

Data Governance Policy			
First Produced:	17/07/13	Authorisation:	Te Kāhui Manukura
Current Version:	13/11/2025	Officer	
Past Revisions:	17/07/13, 19/10/18, 15/07/2020	Responsible:	Director Strategy, Planning, Performance
Review Cycle:	3 year cycle		
Applies From:	Immediately		

1 Introduction

1.1 Purpose

Data governance ensures that systems and business processes are well managed and maintained both at strategic and operational levels on an ongoing basis to ensure data is accurate and available for business purposes. Data governance supports improved decision-making, compliance with regulations, and enhanced data security.

1.2 Scope and Application

The policy applies to all staff of Ara Institute of Canterbury Limited (Ara). It also applies to contractors, consultants and visitors engaged to work with, or who have access to Ara Ltd information. This policy applies to all students at Ara Ltd. Any exclusions that may apply must be stated within this policy.

1.3 Formal Delegations

Te Kāhui Manukura (TKM) has ultimate responsibility for the integrity and management of the institute's data. This is delegated to the Custodians (who may delegate further to the Data Stewards) in their respective areas of expertise. The data management delegation schedule is provided in this policy.

1.4 Definitions

- a **Data Governance:** framework of policies, processes, and standards that ensure the effective and efficient use of data within an organization. It involves managing data's availability, usability, integrity, and security to meet regulatory requirements and support business objectives.
- b **Custodian:** a member of Te Kahui Manukura (TKM) responsible for the collection and dissemination of data in an information system. The Custodian is primarily responsible for the business function supported by a business system and the data used by it.
- c **Data:** The data that resides in the databases, and information storage, associated with the important and business critical applications for the organisation. Data includes but is not limited to – information, shared data about managed entities, interests, finances, employees, resources, customers, students, metadata, providers, business affiliates.
- d **Data Classifications:** The following data classifications have been established to inform the access and utilisation of data within the organisation.

All policies on Waituhi are the current version. Please check date of this hard copy before proceeding.

- i. **Unclassified:** Can be shared externally without restrictions (e.g., marketing material). Policy: Document can be printed, saved, or emailed externally and is available for Copilot.
 - ii. **Internal (default):** Internal use only (e.g., strategy details, project plans). Policy: Document can be printed but not emailed or saved externally and is available for Copilot.
 - iii. **Confidential:** Sensitive information that needs to be shared externally (e.g., student support plans). Policy: Document can be printed or emailed (with a warning) but cannot be saved externally and is available for Copilot. Justification is required to lower classification.
 - iv. **Restricted:** Information that is sensitive and should not be shared externally (e.g., financial reports). Policy: The document can be printed (with a warning) but cannot be emailed or saved externally and is not available for Copilot. Justification is required to lower classification.
- e Data Steward:** An individual who is responsible for the definition, management, control, integrity or maintenance of a data resource. This role will be assigned to an existing senior user/administrator of the system, which produces the data, who has a good understanding of the data and its application.
- f Data Integrity:** Data that has a complete or whole structure. All characteristics of the data including business rules, rules for how pieces of data relate, dates, definitions and lineage must be correct for data to be complete.
- g Disaster Recovery:** the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organisation after a natural or human-induced disaster.
- h Information:** data that has been processed into a meaningful form.
- i Interfaces:** a point of interaction between two systems (or applications).
- j Meta-data:** data that describes data e.g. data format, meaning, source, application etc.
- k Referential Integrity:** a property of data which, when satisfied, requires every value of one attribute (column) of a relation (table) to exist as a value of another attribute in a different (or the same) relation (table).
- l Replication:** the use of redundant resources to improve reliability, fault-tolerance, or performance. This can refer to both databases and supporting technology e.g. server hardware.

