Data Governance Policy

First Produced:	17/07/13	Authorisation:	Te Kāhui Manukura
Current Version:	19/10/18		
Past Revisions:	17/07/13	Officer	
Review Cycle:	3 year cycle	Responsible:	DCE Chief Operating Officer
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.

1.2 Scope and Application

The policy applies to all staff of Ara Institute of Canterbury[1]. It also applies to contractors, consultants and visitors engaged to work with, or who have access to Ara information. Policies also apply to students and any specific exclusion's for students are identified within the 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.

1.4 Definitions

a **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.

b **Data:** The data that resides in the databases associated with the important and business critical applications for the organisation. Data includes, but is not limited to - shared data about managed entities, interests, finances, employees, resources, customers, students, providers, business affiliates.

c **Data Classifications:** The following data classifications have been established to inform the access and utilisation of data within the organisation.

i **Public Data:** Available to general public with no access control or identification required.

ii **Student Data:** Data available to students as a right of enrolment. This includes general student data and data of relevance to the individual student.

[1] Refers to Ara from herein.

iii **Institutional Data:** Proprietary data, data for general administration. Primarily for internal usage, not for student or external distribution.

iv **Protected Data:** Data to be used only by individuals who require it for their jobs. Data containing sensitive personal or confidential information, commercially sensitive information or other information that would usually be regarded as sensitive information. Protected data must be managed in accordance with the relevant statutory obligations such as the Privacy Act 1993 (New Zealand Legislation website).

d **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.

e **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.

f **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.

g **Information:** data that has been processed into a meaningful form.

h **Interfaces:** a point of interaction between two systems (or applications).

i **Meta-data:** data that describes data e.g. data format, meaning, source, application etc.

j **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).

k **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.

Related Ara Procedures(indicate if attached to policy or where they can be found) • CPP105a Code of Conduct for ICT Users •	**Related Ara Policies** • 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
Related Legislation or Other Documentation • Privacy Act 1993 • Public Records Act 2005	**Good Practice Guidelines**(indicate if attached to policy or where they can be found) •
References •	
Notes	

2 Principles

1.1 All Data is the Property of the Institution

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

1.2 Data Must Be Modeled

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 of databases must recognise the informational needs of downstream processes and business units that may require said data.

1.3 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.

1.4 Data Must Be Safe and Secured

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.

1.5 Data Must Be Accessible

Data and information about that data (meta-data) shall be readily accessible to all. data will be public except where determined to have 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.

1.6 Meta-Data Will Be Recorded and Utilised

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

1.7 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

1.8 Data Stewards Will Be Responsible for Data

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,

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

Public Records Act 2005, etc) and aware of their regulatory obligations arising from those regulations.

1.9 Data Stewards will have responsibility through their job description.

2 Associated procedures for

Ara Corporate Policy on: Data Governance

Contents:

2.1 Data Standards And Procedures

The following data standards have been developed for the Ara environment. It is expected that these standards will provide a guideline for all staff and vendors when working with Ara data.

2.2 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 "Access to Data" standards is required for all users.

2.3 Authority over Data

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

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

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

Ara data will only be shared between internal systems or with other organisations with management approval.

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

2.4 Data Integrity

Data and business documents will be managed to preserve and demonstrate their authenticity, integrity and retrievability to meet business and statutory requirements. These procedures cover 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.

d Integrity of Process

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

2.5 Interfaces

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

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

2.6 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.

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

2.7 Data Management

Data Stewards have responsibility for data management of data 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.

2.8 Version Control

Ara 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.

2.9 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.

2.10 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.

2.11 Backup, Recovery and Restore

Ara 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.

2.12 Disaster Recovery

Ara will have a fully tested disaster recovery plan to reconstitute data stores to ensure timely re-establishment of the business.

2.13 Retention requirements

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

2.14 Destruction protocols

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

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

2.15 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

In any disposal of media or devices, Users should ensure that techniques are applied so that unauthorized persons cannot later access sensitive data. Such techniques include, but are not limited to; erasing data from flash/pen drives or hard drives with special 'scrubber' programs, and physically destroying old media containing sensitive data. This role may be conducted by the ICT support team on behalf of the user.

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

2.16 Skills and Training

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

2.17 Corporate Information Systems

(as defined by Te Kahui Manukura (TKM)

Student Management System	
Custodian	**DCE Chief Operating Officer**
Data Steward	Manager Registry
Data Experts	Team Leaders, Admissions & Enrolments Manager, International Admissions Team Leader, Curriculum & Academic Records Team Leader, Registry
Talent2 Alesco	
Custodian	**DCE People & Culture**
Data Steward	Manager - Services, Systems & Compliance, HRS
Data Experts	Team Leader Payroll
Dynamics 365	
Custodian	**DCE Chief Operating Officer**
Data Steward	Manager, Finance
Data Experts	Management Accountants
Asset Management – BEIMS	
Custodian	**DCE Chief Operating Officer**
Data Steward	Manager, Facilities Management
Data Experts	Manager Services
Learning Management System – Moodle	
Custodian	**DCE Learning, Delivery, Innovation & Applied Research**
Data Steward	
Data Experts	
Learning Object Repository – Te Kete	
Custodian	**DCE Learning, Delivery, Innovation & Applied Research**
Data Steward	
Data Experts	
Content Management System – MySource Matrix	
Custodian	**DCE Customer Experience & Engagement**
Data Steward	Manager, Marketing
Data Experts	
Communications – Exchange, Lync, Cisco telephony, Zeacom	
Custodian	**DCE Chief Operating Officer**
Data Steward	Director, ICT
Data Experts	
Library – ALMA	
Custodian	**DCE Learning, Delivery, Innovation & Applied Research**
Data Steward	
Data Experts	Librarian Digital
Programme Repository	
Custodian	**DCE Learning, Delivery, Innovation & Applied Research**
Data Steward	Manager, Portfolio & Assurance
Data Experts	Academic Advisors

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