a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

University Archives
Irving K. Barber Learning Centre
1961 East Mall
Vancouver, BC V6T 1Z1

Records Management Office
Phone: 604 827 3952
Fax: 604 822 9587
alan.doyle@ubc.ca

Electronic Records Management Guidelines

Contents

Electronic Records Management Guidelines

The following guideline provides practical advice in the management of University electronic records. The document begins with the principles of electronic records management and then provides a methodology for implementation. It also refers to the management of shared drives and content management systems such as SharePoint and email. This document is the companion to GUI-0001 Electronic Records Naming Conventions and should be used in conjunction with it.

University Records Management Policy

Records created at the University British Columbia fall under University Policy #117. The purpose of Policy # 117 is to:

- facilitate the efficient management of the University's records through the development of a coordinated institutional Records Management program situated within the University Archives
- ensure records are created, managed, retained, and disposed of in an effective and efficient manner
- ensure preservation of the University's records of permanent value; and
- supports both protection of privacy and freedom of information services throughout the University

University Policy # 117 applies to all University officers and employees who create, receive or maintain records in the course of their duties on behalf of the University. The University Archives, in consultation with Legal Counsel and affected University departments, defines the **minimum** retention period that records must be retained. The University Archives provides coordination, guidance and recommendations on the proper management of records throughout their life-cycle.

General Records Management Principles

Management of University records should be defined, simple and defensible. This is achieved by using documented processes that are widely shared and understood by staff. The four key steps in the control of University records are as follows:

- Organize
- Manage and Secure
- Dispose

Organize. The organization of all records systems, paper or electronic, should mirror each other. Organize shared drives and/or other content management systems such as SharePoint according to the University's records classification system wherever possible. This can be achieved by:

- Folder creation based on University Classification System or
- Tagging content with the University Classification System
- A combination of both methods

Manage and Secure. After your unit has decided how records are going to be organized (either by using folders or tags or a combination of both), the first principle of organization should be according to

the University classification system. If sub-folders are necessary, use common activities and combine the year or some other organizational principle (such as a project number or name) whenever you can. Adding the year to the second level reduces the levels in the hierarchy and helps organise records for future retention. A simple folder structure would look as follows:

Example

FIRST LEVEL – RMO [Records Management Office]

SECOND LEVEL- 2015 Guidelines
2015 Projects
2015 SLAIS Projects
2015 Classification Development

Each unit should understand what documents they are responsible for retaining, the duration for which they must be retained, and what they can, and should, dispose of as transitory.

Office of Primary Responsibility (OPR). Each unit has operational responsibility for a unique set of records. Know what your unit has operational responsibility to keep and what records are retained for convenience. Convenience copies can be destroyed sooner than defined in the University Schedules because a more complete set of records is being retained by the OPR.

For example: Records management does not need to retain records regarding the University budget. If we were retaining those records it would be for **convenience only** and we could, and should, destroy them when no longer required. The office of primary responsibility for University budget would be Finance and they would be responsible for keeping the full and complete set of record.

Define Recordkeeping Responsibility. Responsibility for maintaining and removing records from the system should be identified otherwise the system cannot be said to be managed.

Unit Recordkeeper - A recordkeeper should be identified who will be responsible for the creation of the structure based on the classification system and to oversee maintenance of the records systems.

Project Recordkeeper - Special projects that may have a limited time duration where other recordkeeping systems may be used, such as SharePoint, a project recordkeeper should be appointed to ensure the records in these other systems are retained according to the system and to migrate records to the Shared Drives on an ongoing basis.

Staff - Responsible for filing both records and key email to the shared drive structure

Folder Security Units should create a folder access map to manage how security on their drives are maintained.

Dispose. Records retention and disposition is not automated at UBC. Individual units must manually remove electronic records that are no longer required according to the University schedules. Paper and electronic records that are scheduled for destruction should be done in tandem in order to prove that

the destruction took place in the "ordinary course of business." [i] All destruction of records must be done according to the record schedules.

Contact the Records Management Office for help in the destruction of records in either electronic and/or paper form.

