A Handbook on Information Management best practices for University of Ottawa employees

Information Management HANDBOOK

University of Ottawa Information and
Archives Management Service

Table of Contents

Information Management at the University of Ottawa

Purpose

This Handbook is to help all University of Ottawa employees understand information management best practices applicable to the information created and collected over the course of daily operations. Information Management principles as well as roles and responsibilities are outlined in Policy 23-Information Management.

This handbook will also help ensure that the University's information, regardless of format, is effectively managed throughout its lifecycle.

What is Information Management?

The ability for an organization to capture, manage, preserve, store, and deliver the right information to the right people at the right time.

Why is Information Management important?

Benefits of good Information Management

Information is a strategic asset for the University of Ottawa. By practicing strong information stewardship, the University promotes institutional transparency, openness, accountability and excellence in support of its academic, research and administrative activities.

Information comes in many different formats including paper and electronic, blogs, publications, books, magazines, photos, maps, objects, emails, web pages, databases, telephone conversations, text messages, instant messages, videos and more.

Effectively managing information allows us to:

- Locate and retrieve reliable information efficiently;
- Provide services in a timely manner;
- Make sound, evidence-based decisions,
- Be transparent about decisions and operations;
- Protect the rights and interests of ourselves as well as the University;
- Minimize risk to the University such as information loss;
- Ensure the continued protection and security of information;
- Comply to applicable policies, legislation, and standards; and
- Reduce costs and maximize use of physical space.

We all have a role to play

Every day, we all create, collect, use, and share information that supports and provides evidence of our decisions and activities. Because of this, we are all responsible for effectively managing the information that is under our control. By applying these practices and procedures to your work, you will begin to find that your work becomes much more efficient, and the information you need will be readily available and easy to share with your colleagues and stakeholders.

A Note on Digital and Electronic Information

Digital and electronic information is increasingly becoming the primary piece of evidence of transactions at the University. Additionally, many hard copy documents are being converted to digital format. Advantages to digital information include ease of sharing, less physical storage space used, ease of search, retrieval, access and editing, etc.

Digital and electronic records are no different from paper records. They must be created, used, classified, stored, and retained the same as paper records. The value of information for evidential, legal, or historical purposes dictates how it should be managed, not its format.

As digital information slowly replace paper as the primary record, some requirements must be met.

Digital and electronic records must be created, classified, stored, and retained the same way as paper records.

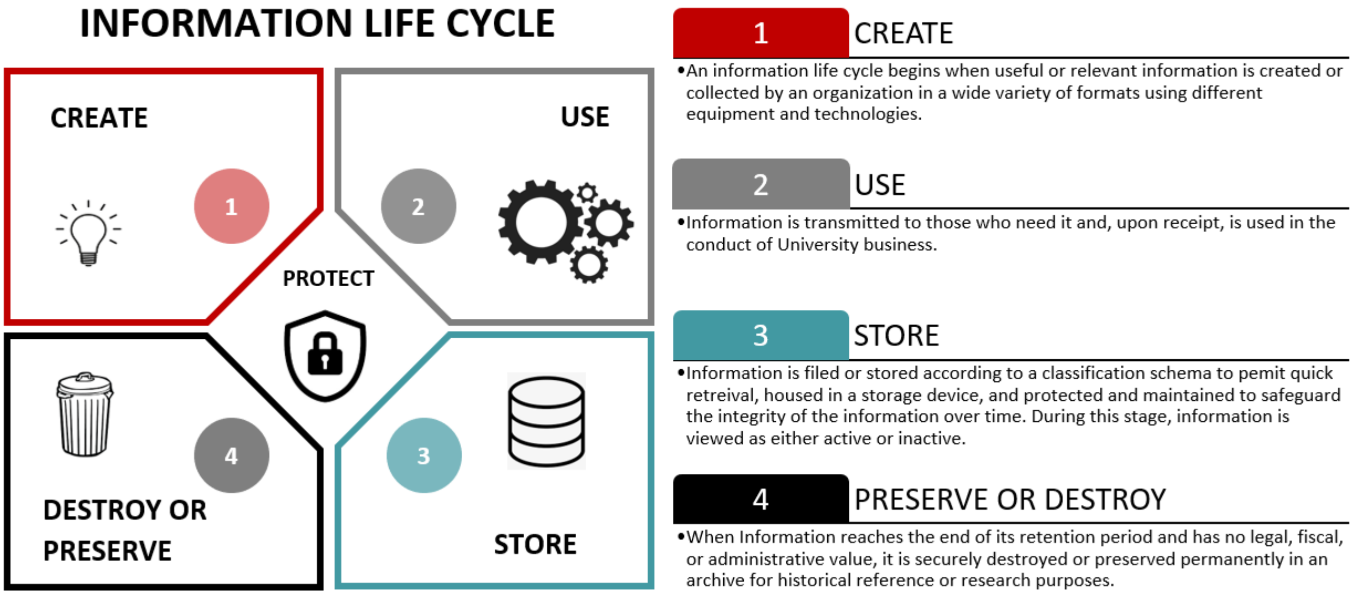
We must take into consideration:

- the authenticity of the information,
- the integrity of the system the information is stored in,
- and that the information was created "in the usual and ordinary course of business"[1].

Appropriately, classifying and retaining only necessary digital and electronic information makes access and retrieval as well as long-term preservation much easier and much less costly.

Information Life Cycle Management

Information must be managed at all stages, from creation, to use, storage, and ultimate disposition or long-term preservation.



- An information life cycle begins when useful or relevant information is created or collected by an organization in a wide variety of formats using different equipment and technologies.
- Information is transmitted to those who need it and, upon receipt, is used in the conduct of University business.
- Information is filed or stored according to a classification schema to pemit quick retrieval, housed in a storage device, and protected and maintained to safeguard the integrity of the information over time. During this stage, information is viewed as either active or inactive.
- When Information reaches the end of its retention period and has no legal, fiscal, or administrative value, it is securely destroyed or preserved permanently in an archive for historical reference or research purposes.

Figure 1[2]

[1] "Electronic records as documentary evidence" CAN/CGSB-72.34-2017, Canadian General Standards Board

[2] Adapted from: Memorial University, *What is Information Management*, https://www.mun.ca/cio/imp/whatisim.php

Following off the Information Life Cycle diagram above, this handbook outlines some key information management guidelines and practices. Begin making a habit of these while you manage the information in your custody.

CREATE: Creating and collecting information

Anticipate information management needs

Anticipating the information management needs of the information you create BEFORE you create it will set you up for successful information management, as you continue to manage this information to the end of its life cycle. Keep in mind that the information created or received during the course of an employee's administrative activities is the property of the University. We should all ensure that when we create information, we are creating **quality**[3] information. This means information where its integrity, reliability and authenticity can be guaranteed.

TOOLKIT

Naming Conventions

What to keep?

What can I delete?

Policy 117

Naming

Consistency is important when saving information. This allows for quick and easy retrieval. To do this, apply proper *naming conventions* when saving information. Re-name information you receive so it fits with the naming conventions.

Determine its Value

As you create and collect information, identify its value to the University and manage it accordingly.

Information of strategic and operational value should be handled, used, shared, and stored with particular care. Consult the best practice *"What to keep?"* to determine how to identify what has strategic and operational value and how to manage it throughout its lifecycle.

Strategic and operational value: Enables and documents **decision-making**, and supports **reporting, performance, legal, and accountability** requirements.

Not all information needs to be handled, used, or stored as information of strategic and operational value. Information that helps us in our day-to-day operations in the short-term, but does not provide evidence of policy, decisions or obligations, is considered transitory. Read the best practice *"What can I delete?"* to help determine what information is not of strategic and operational value, and how to manage it accordingly.

TRANSITORY
Temporarily useful, with **no ongoing value** beyond an immediate and minor transaction.