<p>Related Ara Ltd Procedures (indicate if attached to policy or where they can be found)</p> <ul style="list-style-type: none"> • CPP105a Code of Conduct for ICT Users • 	<p>Related Ara Ltd Policies</p> <ul style="list-style-type: none"> • CPP105 Acceptable Use and Conduct for ICT Users • CPP109 Disclosing Personal Information about Students and Staff • CPP110 Legislative Compliance • CPP114 Records and Archives CPP121 ICT Security Policy
<p>Related Legislation or Other Documentation</p> <ul style="list-style-type: none"> • Privacy Act 1993 • Public Records Act 2005 	<ul style="list-style-type: none"> • Organisational standard operating procedures
<p>References</p>	
<p>Notes</p>	

All policies on Waituhi are the current version. Please check date of this hard copy before proceeding.

- Database modelling and classification standards (as referenced in 2.2-2.6) will be created at a later date (as of February 2025).

2 Principles

2.1 All Data is the Property of the Institution

Ara Ltd, rather than any individual or business unit, owns all data.

2.2 Data Will Be Modeled

Where possible, all databases shall be modeled, named, and defined consistently (according to standards) across the business divisions of the organisation. Every effort must be made by management to share data across divisions and to avoid redundancy. Data Stewards must recognise the informational needs of downstream processes and business units that may require said data.

2.3 Data Must Be Maintained Close to Source

All data shall be created and maintained as close to the source as feasible aligned to consistent data input standards. Data quality standards shall be managed and applied actively to ensure approved reliability levels of data as defined by the Data Stewards e.g. compulsory field validation on all data sets.

2.4 Data Must Be Safe and Secure

Data in all formats shall be safeguarded and secured based on recorded and approved requirements and compliance guidelines as per data classification standards. These requirements are to be determined by the data stewards and validated by the Management Team. Appropriate availability, backups and disaster recovery measures shall be administered and deployed for all databases.

2.5 Data Must Be Accessible

Internal data and information about that data (metadata) shall be accessible . Data will be internally accessible except when determined to require controlled access as per data classification standards. When restrictions are made, data stewards are accountable for defining specific individuals and levels of access privileges that are to be enabled.

2.6 Meta-Data Will Be Recorded and Utilised

All information system development and integration projects will utilise a consistent metadata method for data naming, data modeling, and logical and physical database design purposes.

2.7 Custodians Will Be Accountable for Data

Custodians will be senior staff members with delegated accountability for the collection, dissemination and security of data. They will be accountable for:

- a Legislative compliance
- b Data use
- c Data quality
- d Data security
- e Data Privacy
- f Change management

2.8 Data Stewards Will Be Responsible for Data

All policies on Waituhi are the current version. Please check date of this hard copy before proceeding.

Individuals recognised as business definers, producers, and users of data will be designated "Data Stewards". Data Stewards are those individuals ultimately responsible for the definition, management, control, integrity or maintenance of a data resource. Data Stewards are aware of compliance requirements pertaining to the data held (e.g. Privacy Act 1993, Public Records Act 2005, etc) and aware of their regulatory obligations arising from those regulations.

2.9 Data Stewards will have responsibility through their job description.

3 Associated procedures for

Ara Ltd Corporate Policy on: Data Governance

Contents:	3.1	Data Standards and Procedures
	3.2	Access to Data
	3.3	Authority over Data
	3.4	Data Integrity
	a	Referential Integrity
	b	Integrity of Application Software
	c	Integrity of Content
	d	Integrity of Process
	3.5	Interfaces
	3.6	Migration
	3.7	Data Management
	3.8	Version Control
	3.9	Change Control
	3.10	Replication
	3.11	Backup, Recovery and Restore
	3.12	Disaster Recovery
	3.13	Retention requirements
	3.14	Destruction protocols
	3.15	User Responsibilities
	3.16	Skills and Training
	3.17	Corporate Information Systems Delegation Schedule

3.1 Data Standards and Procedures

The following data standards have been developed for the Ara Ltd environment. It is expected that these standards will provide guidelines for all staff, students, and stakeholders when working with Ara Ltd data.

3.2 Access to Data

“Access” to data is the ability to view, retrieve, alter, or create data. The Custodians will establish and maintain access rules for data and business documents under their control. Access rules must be based on the principle of public and equitable access to information unless explicit reasons preclude this. Access with the ability to alter or create data is likely to be different, and more restrictive, than that for view/retrieve. Where data is held in multiple physical databases e.g. for analysis purposes or technical performance reasons, Te Kahui Manukura (TKM) will designate the master source of the data which will always take precedence should conflict in data values occur.

