

Guideline for Mandatory Standard 1 - Make and Keep

DRAFT



Contents

Introduction.....	3
1. Purpose	3
2. Authority and application	3
3. How to use this Guideline	3
PART 1: EXAMPLE COMPLIANCE INDICATORS	4
Requirement 1: Records management is supported at all levels of the business with appropriate governance frameworks.	5
Requirement 2: Make accurate public records of action and decisions.	8
Requirement 3: Make accurate metadata about a public record.	10
Requirement 4: Keep a public record.	12
PART 2: IMPLEMENTATION ADVICE	15
Requirement 3: Make accurate metadata about a public record.	15
3.1 Metadata is made and captured to ensure authenticity, meaning and context are associated with the public record.	15
3.3 Where relevant, metadata is made and captured by Departments for records relating to Aboriginal and Torres Strait Islander communities, culture, culturally sensitive information and language.	18
Appendix A.....	19
Definitions	19
Related Documents	20
Document History	20
Contact Details	20

Introduction

1. Purpose

This Guideline supports *Mandatory Standard 1 – Make and Keep* (the Standard) issued under the *Public Records Act 2023* (the Act) and provides guidance about how public authorities can implement the minimum requirements set out in the Standard.

2. Authority and application

When approved – This Guideline has been issued by the State Archivist under section 46(1)(c) of the Act and is proposed to come into effect on XXXX 2026.

This Guideline applies to all Queensland public authorities as defined under section 8 of the Act.

This Guideline should be read in conjunction with *Mandatory Standard 1 – Make and Keep*.

3. How to use this Guideline

This Guideline supports the Standard and provides advice in two separate parts:

- **Part 1: Example Compliance Indicators** – outlines brief examples a public authority could adopt to meet the minimum requirements stated in the Standard. These compliance indicators are not mandatory – they are examples of the way in which the minimum requirements could be met and are not exhaustive. Public authorities may also have other ways in which the minimum requirements could be met.
- **Part 2: Implementation Advice** – outlines the methodology for meeting some of the example compliance indicators in Part 1.

For a list of Definitions used in this document, please refer to Appendix A.

PART 1: EXAMPLE COMPLIANCE INDICATORS

DRAFT

Requirement 1: Records management is supported at all levels of the business with appropriate governance frameworks.

Minimum compliance requirements in Mandatory Standard 1 – Make and Keep	Examples of how a public authority can demonstrate compliance with the requirement Note: these are examples only and are not an exhaustive list
1.1 The strategic direction and allocation of resources for records management is determined and documented by senior management and/or an internal governance mechanism.	• Corporate policy on Records Management (RM) is endorsed at the senior executive level. • Corporate policy on RM is made available to all staff, volunteers and contractors. • Plans are in place to improve capability, in particular for staff with specialist RM roles. • There are internal structures for senior managers to engage with skilled RM professionals within the public authority.
1.2 Corporate responsibility for oversight of records management is assigned to a designated individual/s (senior responsible officer/s). Responsibility includes records management across all operating environments.	• Responsibility is assigned in corporate policy on records management (RM), including assigning of a designated individual senior responsible officer. • RM policy reflects Chief Executive's responsibility to ensure compliance with the <i>Public Records Act 2023</i>. • Delegations are updated in a timely manner to include records and management responsibilities and referenced in policy. • RM working group is established to oversee all aspects of RM in a public authority – not divorced from business context. • RM responsibility is assigned in individual performance plans.
1.3 Staff, contractors and volunteers are, during induction and periodically	• Staff, volunteers and contractors have the necessary skills and knowledge to manage

Minimum compliance requirements in Mandatory Standard 1 – Make and Keep	Examples of how a public authority can demonstrate compliance with the requirement Note: these are examples only and are not an exhaustive list
throughout their tenure, trained and supported to make and manage records.	records according to its value as a business and community asset. - Resources are allocated in support of effective records management practices and systems. - Formal and/or informal RM training is undertaken by all staff, volunteers and contractors. - RM Training and development activities are assigned in individual performance plans.
1.4 Governance mechanisms are in place to oversee compliance.	- Records management is monitored and evaluated e.g. as part of internal or external audits. - Information assets are managed strategically with appropriate governance and reporting. - Public authorities have up-to-date governance arrangements covering all information assets. - Monitoring of records management performance, systems and processes occurs and corrective actions to address issues are undertaken and documented. - Reports on monitoring of records management performance, systems and processes, and corrective actions are prepared for governance committees e.g. Audit and Risk Committees.
1.5 Records management responsibilities are identified and included (or defined) in all outsourced, cloud, contracted and similar service arrangements.	In the public authority, responsibilities for identifying and monitoring records management requirements in outsourced, cloud, contracted and similar service arrangements are documented in a policy e.g. portability, appropriate storage, ownership, accessibility, disposal.

