UC Policy Library

Data Management Policy

Last Modified	May 2021
Review Date	October 2021
Approval Authority	General Counsel | Registrar
Contact Officer	Information and Records Manager – Office of the General Counsel | Registrar

Introduction

The University operates in a complex, data-oriented environment that requires those who are responsible for collecting, managing and disseminating data to do so in a systematic, planned and managed way. Data generated and held by the University are key assets that must be managed correctly in order to ensure that the University functions effectively.

This policy outlines the data management framework that covers the roles responsible and accountable for data collection, storage, security, maintenance, dissemination and data quality.

This policy does not apply to:

- data from academic research projects or teaching activities, where these do not form part of the institutional data; or
- the collection of data for ad hoc or targeted/occasional usage via the use of surveys.

This document provides a comprehensive data management framework which is consistent across all of the University's major Line of Business Systems. 'Data management' in this instance refers to the management of institutional data i.e., data which are required for the operation of the University.

Definitions

Custodian – a member of the Senior Management Team (SMT) responsible for the collection and dissemination of data in an information system. The Custodian is typically primarily responsible for the business function supported by a corresponding line of business system and the data used by it.

Data – a general term meaning facts, numbers, letters and symbols collected by various means and processed to produce information. Data may include personal or sensitive personal elements and needs to be managed in accordance with the relevant statutory obligations such as the *Privacy Act 1993 (New Zealand Legislation website)*

Data management – the management of institutional administrative data i.e., data which are required for the operation of the University.

Data management framework – the organisational structure in place to manage the University's data resource.

Data quality – the accuracy, completeness, validity and currency of data.

Expert – technical expert.

Information – data that have been processed into a meaningful form.

Institutional Data – data relevant to the operation of the University (primarily data contained in HR, Finance, Student Management and Course Information systems i.e., excludes departmental specific and research data etc.)

Line of Business System – a system that gathers, condenses, and filters data until they become information, then makes that information available on time and in a useful form for supporting decision-making at various levels of management within an organisation. Current examples include JadeSMS, PeopleSoft and Oracle.

Steward – the person who has oversight of the use made of data and, as such, is the intermediary between users and experts.

Users – staff who use administrative data as part of their day-to-day work.

Policy Statement

Those responsible for University operations are also responsible for the institutional data that concerns the University. Maintaining the quality of this data is crucial to maximise the value of investments that the University has made in data collection and maintenance, and so that internal and external decision-makers have confidence and trust in the information they rely on.

The University is committed to the following principles of data management and expects adherence to them.

Principles of Data Management

The following principles of data management outline best practices at a high level within the University. Every Data Custodian (see below) must be aware of these, and adhere to them. This ensures contributions to data quality are being made at all levels within the University.

These principles must guide all data management procedures.

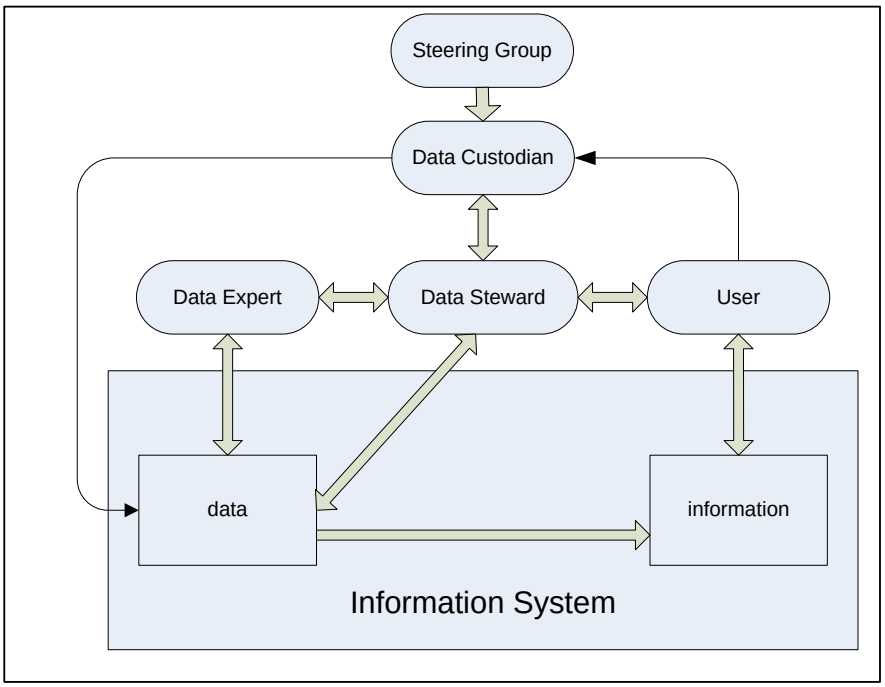
1. The University, rather than any individual or business unit, owns all data.
2. Every data source must have a defined Custodian in a business leadership role, who has overall responsibility for the accuracy, integrity, and security of those data.
3. Wherever possible, data must be simple to enter, be clearly defined and accurately document their subject. They must also be in a useful, usable form for both input and output.
4. Data should only be collected for a specific and documented purpose.
5. Data must be readily available to those with a legitimate business need.
6. Data capture, validation, and processing should be automated wherever possible.
7. Data must be entered only once.
8. Processes that update a given data element must be standard across the information system.
9. Data must be recorded as accurately and completely as possible, by the most informed source, as close as possible to their point of creation, and in an electronic form at the earliest opportunity.
10. Data should be recorded and managed over time in an auditable and traceable manner.
11. The cost of data collection must be minimised.
12. Data must be protected from unauthorised access and modification.
13. Data must not be duplicated unless duplication is absolutely essential and has the approval of the relevant Data Steward. In such cases, one source must be clearly identified as the master; there must be a robust process to keep the copies in step; and copies must not be modified (i.e., ensuring that the data in the source system is the same as that in other databases).
14. Data structures must be under strict change control, so that the various business and system implications of any change can be properly managed.
15. Whenever possible, international, national, or industry standards for common data models must be adopted. When this is not possible, organisational standards must be developed, documented and implemented.
16. Data should be defined consistently across the University.
17. Users must accurately present the data in any use that is made of them.
18. Schemas that describe the data must be developed and maintained for as long as they data that they describe are in use, and these must be maintained separately to the systems that manage the data.