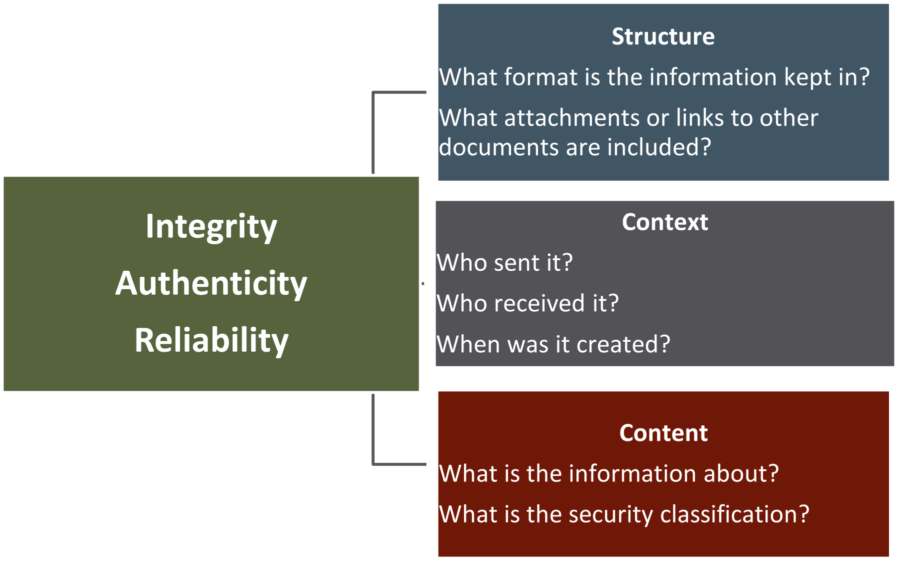
[3] IM Policy 23

Assign Security Classification

When we create or collect information, we must keep its security in mind. Use the classifications *public, internal, confidential, and restricted* from Policy 117. Assigning security classification as soon as the information is created or collected will ensure that they are secured, protected, handled, and shared appropriately throughout their life cycle.

Structure, context and content

Keeping the structure, context and content of information together preserves its integrity, authenticity, reliability, and value, and makes it easier for future accessibility.



Integrity

Authenticity

Reliability

Structure

What format is the information kept in?

What attachments or links to other documents are included?

Context

Who sent it?

Who received it?

When was it created?

Content

What is the information about?

What is the security classification?

USE: Using and sharing information

This is the most complex stage of the information lifecycle. While you are using, sharing, and distributing information, maintaining its accuracy, reliability, integrity and confidentiality is key. We, as employees, are responsible for safeguarding the information as we use it on a day-to-day basis.

Versions

When using information, it is important to use the most up-to-date, authentic, and reliable information possible. Identifying the most current version of an information resource will ensure that its reliability is preserved.

If you use a system such as Docushare or SharePoint to store your information, version control is integrated in the system and managed for you.

TOOLKIT

Accessible formats

Naming convention

File sharing best practice (coming soon)

Instant messaging best practice

One Note best practice

Audio and videoconference best practice

What can I delete?

Policy 119

LiquidFiles

If you do not use a system such as Docushare or SharePoint, then you are responsible for managing version control. Indicate versions as v01, v02 at the end of the file name. The file with the highest number is therefore the most recent version. Where applicable DRAFT and FINAL should be indicated at the end of the file name.

When making changes, edits or additions, always keep in mind that the structure, context, and content must remain intact so the value of that information is preserved.

REMINDER: Check out the *"What Can I Delete?"* best practice for more on deleting drafts.

Sharing and collaborating

Collaborating with colleagues and stakeholders is an important part of our day-to-day activities. Various tools and systems exist to allow for this type of collaboration across campus. Tools such as Office 365 (OneDrive, Teams, SharePoint, etc.), email and instant messaging applications, are just some of the products available to employees.

Do not share personal information over collaboration platforms. Use a secure means of transmitting information such as LiquidFiles.

We should all ensure that the information we create and keep in these systems is managed according to its value.

Following best practices for each of these tools will ensure that information of strategic and operational value is handled and stored appropriately, and that transitory information is disposed of in a timely manner.

Social Media

Social media platforms are becoming increasingly useful for distributing important information to a diverse audience. The same types of measures must be taken to ensure that any decisions or information of strategic or operational value are documented and managed appropriate to their value. We cannot rely on the social media platform to manage and preserve this information for us. To properly save information that is communicated through social media; please refer to the STORE section of this handbook.

Accessibility[4]

Information published and made available to the University community, as well as the external community, must be made available in accessible formats.

It is also good practice to keep accessibility in mind when creating, sharing, and distributing information. For more information on accessibility, please refer to Policy 119.

Accessible formats

- HTML and Microsoft word
- Braille
- Accessible audio formats
- Large print
- Text transcripts of visual and audio information

STORE: Classify and manage your information

Information that is well organized and stored in designated repositories will not only help you work better, but it will also support efficient and effective service delivery.

[4] https://www.ontario.ca/page/how-make-information-accessible

Where should I store information?

This depends on the value of the information. Information of strategic and operational value should be stored in a shared repository and must be filed according the classification plan.

Transitory information does not need to be stored in the designated repository, but should be managed and disposed of according to the best practice guideline.

How should I organize my information?