Minimum compliance requirements in Mandatory Standard 1 – Make and Keep	Examples of how a public authority can demonstrate compliance with the requirement Note: these are examples only and are not an exhaustive list
	• Responsibilities for all parties (public authority and those providing outsourced, cloud, contracted and similar service arrangements) are included in contracts and instruments, including egress of records at end of contract lifecycle.

Requirement 2: Make accurate public records of action and decisions.

Minimum compliance requirements in Mandatory Standard 1 – Make and Keep	Examples of how a public authority can demonstrate compliance with the requirement Note: these are examples only and are not an exhaustive list
2.1 Actions and decisions are consistently and routinely recorded.	• Policies, business rules and procedures document staff requirements and responsibilities for the making, capture and management of public records. • Records management requirements are included in procedures and work instructions to identify: - where public records are being made/received - what actions are required around where public records are captured - who is responsible for capturing, security and other considerations relating to public records. • Assessments or audits demonstrate that systems operate routinely, and records and metadata are made and captured.
2.2 A decision about a public record and records management is defensible and can be traced back to responsible parties or decision makers.	• Decisions, policies, business rules or procedures are identified and documented to guide what records, information and data are required to meet or support: - business needs - community expectations.
2.3 A decision about a public record and records management appraises value and considers risk.	• Permanent value of records is assessed through an appraisal process consistent with the QSA Appraisal Statement. • Permanent value, high-risk and/or high-value records are identified and are formally documented e.g. as part of your Information Asset Register.

Minimum compliance requirements in Mandatory Standard 1 – Make and Keep	Examples of how a public authority can demonstrate compliance with the requirement Note: these are examples only and are not an exhaustive list
	• Risks are identified, managed or mitigated, and documented as part of your public authority's risk management approach. • A value and risk assessment process is in place which is modelled on a process developed by an archival institution in Australia or New Zealand e.g. State Records of South Australia Value and Risk Assessment process. • Permanent value, high-risk and/or high-value records, information and data are protected by business continuity strategies and plans. • Risk management of records is included in all corporate risk management systems including specific records management policies, plans and procedures. • A process to recover and restore public records in the event of a disaster, including a cyber-attack, is documented and included in risk management processes or other processes (e.g. Business Continuity Plans).
2.4 A public record is made and kept digitally by default throughout the lifecycle of the record, whenever practicable.	• Policies, business rules and procedures articulate that public records made digitally are kept and maintained in their digital format. • Business processes identify and document digital ways of working when making or amending records. For example, applying digital signatures on electronic documents instead of wet signatures on paper copies. • Digital workflows and business processes are prioritised to enable public records to be made and kept digitally.

Requirement 3: Make accurate metadata about a public record.

Minimum compliance requirements in Mandatory Standard 1 – Make and Keep	Examples of how a public authority can demonstrate compliance with the requirement Note: these are examples only and are not an exhaustive list
3.1 Metadata is made and captured to ensure authenticity, meaning and context are associated with the public record.	• Minimum metadata set developed by Queensland State Archives is applied to all public records regardless of format. • Minimum metadata set developed by an archival institution in Australia or New Zealand is applied to all public records regardless of format. • Metadata is mapped to systems that capture and store records and is updated whenever changes occur. • Metadata assigned to records explains their content and context: • Training for staff, volunteers and contractors includes how to appropriately title documents and may include a standardised dictionary that outlines acceptable acronyms and established phrases.
3.2 Public records are identifiable, retrievable and accessible for as long as they are required.	• A system is implemented that applies unique identifiers to records. • The process for migrating records between systems ensures all metadata attached to the records is also carried over in its entirety. • A records management system is maintained that supports easy searching and retrieval functions. • A system of access controls (e.g. security classification, sensitivity labels) is implemented that defines who can access, modify or delete records, ensuring only authorised access is permitted.

Minimum compliance requirements in Mandatory Standard 1 – Make and Keep	Examples of how a public authority can demonstrate compliance with the requirement Note: these are examples only and are not an exhaustive list
	• An inventory listing for locations of all public records is available and regularly updated (e.g. an Information Asset Register). • Lawful disposal authorisations are complied with.
3.3 Where relevant, metadata is made and captured by Departments for records relating to Aboriginal and Torres Strait Islander communities, culture, culturally sensitive information and languages.	• Identify records or groups of records which should have additional metadata applied and implement with a consideration of cultural appropriateness and sensitivity. You could engage with: - Relevant Aboriginal and Torres Strait Islander communities and/or cultural custodians - relevant areas of your public authority. • Document and regularly update metadata creation and capture policies and ensure staff, volunteers and contractors are aware of any changed requirements. • Develop policies around who can view, modify, or disseminate records with restricted culturally sensitive information.

