Recordkeeping Metadata Standard

Name of Record	Recordkeeping Metadata Standard
Author	Senior Information and Improvement Officer
Owner	Chief Executive's Business Manager
Date	5/5/21
Review Date	ongoing

Version	Notes	Author	Date
0.1	First Draft	HJ	28/03/2021
0.2	Updated following CMG review	HJ	20/04/2021
0.3	Adopted for RMP	SIIO	5/5/21

Introduction

This Guideline[1] recognises the need for management of metadata as a key component of information and records management in the digital environment. Better metadata management will:

- support information discovery
- reduce duplication in data collection
- facilitate information sharing for better service delivery
- assist in identifying critical information assets that require more intensive management.

The term ‘metadata’ is used and understood by different communities in different ways. Software programmers, librarians, spatial data managers, statisticians and other professionals have all defined their own sets of metadata to serve their own business purposes. As a consequence, there are many different ‘types’ of metadata; for example, information resource discovery metadata, statistical metadata and geospatial metadata.

The recordkeeping profession has also defined what metadata they need to manage and preserve records now and into the future. This Guideline does not attempt to replace any existing standards, which are extremely comprehensive, but rather define a simplified metadata set that can be immediately applied in East Renfrewshire Council.

Recordkeeping metadata can be used to identify, authenticate and contextualise records and the people, processes and systems that create, manage and use them. Recordkeeping metadata such as classification schemes or taxonomies also assist users to find, understand, access, share and use information. Metadata is also necessary to develop system upgrade, migration and other preservation strategies that will sustain digital records in the long term. Recordkeeping metadata may not always need to be created, but simply identified in existing systems and software applications and then managed over time.

[1] This document has been adapted from the Tasmanian Government Office of the State Archivist - https://www.informationstrategy.tas.gov.au/

A key feature that differentiates recordkeeping metadata from other types of metadata is that it is not a static profile of a document or other information asset. Recordkeeping metadata initially defines a record at the point of creation or capture, but is also dynamic and accrues through time, to describe how a record has been used or managed. In the digital environment, it is the management of metadata over time that will allow your records to be accepted as meaningful and accountable evidence. For example, systems with electronic document & records management functionality, such as M365 SharePoint Online, will capture an audit trail of all users who view, edit, print or modify a document.

Purpose

This Guideline outlines minimum requirements for recordkeeping metadata to support the creation, capture, management, storage, retention and eventual disposal of Council records in digital format. It has been developed to ensure that digital records are protected and accessible for current and future use as long as there is a business need to retain them, in line with the Council's Record Retention Schedule.

It should be used:

- to set down minimum metadata requirements that should be applied in the design of any new application or architecture that holds Council information and records.
- to assess recordkeeping requirements of existing business systems and file repositories that hold information and records where these have been identified as representing high risk and/or high value to the Council.

It includes, as an appendix, a metadata template that can be used to support the assessment process by mapping the recordkeeping metadata elements in this guideline to the equivalent field and tables in the specific system or repository that is being assessed.

The application of metadata standards should come at system level through automation rather than requiring the manual effort of each officer when they are creating and capturing records. This is particularly challenging for information and records stored in network shared drives. The guideline therefore includes a section on different approaches to the application of metadata standards in different digital environments.

Key Terminology

Keyword	Interpretation
MUST	The item is mandatory.
MUST NOT	Non-use of the item is mandatory.
SHOULD	Valid reasons to deviate from the item may exist in particular circumstances, but the full implications need to be considered before choosing this course.
SHOULD NOT	Valid reasons to implement the item may exist in particular circumstances, but the full implications need to be considered before choosing this course.
RECOMMENDS / RECOMMENDED	The item is encouraged or suggested.

'MUST' and 'MUST NOT' statements are highlighted in capitals throughout the Guideline. Business Areas or projects deviating from these MUST advise SIIO of the decision to waive particular requirements.

Business areas or projects deviating from a 'SHOULD' or 'SHOULD NOT' statement MUST record:

- the reasons for the deviation,
- an assessment of the residual risk resulting from the deviation,
- the date at which the decision will be reviewed, and
- whether the deviation has Senior Information Risk Owner (SIRO) and Executive Director approval.

Business areas or projects deviating from a 'RECOMMENDS' or 'RECOMMENDED' requirement are encouraged to document the reasons for doing so.

Minimum recordkeeping metadata

Recordkeeping metadata MUST be applied to Council records in all formats.

Typically, digital records will have a lifespan beyond the system in which they are

created and managed. Identifying, capturing and managing recordkeeping metadata is necessary for digital preservation strategies such as system migration that will sustain records that are needed to meet long term Council requirements including those that need to be preserved permanently as part of Council archives.