Data element content and business documents will be retrievable in formats that meet open international standards. Technology will be supported for future retrieval of data.

Compliance with Ara Ltd “Access to Data” standards is required for all users.

3.3 Ethical Data Use

All policies on Waituhi are the current version. Please check date of this hard copy before proceeding.

Ara Ltd will ensure it is employing an ethical approach to data usage that aligns with the expectations of the Ara Ltd community. Using data ethically will enable Ara Ltd to uphold privacy rights and individual rights arising from data, while also providing a framework to engage in an agile way with the ethical issues that naturally arise in an evolving data landscape.

3.4 Authority over Data

Ara Ltd has authority over use of the organisation's physical computer assets. Ara Ltd is the legal custodian of all data that is collected or generated during the execution of the Institute's business processes.

The Chief Executive or delegate is responsible for protecting Ara Ltd data at the level appropriate for its sensitivity, as per the data classification standards.

Ara Ltd data will only be shared between internal systems or with other organisations with management approval, Limited unclassified data will be publicly available once approved at this level, and will remain so unless determined by relevant management or data custodian.

Compliance with Ara Ltd "Authority over Data" standards is required for all users.

3.5 Data Integrity

Data and business documents will be managed to preserve and demonstrate their authenticity, integrity and retrievability to meet business and statutory requirements. This includes both the logical and physical integrity of data and document stores and their contents. In order to present consistent information both internally and externally, document and data stores must be managed as a coherent whole. This means:

- All data stores are known & documented
- Duplication of content between stores is minimised and controlled
- The original content, context, and structure of documents is preserved
- Authorised activities are permitted
- Unauthorised activities are prevented
- Relevant events are logged as determined by business or legislative requirements
- Content is retrievable in a usable format.

a Referential Integrity

Data Stewards must ensure that systems are put in place to maintain the context of data elements in database structures.

b Integrity of Application Software

The integrity of any application software operating on approved data stores will be monitored at appropriate intervals, and action taken to repair and prevent defects.

c Integrity of Content

Where users enter data into a data store, validation at the time of input is required wherever practical.

Processes must be in place to monitor and correct errors in the data and metadata.

Any changes to the use of data or metadata fields must be agreed with the relevant Data Steward and documented and effects on downstream systems taken into account.

All policies on Waituhi are the current version. Please check date of this hard copy before proceeding.

d Integrity of Process

Ara Ltd must be able to demonstrate that their processes fully capture the required data elements, that business rules and standard operating procedures are in place for their management and that they have been implemented.

Compliance with Ara Ltd "Data Integrity" standards is required for all users.

3.6 Interfaces

Electronic interfaces between systems must use mechanisms based on open industry standards as specified in the Ara Ltd information technology policies and standards. Redundant or non-standard interfaces will be phased out over time.

3.7 Migration

Data stores will be constituted such that all content, structure and metadata can be migrated to a different environment without loss of integrity. In the event of a migration or major upgrade, migration plans will be produced and require appropriate approval.

3.8 Data Management

Data Stewards have responsibility for data management within institutional business systems. Metadata will be collected for all databases and must be sufficient to describe the document, dataset, or data store, and to establish its validity and relevance for business or evidential purposes. Capture of most metadata for business documents is best undertaken at the time they are created or received, usually by the individual involved.

Data and business documents will be managed within a defined retention process, as per the formal retention and disposal schedule for the institute.

3.9 Version Control

Ara Ltd will determine business rules for version control of data elements and data sets. Rules will be built into systems or expressed as guidelines for users.

3.10 Change Control

Change control procedures will be applied to the structure of data stores and the business processes that affect them, to ensure the contextual integrity of current content and that historical material maintains its integrity. This includes being cognisant of Applications that create or maintain data and interfaces to downstream systems.

3.11 Replication

Replication of data will be controlled by the Data Stewards involved and will only come from prime authoritative data sources. All replication arrangements will be auditable to ensure that a true replica is made.

3.12 Backup, Recovery and Restore

Ara Ltd will have a backup regime for data stores to insure against system failure or human error. Backup operations will be regularly monitored for completeness and tested for retrievability.