Method to Organize and Manage University Records

Shared Drive Organization. Avoid creating a complex folder structure of folder within folder. The folder structure should be as flat as possible based on the function that the records support then the activity they detail. Creating folders on shared-drives also encourages user access through navigation of the folder structure. Clicking through a multitude of folder is frustrating when searching for information. Tagging content, on the other hand, does not rely on user navigation or folder creation to segregate information. User access is achieved through a search. Furthermore, if a document relates to two areas within the classification it can be tagged into two areas of the classification without having to be copied to into two folders. This creates better control over copies of records.

We recommend using a **combination of folders** for the highest level of classification then using an agreed system for **tagging content**. The same principle of using a combination of folders and tagging also holds true for Outlook records (see Email Management later in this document for more information.). Units should agree on when email will be stored on the shared drives (substantive[ii] emails that can and should be shared with the team) and when they can be retained in a single personal silo.

Example:

Level 1 – RMO

Level 2 – ADMINISTRATION

Level 2 – HUMAN RESOURCES
Level 3 **Awards2015**

Level 2 – RECORDS MANAGEMENT SERVICES – GENERAL

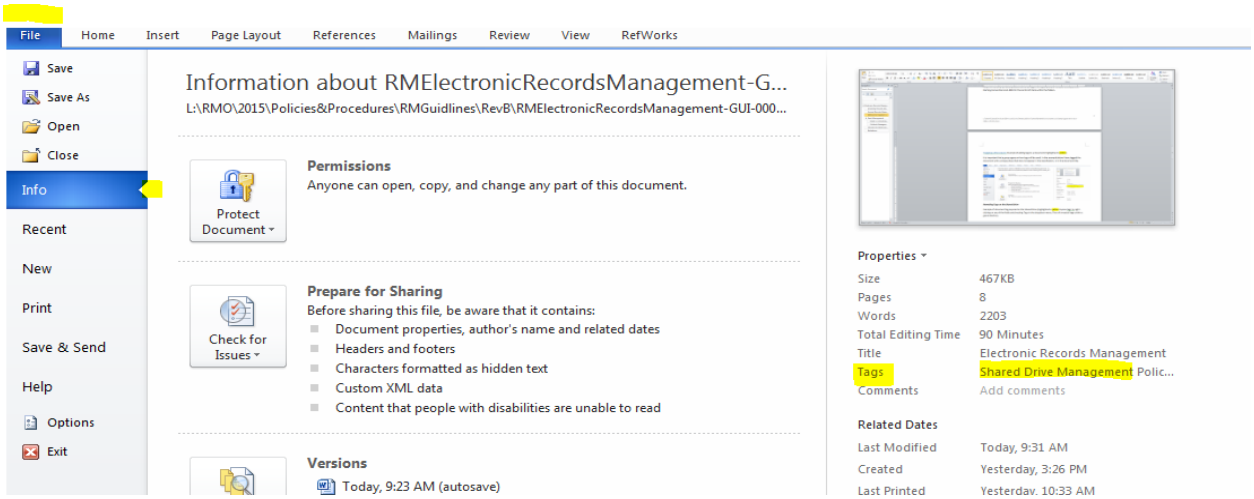
Level 3 **Classification**
Level 3 **Outreach** (organized by year and office)
Level 3 **Planning** (organized by year)
Level 3 **Policies and Procedures**
Level 3 **Projects** (organized by year & project name**)**

Level 2 – OFF-SITE STORAGE AND DISPOSITION SERVICES

It will not always be possible to create just three or fewer levels of folder hierarchy but an effort should be made to keep the hierarchy as flat as possible and to use tags where granularity is needed. See Electronic Records Naming Conventions GUI-0001 for the control of items within the folders.