Data Management Roles and Accountabilities

In order to ensure that data are consistent, correct, and available to those with legitimate requirements, the establishment of the following data management roles for each major

Line of Business System is necessary. This establishes a data management framework which is consistent across the University.

Figure 1: Data Framework:



The Information Governance Group is charged by the Vice-Chancellor with acting as a governance body (steering group) in relation to the University's information environment.

The **Data Custodian**, holding delegated authority from the Vice-Chancellor, is responsible for the business function the Line of Business System performs and all of the data associated with it.

The **Steward** has oversight of the data use/s and is thus the intermediary between experts and users.

The **Data Expert** is primarily concerned with data and the technical aspects surrounding data management.

The **User** works with administrative data and where necessary, transforms this into information.

Information Governance Group

The purpose of the Information Governance Group is to ensure that the University's Information Strategy and related policies are given effect; and that the University develops the frameworks and environments from which benefits and efficiencies can be realised,

while mitigating risks and issues associated with managing significant information holdings.

With respect to data management, the purpose of the Information Governance Group is to:

- oversee the Data Management Framework (see above), and ensure its alignment with other University information management initiatives and strategies;
- ensure systems are compliant with University policies and external mandates;
- oversee and report on risks to information assets (including data);
- advise key stakeholders on data management risks and issues;
- oversee implementation and compliance with this policy; and
- ensure proper and effective coordination of the operation and outputs of all University Line of Business Systems, and adjudicate on disputes that may arise from time to time.

Data Custodian

The Data Custodian is an SMT member with delegated responsibility from the Vice-Chancellor for the collection, dissemination and security of data in a major information system.

The establishment of the Data Custodian role is based on two key concepts:

1. Data are critical to the University and must be shared across the University.
2. Data assets must be coordinated across the University at the highest level to ensure maximum return on investment.

The overriding philosophy of data custodianship should be one of a trustee acting in partnership with all participants. Custodianship reinforces the concept of one individual being ultimately responsible and accountable for the information that others might use. The Data Custodian provides guidance, decision-making and leadership for the Data Stewards (below), so that University-wide information needs are met.

Data Custodians are senior members of staff within the University. They are not expected to carry out the necessary work themselves; their role is to ensure that visibility and responsibility for their data is articulated from a senior level to ensure progression towards a common goal of high quality and clearly defined data. Actions should be guided by the principles of data management outlined above.

Responsible for:

- understanding legislation and University policies surrounding data e.g., privacy, protected disclosures, communications, official information, records management, as well as consequences of misuse of data, the legal and administrative consequences of maintaining and disseminating data within their custody;
- corporate use of data, in both uploading and downloading data;

- data quality;
- security;
- customised business interpretations (and negotiates with Data Steward for delivery of reporting functions); and
- change management – will provide advance notice of proposed business changes and corresponding impacts on data structures, and will negotiate resources necessary to implement the change (i.e., the Data Custodian is the one who decides the necessity for change rather than the Data Steward or the Data Experts).