Information should be organized according to the *University of Ottawa General Classification Plan,* which is structured by common functions and activities.

Using a classification plan ensures that everyone within a unit stores the information in their custody in a consistent manner. This means that everyone will be able to find reliable, authentic information quickly.

TOOLKIT

What to keep?

What can I delete?

Docushare Guide

Classification Plan

Email management best practice

Email etiquette best practice

What about my emails?

Good email management includes classifying those with strategic and operational value according to the *General Classification Plan*. When you have identified that an email provides evidence of a decision, then you are responsible for storing it in the designated repository, according to the Classification Plan. Classification should be done according to the activity/function that the email relates to. This ensures that the information documented in the email will be retrievable.

Refer to the best practice on *email management* and *email etiquette* for more information.

HELPFUL TIP!

Integrate the General Classification Plan into your Outlook folders so that managing your emails is as quick and efficient as possible!

DESTROY OR PRESERVE: Final Disposition of Information

When information is no longer consulted on a regular or even semi-regular basis for operational needs, it is considered inactive. Some of it will need to be kept for a specific period of time, and some of it can be disposed of.

How long should I keep information?

Since not all information has the same value, not all information needs to be kept long-term. Information that is no longer needed to support operational needs can disposed of when it has outlived its usefulness.

The Retention and Disposition Schedule dictates how long information needs to be kept, which unit is responsible for keeping the most complete copy, and when that information is ready to either be destroyed, or transferred to archives for long-term preservation. This tool also indicates if you, as an employee or unit, are authorized to destroy the information yourself, or whether destruction must be done through the official disposition procedure.

TOOLBOX

What to keep?

What can I delete?

Retention and disposition schedule

Policy 117

Archives management procedure (coming soon)

Access to the University archives procedure (coming soon)

Can I destroy information myself?

If your unit **is identified** as the Office of Primary Responsibility, meaning that you hold the most complete, master version of the information, then you **are not authorized** to destroy information yourself. Destruction of this information must go through the official disposition procedure.

If your unit **is not identified** as the Office of Primary Responsibility in the Retention and Disposition Schedule, and the versions you have are simply duplicates, you **are authorized** to dispose of it yourself.

As a general rule, employees are authorized to destroying transitory information themselves. Once you have determined that information is no longer needed for operational purposes and is not of strategic value, you may dispose of it. Read the best practice *"What can I delete?"* for more information.

Destruction of information should be done appropriate to its security classification. Consult Policy 117.

Where does information of long-term value go?

Information identified as having long-term value will be preserved according to the *Archives Management Procedure* (coming soon).

Access to information being preserved for long-term is governed by the *Access to the University Archives Procedure* (coming soon).

Other Important Best Practices

Protection of Information

We have an obligation to protect all information while it is in our custody and control. This includes protection from unauthorized access, discloser, distribution and destruction.

Classification of information is important because it identifies the level of security and protection required for each type of information, such as public, personal, confidential, or restricted information. More information can be found in Policy 117.

Working remotely

Before you take University Information with you, ask yourself if it is a necessary part of your job to take the information with you, or to access the information remotely.

Refer to Access To Information and Privacy Office's (AIPO) guidelines for more information.

Mobile Devices

Using mobile devices for work-related purposes is convenient, and often allows for more efficient and streamlined work processes. We must all, however, ensure that we are safeguarding the University information that is stored and accessible on mobile devices.

If you use mobile devices for your work, always follow these best practices:

- Avoid saving personal information directly on mobile devices.
- Use strong passwords to access University accounts and never share your passwords, do not use default passwords.

- Use biometrics (when the option is available) and limit the number of password attempts.
- Use the automatic lock feature so that a password is required to access information on the device.
- Use multi-factor authentication.
- Regularly update your device's operating system (Ex. iOS for Apple).
- Do not install unknown or suspicious programs or applications, and limit the information that they can access.
- Install anti-virus or anti-malware applications.
- Only connect using trusted Wi-Fi networks. If you do need to use a public network, use a Virtual Private Network (VPN) service.

Position Change/ departure

Leaving your position

In today's work environment, it is not unusual for employees to change jobs quite often during their career or simply retire. This trend can actually have a significant effect on how well we manage our information resources. Whatever the situation, you must ensure to properly manage the information.

Information created or collected during the course of an employee's administrative and operational activities are the property of the University.