Recordkeeping metadata is also critical to sustaining the authenticity and integrity of our records as meaningful and accountable evidence. Therefore, minimum recordkeeping metadata SHOULD be applied to all high-risk business information. The following recordkeeping metadata MUST be linked to the records at point of capture, and these linkages maintained over time. Where possible, metadata SHOULD be automatically captured:

Element	**Mandatory point of capture metadata**	**Explanation**
1	Record identifier (ID)	Ideally, this is unique and system assigned, but in practice (i.e. shared network drives - may be manually assigned and not unique.) It may be the same as 2.
2	Title/name	Meaningful title which should be manually entered or assigned by the system. This will align with our approved file naming procedures
3	Date of creation	Date the record was created, not the date captured or registered in system. Can be manually recorded or system-assigned.
4	Author/creator	Original creator of the record content. This may refer to a person or a system that created the original record. The creator may be external to the agency.
5	Business purpose / process / activity	Why this information is captured (i.e. the business context). This is normally assigned by classifying according to the Council's Business Classification Scheme (BCS).
6	Creating software	For digital records, the system/software

Element	Mandatory point of capture metadata	Explanation
	application	name
7	File format	Standard structure and type of data files. May be proprietary or open format. For example, Microsoft Word documents saved as .doc are proprietary, whereas .docx format is supported by multiple applications.

The following recordkeeping metadata MUST be linked to the records and accrue through time, to describe how a record has been used or managed. Where possible, metadata SHOULD be automatically captured.

Element	Mandatory point of capture metadata	Explanation
8	Action that was taken, such as: • Registration into the recordkeeping system • Apply or change access rules • Modify or edit • Transfer of control/custody • Migration	Any action that is carried out on the records should be captured as metadata. When a record is registered in the system, security classification is added, access is changed or retention and disposal is applied, these actions should be recorded in audit logs.
9	Date of Action	Can be manually recorded or system-assigned.
10	Responsible Officer/ID	Person responsible for taking/applying the action.

There are also additional properties that MUST also be applied to records at the file, folder or aggregated level (e.g. applied to each folder, to an identified information asset or whole-of-system):

Element	Mandatory process	Explanation

	metadata	
11	Disposal actions taken	The retention and disposal action, authority and trigger
12	Information security	Protective Marking and Descriptors (if not 'OFFICIAL')

Recordkeeping metadata **SHOULD** be actively used as a planning tool to manage digital records and implement automated workflow actions. For example, retention and disposal metadata is commonly used to trigger disposal operations, however, if 'last action' dates are not applied to each record, the trigger cannot be activated. Council Departments can make use of recordkeeping metadata to identify vital, closed, sensitive and legal-hold records. Recordkeeping metadata also supports data sharing, data integration and linking activities.

It is important that business areas recognise that this is a minimum metadata set. Business areas SHOULD add to the value of records by supplementing recordkeeping metadata with geospatial, statistical, legal, financial, multimedia and other types of metadata.

Implementation

It is only practical and cost effective for compliance with this Guideline to be applied retrospectively in existing business systems and file repositories where these have been identified as holding information and records that represent high risk or high value to the Council. The Council's Performance Risk and Compliance Framework addlink includes a risk assessment template that can be used to support this identification process.

The most appropriate time to implement minimum recordkeeping metadata standards is when new or enhanced systems are being implemented. When deciding what metadata to capture, consider that any data that is currently captured in systems may be used differently in the future. To make the most of future developments in business intelligence, open government and data analytics, consider any metadata as potentially useful, and as part of your mitigations for Information Risk as identified in Data Protection Impact Assessments and other business risk assessments.

Several approaches are available for the capture, management and storage of recordkeeping metadata:

Embedding or encapsulating metadata within the record itself.

Digital image files have embedded metadata that can be automatically captured when a photograph is taken, such as unique id, date taken, creator's name, geo-location, etc. An archival preservation file format has recordkeeping metadata encapsulated with the record, and managed as an integral part of it.

This is the approach to take for documents stored on shared network drives, where metadata can be manually captured in the properties when a record is created and then viewed via the File/Properties menu. Successful compliance here is very difficult without strong governance in place.

Maintaining metadata separately and linking it to the record.

For example, business systems metadata can be mapped to the minimum recordkeeping metadata, and the metadata managed separately to the business system. This requires the development and maintenance of reliable and robust business processes to maintain links between the record and its associated metadata.

