

Guideline



Recordkeeping Metadata Requirements

Records Management and Privacy Office
Kingston, ON K7L 3N6
Tel. (613) 533-6095
recordsmanagement@queensu.ca

This guideline is designed to assist units when implementing or reviewing a system or service that will store or manage university records. University Records as defined by the [Queen's Records Management Policy](#) are records, in any media or format, within the university's custody or under its control that are created or received, and maintained as evidence or information in the administration and operation of the activities of the university. The minimum recordkeeping metadata requirements, based on the [ISO 23081 standard](#) (Metadata for records), promote a standardized approach to managing metadata necessary for effective records management across the university at a systems level. The purpose of this guideline is to identify necessary metadata elements and define the features of each element.

What is recordkeeping metadata?

Recordkeeping metadata is structured information used to assist with locating, retrieving, managing, maintaining, and disposing of records. Metadata evidences the business context and use of records, and when properly applied and managed, helps ensure records can serve as authentic and reliable evidence of university business for as long as they are required. Metadata in this context is data that describes records throughout their lifecycle, and when applied effectively and consistently can provide descriptive, structural, and administrative information about university records.

It should be understood that the university's recordkeeping systems include all systems used to capture, create, manage, access, retain and dispose of the university's business records over time, including enterprise systems such as PeopleSoft and Microsoft 365, externally hosted (cloud) services such as Qualtrics, and shared directories in offices.

Recordkeeping metadata is often already available in existing recordkeeping systems and even imbedded in the files themselves, documenting facts about the record such as author, date of creation, name of the file, and current storage location,* but metadata must be identified and then actively managed and preserved to meet the university's requirements for effective recordkeeping.

Recordkeeping metadata is generated when a record is created or imported into a system, and also as the record is used and maintained in work processes, allowing its use and changes to be tracked through time, and its connections with other records to be documented. Systems such as Salesforce and QDocs can collect metadata from a user's unique login credentials to detail who accessed a record and what updates were made to it. This type of metadata is collected automatically by the system once it has been properly configured, and

* All of these metadata elements can be found in the properties of a Microsoft Office file such as Word, Excel, or PowerPoint.

Recordkeeping Metadata Requirements

requires no user input. Other elements of metadata may require the user to input information so that the metadata for a record will be complete.

Regardless if it is collected automatically by the system or input by the user, metadata can be stored either as a constituent element of the record or as information in the system that is fundamentally linked to the record. Where the metadata is stored is frequently dictated by the system itself, though metadata that is stored separately from the record can be more easily preserved after the record has been appropriately disposed of. Typically, metadata should not be altered unless it is later found to be incorrect or incomplete.

Managing minimum requirements for recordkeeping metadata

A unit's records must have enough metadata to ensure they are trustworthy. Records must be accurate, authentic, and reliable as evidence of transactions, decisions and actions. Units must ensure that records have appropriate metadata to provide meaning and context through the entire lifecycle of the record, and that this metadata remains associated up to, and at times after, the record has been disposed of.

In complex business and systems environments, it is advisable to design systems with a mind towards records management from the beginning. A unit should consider at the start how to facilitate system maintenance, migrations and decommissioning by ensuring that systems specifications include requirements for minimum metadata needed to support records identification, usability, accessibility and final disposition.

Roles and responsibilities

Information Stewards are responsible for:

- ensuring that recordkeeping metadata is available for the records under their control, and is described in their unit's recordkeeping protocols;
- in consultation with the university's Records Manager, identifying any absent recordkeeping metadata, and developing strategies to fill these gaps;
- ensuring that their unit can retrieve records when requested, including information on the history, use, and disposal of their unit's records; and
- ensuring that quality assurance procedures for recordkeeping metadata are implemented and followed by their staff and reviewed on a regular basis.

Systems Administrators are responsible for:

- identifying system-generated metadata corresponding to the metadata elements recommended by this guideline;
- identifying any mandatory metadata elements that are not automatically generated by the recordkeeping system, and assisting unit managers in developing methods to persistently link to the records any metadata which must be stored outside of the system;
- ensuring that this metadata is available and usable for as long as it is required by the university; and

Recordkeeping Metadata Requirements

- documenting recordkeeping metadata elements and their retention requirements in the system documentation.

University employees are responsible for:

- following their unit’s protocols for recordkeeping metadata creation and maintenance;
- alerting their supervisors to any inconsistencies or inaccuracies in recordkeeping metadata they find in the course of their daily work; and
- when the need arises, recommending additions or alterations to recordkeeping metadata required to support the business activities or processes for which they are responsible.

Director, University Records Management is responsible for:

- advising on the inclusion of recordkeeping metadata for all new systems being implemented at the university.

Metadata requirement rankings

As not all systems may be capable of achieving all of the recommended metadata elements, a ranked standard has been devised. The minimum standard is **Bronze**, the intermediate standard is **Silver** and the comprehensive standard is **Gold**. All systems must achieve a Bronze status to be considered for use as a recordkeeping system at Queen’s University. Silver status is for all systems that exceed the Bronze minimum and the Gold standard is for systems that implement all of the applicable metadata elements.