Requirement 4: Keep a public record.

Minimum compliance requirements in Mandatory Standard 1 – Make and Keep	Examples of how a public authority can demonstrate compliance with the requirement Note: these are examples only and are not an exhaustive list
4.1 A public record is consistently and routinely kept in appropriate storage conditions.	- Records stored in business systems are actively managed to ensure they remain discoverable and accessible in a meaningful way. - Appropriate security and access controls, e.g. audit trails or user permissions, are implemented. - Considered effort is made to migrate records from digital carriers – e.g. portable hard drives or optical discs – to a centralised location such as a dedicated business system. - Training and development opportunities are established to create awareness of the risks and limitations of using portable storage media as long-term storage solutions. - Information Asset Register or other instrument captures and tracks the location of all records. - Storage is assessed as suitable for the type, quantity and access requirements of public records e.g. appropriate storage of permanent value, high risk and high value records is prioritised. - Storage facilities are assessed as suitable for the type, quantity and access requirements of records e.g. appropriate storage of permanent value, high-risk and high-value records is prioritised.
4.2 Storage arrangements protect public records from misuse, loss, deterioration or damage.	- Appropriate security and access controls, e.g. audit trails or user permissions, are implemented. - Systems holding records of potential or identified permanent value or medium to long-

Minimum compliance requirements in Mandatory Standard 1 – Make and Keep	Examples of how a public authority can demonstrate compliance with the requirement Note: these are examples only and are not an exhaustive list
	term value are identified and documented e.g. Information Asset Register. • Migration plans are in place (and regularly reviewed) for older systems or systems marked for decommissioning to ensure all records are migrated. • Regular integrity checks are carried out on digital records that are required to be retained for the medium to long term. • Physical records storage areas are protected against and monitored for pests and vermin. • Physical records storage areas are protected and maintained against external weather, natural and man-made hazards such as floods, bushfires, utility failures, physical agents, pollutants and light exposure. • Protection and remediation of records are included in any Disaster Planning strategy documents or Business Continuity Planning documents.
4.3 Security and preservation activities protect public records from inappropriate access and changes.	• Appropriate security and access controls, e.g. audit trails or user permissions, are implemented within a content management system. • Policies, business rules and procedures are in place that identify how access, use and the appropriate sharing of information and records are managed. • Preservation activities (including salvage of damaged records performed on physical records) follow principles of protection and preservation of integrity, cultural value and significance, security, documentation and reversibility. e.g. in accordance with the AICCM Code of Ethics and Practice.

Minimum compliance requirements in Mandatory Standard 1 – Make and Keep	Examples of how a public authority can demonstrate compliance with the requirement Note: these are examples only and are not an exhaustive list
	Professional consultation and advice is sought to evaluate risk associated with security and preservation activities.
4.4 Public records are accessible until disposal is appropriately endorsed and authorised.	- A content management system is maintained that supports easy searching and retrieval functions. - A system of access controls (e.g. security classification, sensitivity labels) is implemented that defines who can access, modify or delete records, ensuring only authorised access is permitted. - Lawful disposal authorisations are complied with.
4.5 A public record in a digital system can be migrated or exported accurately and completely.	- Whenever a business system containing public records is implemented, a plan is in place to identify and document exit strategies and functionalities to retrieve the records in the event of system decommissioning. - All data migration activities include quality assurance measures to ensure no data is lost or damaged.

PART 2: IMPLEMENTATION ADVICE

Requirement 3: Make accurate metadata about a public record.

3.1 Metadata is made and captured to ensure authenticity, meaning and context are associated with the public record.

Compliance Requirement Exemplar: Apply the minimum metadata set specified by Queensland State Archives.

The minimum mandatory metadata set specified by QSA is designed to be flexible, extensible and compatible with several established metadata standards. It specifies metadata elements that are recommended to be captured for all records.

