It is essential to keep RIM practices top of mind to ensure that staff don’t slip into old practices.
4. **Communicate clearly**: Communication and training on RIM should be clear and straightforward, using plenty of examples and real-world scenarios so that staff can fully understand their responsibilities and how to implement new practices.
5. **Commit to maintaining practices over time**: Implementing RIM practices is not a simple one-time event. It takes time and dedication to ensure that best practices become everyday practices.

Office of the
Saskatchewan Information
and Privacy Commissioner

503 – 1801 Hamilton Street
Regina SK S4P 4B4
306-787-8350

www.oipc.sk.ca