All policies on Waituhi are the current version. Please check date of this hard copy before proceeding.

3.13 Disaster Recovery

Ara Ltd will endeavour to develop systems and plans to ensure that the business can reconstitute data stores to enable timely re-establishment of business operations in the event of a disaster. These plans and systems will be tested to ensure they are fit-for-purpose.

3.14 Retention requirements

Ara Ltd must identify, describe and comply with their retention and destruction requirements for data elements as per legislative requirements, including the Public Records Act (2005).

3.15 Destruction protocols

No data will be destroyed while it is needed to fulfil the statutory or business requirements of Ara Ltd. Any deletion or destruction process must be secure, deliberate, authorised and auditable.

Compliance with Ara Ltd "Data Management" (3.8) standards is required for all users.

3.16 User Responsibilities

Users of Institute data include but are not limited to the following categories:

- a Institute employees
- b Volunteers
- c Contractors
- d Vendors
- e Partners
- f Students

Individual Institute Users play a critical role in ensuring the security of Institute Data. Ultimately, only the User can prevent unauthorized access and ensure responsible use of the data. Proper use of data, including assurance of security and privacy, is a requirement for all Institute employees and should be included in all Institute agreements providing access to Institute Data, and is a condition of enrolment for students.

a Users are responsible for the following actions

- i Store data under appropriately secure conditions for the data classification level
- ii Make every reasonable effort to ensure the appropriate level of data privacy is maintained
- iii Use the data only for the purpose for which access was granted
- iv Not to share identities or passwords with other persons
- v Securely dispose of sensitive Institute data

Must follow CPP121d ICT Asset and Media Security Standard.

Compliance with Institute "User Responsibilities" standards is required for all users (3.16).

3.17 Skills and Training

Staff will be trained in their responsibilities when working with Ara Ltd data. These responsibilities will be written or referred to in Job Descriptions and Performance Agreements, for staff at all levels.

All policies on Waituhi are the current version. Please check date of this hard copy before proceeding.

3.18 Corporate Information Systems Delegation Schedule

(as defined by Te Kahui Manukura (TKM))

Student Management System	
Custodian	Director – Strategy, Planning, Performance
Data Steward	Head of Student Administration Services
Data Experts	Team Leaders, Admissions & Enrolments Manager, International Admissions Team Leader, Curriculum & Academic Records Team Leader, Registry Manager, Student Information Systems
Ceridian aPay	
Custodian	Director – People & Culture
Data Steward	Manager - Services, Systems & Compliance, HRS
Data Experts	Team Leader Payroll
Dynamics 365	
Custodian	Director – Corporate Services
Data Steward	Manager, Finance
Data Experts	Management Accountants
Asset Management – BEIMS	
Custodian	Director – Corporate Services
Data Steward	Manager, Facilities Management
Data Experts	Manager Services
Learning Management System – Moodle	
Custodian	Director – Strategy, Planning, Performance
Data Steward	Head of Digital
Data Experts	Digital Learning Environments team
Learning Object Repository – Te Kete	
Custodian	Director – Strategy, Planning, Performance
Data Steward	Head of Digital
Data Experts	Digital Learning Environments team
Content Management System – Optimizely	
Custodian	Director – Strategy, Planning, Performance
Data Steward	Manager, Marketing
Data Experts	Web team
Communications – Exchange, Teams telephony, Zoom etc	
Custodian	Director – Strategy, Planning, Performance
Data Steward	Head of Digital, Information Systems Manager
Data Experts	Digital team
Library – ALMA	
Custodian	Director – Ākonga Success
Data Steward	Manager - Academic Support
Data Experts	Manager – Library & Information Services
Streaming Video – Panopto	
Custodian	Director – Strategy, Planning, Performance
Data Steward	Head of Digital
Data Experts	Digital Learning Environments team
Microsoft 365	
Custodian	Director – Strategy, Planning, Performance
Data Steward	Head of Digital, Information Systems Manager
Data Experts	Digital team

All policies on Waituhi are the current version. Please check date of this hard copy before proceeding.