Minimum metadata set

Metadata element	May also be known as	Description
Identifier	Record identifier	A concise, unique value that clearly identifies a record. Identifiers may be system generated or manually applied IDs
Name	Title	This element states the name given to a record as free text
Date/s		All relevant date/s of an action on the record, e.g. creation date, modification date, date of transfer to another public authority etc
Creator	Record creator	Information about who made the record. This may include individuals, roles, business units and systems
Access Rights - Security classification	Protective marking	A label or warning that denotes a record's security

Metadata element	May also be known as	Description
	Security caveat Dissemination Limiting Markers Security label Security level	status or sensitivity and/or indicates that special handling is required
Access Rights – Restrictions	Rights management Access conditions Access controls	A label or warning that denotes restricted access is required or has been applied
Disposal including: • what record is being disposed of • date of disposal • sentence (Disposal authorisation) • who authorised disposal to occur • proof of disposal	Disposal authorisation Disposal sentence Authorising officer Destruction notification Destruction certificate	Information about the Disposal Authorisation (e.g. retention and disposal schedule) and the disposal actions that relate to a record
Location: • Current location • Store location	Assignee Current location Home location	

The following are additional metadata elements (not minimum metadata) which should be considered for use by public authorities:

Metadata element	May also be known as	Description
Event history	Audit trail/history Recent activity	Documents the preservation, retrieval, disposal, control, access or use related activities performed on a record or aggregation of records
Integrity	Fixity Checksum Hash	Only mandatory when integrity checks are performed
Relationships	Related entity	
Format	Record type or format	A description of the record's format

Compliance Requirement Exemplar: Minimum metadata requirements specified by other archival institutions

Relevant minimum metadata requirements are also specified in standards or guidelines issued by other archival institutions (or similar) across Australia and New Zealand. These include, but are not limited to:

- Australian Government Recordkeeping Metadata Standard
- Office of the National Data Commissioner
- AS/NZS 5478:2015 Recordkeeping Metadata Property Reference Set (AS/NZS 5478)

3.3 Where relevant, metadata is made and captured by Departments for records relating to Aboriginal and Torres Strait Islander communities, culture, culturally sensitive information and languages.

Compliance Requirement Exemplar: Identify records or groups of records which should have additional metadata applied with a consideration of cultural appropriateness and sensitivity.

Some public records relating to Aboriginal and Torres Strait Islander communities, culture, languages and culturally sensitive information should have additional metadata applied to make discovery and access easier. For instance, public records containing Aboriginal or Torres Strait Islander language should have additional metadata which includes the language.

To meet this requirement and determine which public records should have additional metadata applied, the public authority may engage with:

- Aboriginal and Torres Strait Islander communities and/or cultural custodians
- other relevant areas of your public authority with knowledge or experience.

Compliance Requirement Exemplar: Identify and implement metadata standards specific to records relating to Aboriginal and Torres Strait Islander communities, culture, culturally sensitive information and languages.

Relevant advice for additional metadata for records relating to Aboriginal and Torres Strait Islander communities, culture, culturally sensitive information and languages includes:

- First Nations place data where possible using AIATSIS AustLang as a guide:
<https://aiatsis.gov.au/austlang/> AIATSIS corporate website
- If the First Nations place data is not available or challenging to include, capture all locations connected to the activity in the metadata and ensure it is captured accurately.

Appendix A

Definitions

Term	Definition
Accessible	The ability of authorised individuals to locate, retrieve and use records and information.
Appraise	Evaluate the merit, significance or value of records and information.
Availability	The degree to which records are accessible to authorised users when needed.
Defensible	The requirements can be supported by logical argument or sufficient evidence.
Department	A department is a department of government declared by Governor in Council under section 197 of the <i>Public Sector Act 2022</i> . Departments are a type of public service entity
Digitally by default	A principle that prioritises the creation and management of records in digital form as the primary and official version.
Disposal authorisation	An authorisation given by the State Archivist to dispose of a public record, or class of public records, for a public authority or multiple public authorities.
Dispose	Dispose of a public record means: - destroy or delete the record; or - alter or damage the record in a way that: - changes how accurately an action or decision is shown in the record; or - otherwise affects the integrity of the record; or - abandon the record; or - give away the record, whether by sale, donation or other transfer.
Governance framework	A structured set of guidelines, policies and processes designed to ensure activities are conducted in a compliant manner and uphold the principles of accountability, transparency and integrity.
Metadata	Structured or semi-structured descriptive information about a record that enables the management, use and preservation of records through time. It provides context such as creator, date, activity, and relationships.
Source record	Documents or records that have been copied, converted or migrated from one format or system to another. The source records are those that remain following the successful conversion or migration. Source records may be an original record or a reproduction generated by an earlier copying, conversion or migration process.

Related Documents

- *Mandatory Standard 1 – Make and Keep*
- *Mandatory Standard 2 – Disposal*
- *Guideline for Mandatory Standard 2 - Disposal*

Document History

Number: 1

Version: 1.1

Implementation Date: XXXX/2026

Review Date: 3 April 2029

Contact Details

Owner: Queensland State Archives, Policy and Assurance, Government Records

Contact Officer: Manager, Government Records

Phone: 3037 6777

Email: rkqueries@archives.qld.gov.au