Data Steward

The Data Steward coordinates Data Experts (outlined below) and business users from across the University. By using their knowledge and collective views about the data and issues faced by the user community, issues can be addressed in a University-wide context. The Data Steward must understand the larger business context in which the data will be used and should be able to relate University user needs to specific technical capabilities and requirements.

Responsible for:

- ensuring data in each system are accurate, complete, valid and up-to-date;
- working with Data Experts to define appropriate nomenclature, data definitions, and documenting these;
- working with system designers, data experts and technical experts on applying business rules governing data migration and data retention and disposal and permissions/access management;
- data quality monitoring; and
- maintenance of data quality and security.

Tasks within relevant Administrative Systems:

- establish procedures governing data elements;
- establish access authorisation procedures;
- determine and evaluate the most reliable source of data;
- make data dictionary understandable to users;
- ensure that only needed versions of each element exist;
- assign responsibilities for data integrity;
- resolve conflicts involving shareable data;
- consult with users on use of electronic data;
- analyse and enhance data quality;

- maintain direct expertise in the data set;
- control data entry into a system;
- maintain data integrity;
- develop and maintain standard entity definitions;
- develop standard attribute definitions;
- document data definitions, calculations, summarisations, etc.;
- provide customised reporting;
- establish data security specification; and
- apply data retention criteria.

Data Experts

These are staff with detailed technical knowledge and experience in their respective data processing and application areas. They understand the technical framework supporting the University's data processing and management activities.

Data Experts cannot act as Data Stewards or Data Custodians because those positions are responsible for the University operations and are also responsible for the institutional data concerning these operations.

Responsible for:

- delivering data and providing the infrastructure, security and data framework for delivering quality data in a timely fashion to University clients;
- carrying out data quality analyses;
- ensuring technical security; and
- deploying the requisite technology.

Users

Everybody who uses data throughout the organisation must understand their role in data quality and be able to provide feedback that will help prevent bad data habits spreading throughout the University. It is important that users are aware of the many uses of data in order to understand how crucial high quality data are to the operation of the University.

Security

The University acknowledges an obligation to ensure appropriate security for all institutional data in its domain of ownership and control.

Application level security at the University is generally well set up and managed. This policy ensures consistent application of the same security across all information systems within the University. Security must be directly related to the category in which data are classified. These categories being: public data, general administrative data, protected data, and restricted data.

There are two aspects surrounding the security of administrative data:

1. **Data security** – refers to user access, and the amount of access each user is allowed. Data security is administered by Data Custodians (or by delegation to Data Stewards). The technical security framework is the responsibility of Data Experts.

2. **Physical security** – Data Users throughout the University must understand that certain information is privileged and should be kept secure. Physical security is important to ensure unauthorised access does not occur. Physical security is the responsibility of all staff.

Related Documents and Information

Legislation

- Privacy Act 2020 (New Zealand Legislation website)

UC Policy Library

- IT Policy Framework (PDF, 305KB)
- Official Information Policy (PDF, 347KB)
- Privacy Policy (PDF, 823KB)
- Protected Disclosures Act: Internal Procedures and Code of Conduct (PDF, 416KB)
- Records Management Policy (PDF, 325KB)
- Student Community Online Survey Policy (PDF, 300KB)
- UC Web Policy (PDF, 219KB)

Document History and Version Control Table			
Version	**Action**	**Approval Authority**	**Action Date**
For document history and versioning prior to 2013 contact ucpolicy@canterbury.ac.nz			
1.00	Conversion of document onto new template and document pushed out	Policy Unit	Aug 2013
1.01	Change of contact officer and hyperlinks updated.	Chief Information Officer, ICTS	Oct 2013
1.02	Document review date pushed out	Policy Unit	Feb 2014
1.03	Hyperlinks updated.	Policy Unit	Jul 2014
1.04	Review date pushed out	Policy Unit	Sep 2014
2.00	Scheduled review by Contact Officer - updated to reflect organisational changes	University Registrar	Aug 2015

2.01	Reference to Computer Use Policy and Procedures changed to IT Policy Framework.	Policy Unit	Sep 2015
2.02	Review date moved to Oct 2018 due to IRM initiatives needing to be finalised before the policy is updated.	Policy Unit	June 2018
2.03	Review date pushed out	Policy Unit	Nov 2019
3.00	Schedule review, no changes to substantive content	Policy Unit	Sep 2020
3.01	Review date pushed out for 6 mths	Policy Unit	May 2021

This document remains in force until it is updated.