Most business systems process uniform transactions, (e.g. applications for leave in an HR system, payment of invoices in a finance system). Contextual metadata created by the system can often be derived from system documentation and is therefore one way of identifying and mapping business system metadata to the recordkeeping metadata set.

Automatically capturing metadata in the system.

This metadata is managed within the recordkeeping or business information system in which the record is created or stored. For example, in SharePoint Online, metadata is both embedded in the record and linked to a record. Some metadata is maintained as a placeholder, even after the content of the record has been destroyed.

Where possible, recordkeeping metadata should be automatically captured by the

system, and be persistently linked to the record. Some business systems have this capability. Systems that are designed to manage digital records, such as SharePoint Online, do have this functionality. Currently, this is the best possible means of 'future-proofing' digital records.

Managing metadata

The Council MUST manage recordkeeping metadata as part of Records Management Policy compliance. The effective application of recordkeeping metadata ensures digital records remain retrievable, accessible, usable and shareable. Therefore, the Council MUST establish effective planning and management practices to ensure that capture and management of recordkeeping metadata remains consistent across all systems that hold Council records, irrespective of the technology format or medium.

At a minimum, we SHOULD:

- Have documented metadata standards and established procedures to ensure that accurate, standardised and relevant recordkeeping metadata is captured in systems that keep records.
- Implement monitoring and review processes to ensure the quality, integrity and consistency of recordkeeping metadata over time, across systems and digital formats.
- Undertake metadata mapping to support data integration, system migration and sharing of information.

Standardised metadata supports interoperability between systems and ensures successful system migrations. Procedures for the application of standardised metadata schemas and controlled vocabularies to all information assets in the Council will support the capture of meaningful, accurate and consistent recordkeeping metadata.

Appendix 1: Record Keeping Metadata Mapping Template

This metadata template can be used to map the recordkeeping metadata elements in this standard to the equivalent field and tables in business systems and file repositories that holds Council records and could be integrated with the Council's Information Asset Register. If there is no equivalent metadata element in the system, this must be documented. Examples are provided.

Date:	
Person responsible for undertaking mapping:	
Information Asset / system Name:	
Asset Description:	
Status (e.g. in use/inactive/legacydata):	
Information Asset Owner:	

Recordkeeping Metadata Element		**Equivalent table/data field in agency system**	**Level applied**	**Comments**
1	Record identifier (ID)	< Record Number > < Unique Identifier >	< Record level >	< Record Number is automatically generated bysystem, based on a structure of: DOC/YY/NNNNN. However, the Unique ID is system generated and is sequential number >

2	Title/name	< Document Title >	< Record level >	< Three level naming structure. Top two levels are generated based on the title of the folder using the agency's BCS. The third level of the titleis a free text field of 254 characters maximum >
3	Date of creation	< Date Written (Date Created) >	< Record level >	< This is automatically generated by system unless the record was originally hardcopy and then digitised, in which case the date created is manually applied >
4	Author/creator	< Author / Signatory > < Provenance >	< Record level >	< This is automatically assigned by system, based on user login if created in Office software and saved in the system. If the record is saved into the system from an outside source, metadata may need to be manually applied. >
5	Business purpose/process/activity	< Business Classification Scheme >	< Folder (Container) level >	< Two level Function/Activity classification scheme, implemented in the system in 2014 based in unique and common administrative functions >
6	Creating software application	< Item Type > < Information Asset Description >	< Record level > < Information Asset level >	< e.g. Microsoft Word Document. The software name and version number is listed in the agency's Information Asset Register >

7	File format	< Extension >	< Record level >	< e.g. DOCX >
8	Action that was taken, such as: • Registration into the recordkeeping system • Apply or change access rights • Modify or edit • Transfer of control/custody • Migration	< Edit Status > < Access Control > < Document Details > < Document History > < All Actions >	< Record level > < Folder (Container) level >	< The system has a number of metadata fields that document actions to the record and to the folder >
9	Date of action	< Date Modified > < Date Closed > < Date Imported > < Date Inactive > < Date Due for Destruction >	< Record level > < Folder (Container) level >	< The system has a number of date fields that document process actions. >
10	Responsible officer/ID	< Access Control >	< Record level > < Information Asset level >	< The Access Control field logs all changes to the record and record metadata including the date of the action and the name and position of the officer responsible for the action.
11	Disposal	< Retention Schedule > < Date of Disposal >	< Folder (Container) level >	< This applies the RRS ref number, and disposal action >

12	Information security	< Security Marking >	< Record level >	< This is a custom field that is applied by the System Administrator. This is updated to a higher protective level if requested by folder owners, if the information registered to the folder is assessed as requiring higher protection levels. This process is documented in the Council's Information Security Procedures >