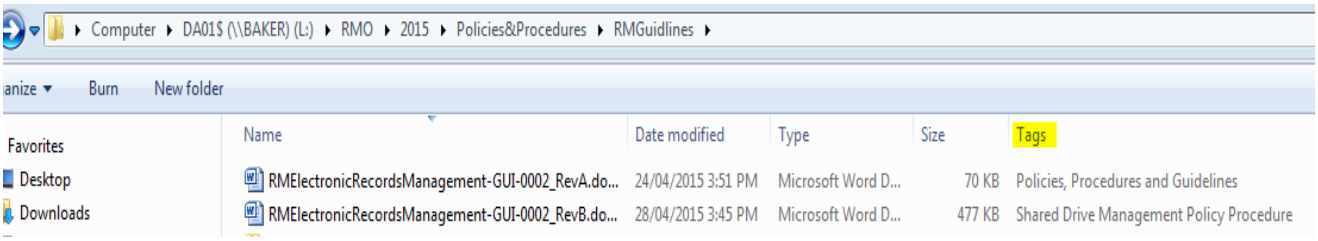
Tagging a Document. Example of adding metadata tags to a document (highlighted in yellow)

It is important that a group agree on how tags will be used. In the example the document is tagged with a **unique phase** that does not appear in the classification, or in the document title.



Revealing Tags on the Shared Drive

Example of document tag exposed on the Shared Drive (highlighted in yellow). Expose tags by right-clicking on any of the meta-data fields and choosing *Tags* in the dropdown menu. This will reveal all tags within a given directory. In the example below I have updated the tags from the first revision (RevA)of the document to the second (RevB).



Security of Shared Drive Folders. Some folders require different access requirements either because of Freedom of Information and Protection of Privacy legislation or administrative requirements. Access should be defined, mapped and managed by the unit and should employ a "risk based approach" as outlined by Risk Management.

http://riskmanagement.ubc.ca/personal-info/risk-based-universe-approach

Access to records should be the same between paper and electronic. It is not recommended that users create their own security on folders or documents, no password protected documents for example, unless the need for such security is defined and documented.

SharePoint Sites and/Content Management Systems. Unless a unit has defined their recordkeeping system in SharePoint or another transactional system,[1] units using such sites for team collaboration should always consider the Content Management system as a **copy** of what exists on the shared drive. Use the same method of organizing the libraries and naming documents on SharePoint as on the Shared Drive. Doing so will ensure that any bulk movement between systems is simple and seamless.

Be sure that any new or existing SharePoint site also has a named recordkeeper responsible for managing the site's permissions and documents.

Email Management

Use the same principles for creating and managing email records as you would for any other University record.

Email is a University Record

- Name the email according to the naming conventions defined for your unit. See *Electronic Records Naming Convention GUI-0001*
- Unless your unit is following a role-based system for email management - store substantive email on the shared drives in the appropriate folders[2]
- Keep attachments with the email
- Wherever possible do not issue native files but convert to PDF
- Store substantial **confidential email** on the shared drive in a secured folder if possible, if not possible document a plan for how confidential information will be retained

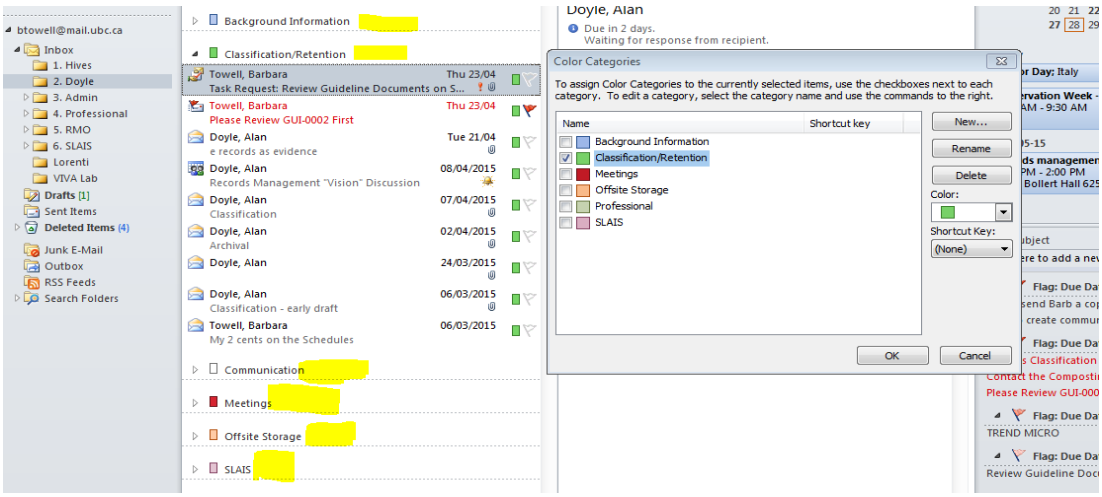
Outlook Management

- Delete Transitory (see definitions section at the end of this document) emails from your Outlook inbox on a daily basis
- If you must create folders within your email system retain them for **convenience only** (substantive emails should be stored on the shared drives)