Recordkeeping Metadata Element	Rankings		
	Bronze	Silver	Gold
Title	Required	Required	Required
Creator	Required	Required	Required
Record Date	Required	Required	Required
Security Classification	Required	Required	Required
Access	Required	Required	Required
Event Date and Time	Required	Required	Required
Event Type	Required	Required	Required
Identifier	-	Optional	Required (if applicable)
Agent Institution Identifier	-	Optional	Required
Agent Role	-	Optional	Required (if applicable)
Format	-	Optional	Required (if applicable)
Addressee	-	Optional	Required (if applicable)
Location	-	Optional	Required
Record Associations	-	Optional	Required
Agent Individual Identifier	-	Optional	Required
Record Lock	-	Optional	Required (if applicable)
Retention Information	-	Optional	Required
Disposition Action	-	Optional	Required

Recordkeeping Metadata Requirements

Recordkeeping Metadata Elements

Title	
Description	A human readable and comprehensible name given to the resource by which it is commonly known.
Implementation	Identify the resource by means of a name conforming to a unit-established file naming convention.

Creator	
Description	An entity primarily responsible for making the content of the resource. Examples of a Creator include a person, an organization, or a service.
Implementation	Identify the name of the Creator and (if applicable) their unique identifier (e.g., NetID).

Record Date	
Description	The date of an event in the lifecycle of the record. Typically, Record Date will be associated with the creation, implementation, or publication of the record.
Implementation	Log the date in YYYY-MM-DD format (as detailed by the ISO 8601 standard) unless restricted by system limitations.

Security Classification	
Description	The Data Classification Level of the record as determined by the Queen's Data Classification Scheme.
Implementation	Identify the record as Confidential, Internal, or General as determined by the Queen's Data Classification Scheme.

Access Rights	
Description	Permissions assigned to a record that govern or restrict access to actions taken on the record.
Implementation	Set and log permissions as appropriate within the system or storage environment.

Event Date and Time	
Description	The date and time of the action taken on a record.
Implementation	As per the ability of the system or process, log the precise date and time of actions taken on a record. Minimally this should include YYYY-MM-DD-HH:MM (as detailed by the ISO 8601 standard).

Event Type	
Description	An action taken on a record during its existence.
Implementation	Identify edits, deletions, permission changes and any other significant events during a record's existence.

Recordkeeping Metadata Requirements

Identifier (only applicable for electronic recordkeeping systems)	
Description	An explicit reference to the resource that identifies it using a system-generated unique identifier.
Implementation	Identify the resource by means of a string or number conforming to an established identification system.

Agent Institution Identifier	
Description	Official name of the department, office, Faculty, or institution of the individual who performed an action on a record at the time the action was taken.
Implementation	Use Division ID and/or Department ID, or other relevant identifier of the individual's department, office, Faculty, or institution.

Agent Role (where applicable)	
Description	A category that identifies the job function or responsibility of a particular individual at the time an action was taken on a record.
Implementation	Identify the role of the individual as defined by their department, office, Faculty, or institution.

Format (where applicable)	
Description	The size and manifestation of the record.
Implementation	Identify the page count (analog) or file size (digital), and/or the physical or digital manifestation (file type) of the record.

Addressee (where applicable)	
Description	The name of the recipient(s) to which a record has been sent.
Implementation	Identify the addressee(s) using recipient(s) name(s), or the name of the office/unit/company as appropriate.

Location	
Description	A description or indication of where the analog or digital record resides.
Implementation	Document where the record resides using the system, or by creating an associated record that logs the physical or digital location.

Record Associations	
Description	Identification of connections that link the constituent parts of a record.
Implementation	Determine the associations by means of identifying links, or logically grouping the constituent parts of a record by tagging digital records, or physically grouping hard copy records.

Recordkeeping Metadata Requirements

Agent Individual Identifier	
Description	A unique indicator that identifies the individual who performed an action on a record at the time the action was taken.
Implementation	Provide the Net ID or other unique ID that grants an individual access to the records system.

Record Lock (where applicable)	
Description	An indicator that a record may not be further altered.
Implementation	Identify the status of the record via the file naming convention (e.g., LOCKED) or disable editing capabilities via the system.

Retention Information	
Description	Retention trigger and date: A condition and date that must be met to initiate the retention period countdown. Retention period: The period of time a record must be retained before authorized disposition is permissible.
Implementation	Determine retention triggers and dates and retention periods using the Queen's Records Retention Schedules.

Disposition Action	
Description	The action that will be taken on a record after surpassing its minimum retention period.
Implementation	Identify disposition actions using the Queen's Records Retention Schedules.

Additional metadata

If a unit determines that additional metadata elements are valuable for its business, the unit is encouraged to consult with the university's Records Manager and the people who manage or maintain the system or service to determine the feasibility of the suggested addition(s).