When leaving your job, good information management practices, as outlined below, ensure that your colleagues can continue to access and manage the information and resources they need to do their jobs well. Regular attention to these activities (rather than waiting until you leave) will also help to minimize the stress often associated with a job change. It is recommended that you:

- Provide pertinent information about everything you leave for your successor, explaining why it will be needed.
- Remove all personal information from any shared and personal drives.
- Transcribe any business-related information of strategic or operational value contained in notebooks and place it into the shared repository.
- Properly destroy or delete all transitory records, consult the best practice *"What can I delete?"*.
- Ensure that information resources of strategic and operational value, in all format, are organized and filed according to the policies, standards, and procedures outlined in this handbook so that the information continues to be accessible to other employees. Consult with the Information and Archives Management Service to confirm the procedures.
- Ensure that files in your custody are transferred to the custody of another employee or to the appropriate repository.

Starting a new position

Starting a new position provides an opportunity to establish good information management practices right from the beginning. When starting a new position it is recommended that you:

- Check if any electronic and paper information resources of strategic and operational value have been transferred to your custody. Speak to your supervisor to find out if there is a list of these that can be provided to you.
- Take note of any instructions or messages you receive regarding access to electronic tools such as a shared drive and shared repository(ies).
- Familiarize yourself with your information management responsibilities and practices by reviewing the information in this guide. Contact the Information and Archives Management Service to obtain more information.
- The Information and Archives Management Service is available to help you make the transition to your new job.

Access to Information Request and Legal Hold

All information created and collected during the course of our activities is subject to *Freedom of Information and Protection of Privacy* (FIPPA) legislation. This includes all types of information. When you receive notification of an access to information request by AIPO, transfer responsive records located as a result of the search to AIPO. Refer to the AIPO's Website for more information.

The same principals apply to legal hold proceedings.

Once a request is received through a FIPPA or legal hold procedure, manipulation, alteration, falsification, concealment, and/or destruction of information relevant to these requests is strictly prohibited and illegal.

Questions? Concerns? More help/information?

Contact the Information and Archives Management Team

Website: https://www.uottawa.ca/archives/en
Email: archives@uottawa.ca
Phone: 613-562-5750

This Handbook is a living document and will be updated frequently as more tools are created and made available. Feedback and comments are strongly encouraged.

Appendix A: Definitions

Active information

Those records that are in frequent use (more than once a month) by the administrative unit in which they were created, received, or maintained. These are stored by the office using them.

Authenticity (of information)

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;
- To have been created or sent at the time purported.

Classification Plan

A classification plan is the systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods and procedural rules and represented in a classification system.

Disposition

Disposition means disposal of Records no longer needed for day-to-day operations by a Unit, through destruction, secure destruction, or transfer to the university archives.

Evidential value

Value of those records which are necessary to provide an authentic and adequate evidence of an organization's actions, functioning, policies, and/or structure. Evidential value relates to the document's creation and not necessarily to its content or informational about the activities, functions, and origins of its creator.

Historical value

Measure of the importance of a document (record) that justifies its permanent retention. Also called archival value, continuing value, or enduring value.

Inactive information

Those records that are no longer required for the day-to-day operations they once supported.

Information

Information means all information on any format including but not limited to hard-copy textual and electronic documents, structured data, graphic images, sound and video recordings, books, maps, drawings, photographs, and any other information that is written, photographed, recorded or stored in any manner.

Information Life cycle

Stage through which every (written or computerized) record goes through from its creation to its final archiving or destruction.

Integrity (of information)

Integrity refers to the reliability of information content, processes and systems as to its completeness, accuracy, consistency and authenticity

Legal value

Usefulness of a document or record as a legal proof of authority or business transaction, enforceable rights or obligations, or as the basis for a legal action.

Office of Primary Responsibility
The office that has primary responsibility for a category of records or holds the master/official file copy of any record. The OPR maintains the official master copy of the records in order to satisfy operational, financial, legal, audit and other requirements.

Reliability (of Information)
Reliability refers to the degree to which the quality of information content, processes and systems can be depended upon to be trustworthy, complete, accurate and authentic.

Retention and Disposition Schedule
A records retention and disposition schedule is a University document that guides the management of a record. It dictates how long the records need to be retained to meet operational and legislative requirements and authorizes the disposal of information either by secure destruction or transfer to Information and Archives Management.

Repository
Storage for indefinite or permanent placement.

Semi-active information
Those records that are infrequently used in day-to-day operations (less than once a month).