Tagging Email Users can also use tagging to help organize content where further granulation is required. Instead of creating a complex hierarchy of folders within folders, I have tagged the content using *Color Categories*. In the example below transitory emails are organized by sender then tagged roughly based on the University Classification (called Category in Outlook). These are all working emails saved for convenience only and purged on a scheduled monthly basis. All substantive emails are saved to the shared drives according to classification.

[1] Transactional systems such as Student Information System would be an example of a declarable recordkeeping system.
[2] For more on Role-based email management contact the Records Management Unit

Example of tagged **transitory email** using *Color Categories* within OutLook.[iii] Tags are highlighted in yellow



Use of non-UBC email systems. Do not use non-UBC email accounts to conduct University business. See **Privacy Fact Sheet – Privacy of Email** Systems for more information.[iv]

Email Security: ensure all mobile and other devices are at the very least password protected and if there is any personal or confidential information the device should be encrypted. Contact IT Services for help with encrypting devices.

https://it.ubc.ca/services/security/encryption-services

Checklist for Electronic Records Management.

- ✓ Define recordkeeping responsibilities for each record keeping area (e.g. Shared Drives, Project SharePoint site)
- ✓ Set up a top folder structure according to the University Classification Plan
- ✓ Keep folder hierarchy as flat as possible (no folder within folder)
- ✓ Add a year (or some other organizing principle) to the folder under which the records accumulate to facilitate records retention
- ✓ Manage the folder security by creating and maintaining a folder/security matrix on paper
- ✓ Declare and map where the recordkeeping system is retained typically transactional system and/or shared drives as the primary records storage area where all substantive records should be retained. All other systems (Outlook, SharePoint, Website) are for convenience only.
- ✓ Manage libraries in content management systems such as SharePoint using the same naming standards as the shared drives
- ✓ Use agreed upon common tagging system for documents going into the folder structure to compliment folder structure as required

- ✓ Dispose of electronic records according to the University Schedules and coordinate with destruction of paper records
- ✓ Store substantive emails on the shared drives
- ✓ Remove transitory emails regularly
- ✓ Contact the University Archives if you need help

Definitions

Digital Record Records made or received and set aside as evidence of a unit's activities, by means of electronic or computer equipment.

Disposition of records means disposal of records no longer required by the unit either through destruction, secure destruction, or transfer to the University Archives.

Office of Primary Responsibility means the office or offices that are responsible for holding the complete record and who approve disposition orders.

Recordkeeper is the person or persons who have been defined by the unit, or group to ensure the structure on the shared drives or SharePoint site are according to the agreed-upon system.

Transitory Record means a record or email of temporary usefulness that is required for a limited period of time. Records include drafts, once the final has been produced, copies, and superseded documents.

Substantive Record means written evidence that an action did, or did not happen, transactional records, decisions and polices.

University Classification System is a system that describes the Functions and activities of the University of British Columbia that is controlled by policy through the University Archives.

---

[i] Evidence Act [RSBC 1996], Chapter 124, uses the typical test for integrity and authenticity of a records system as the records were managed in the "ordinary course of business."

[ii] Substantive means: records that prove that an action, decision or transaction did, nor did not, get approved or take place; records that document decisions, transactions and polices.

[iii] All substantive email should be saved in the Shared Drives leaving only transitory emails within email system.. For more information on what constitutes a substantive email or record see Shared Drive Guidelines.

[iv] Privacy Fact Sheets are available on the Office of the University Counsel website http://universitycounsel.ubc.ca/access-and-privacy/privacy/