DATA MANAGEMENT POLICY

Section	Information Technology Services
Contact	Data Management Specialist
Last Review	N/A
Next Review	July 2017
Approval	SLTWH 24/11/2014 Item 2C
Effective Date	1 July 2015

Purpose:

The purpose of this policy is to ensure that data management responsibilities and principles apply to the management, security and use of Massey University's corporate data assets and forms part of Massey University's internal control and corporate governance arrangements.

Scope:

All University staff or anyone performing work on behalf of the University, including contractors, consultants and volunteers, must comply with this policy. This policy extends to its affiliated organisations, including its controlled entities, namely business enterprises and research centres majority owned by the University, and as defined in the *Controlled Entities Governance Framework Policy*.

This policy applies to all corporate data that in respect of which Massey has rights regardless of:

- form – electronic or printed; structured or unstructured
- media – internal network, cloud or hosted by a vendor
- source – primary, duplicated, business intelligence or a republished copy.

The focus of this policy is primarily institutional data. Management of data associated with academic research activity will be covered by the Research Data Management Policy which will address the specific requirements at a more detailed level.

Rights:

The University asserts its rights in respect of all data that is created and captured during the operation of the University. All corporate data must be managed therefore individual units or departments may have stewardship responsibilities for a defined segment of data. The University asserts its rights in respect of all research data generated by research projects conducted at or under the auspices of the University regardless of funding source, unless specific terms of sponsorship, other agreements or University policy supersede these rights.

Principles:

Massey University is committed to the implementation of data management practises which are based on the following principles[1].

Name	Statement	Rationale (the value)	Implications (the resources)
Data is a managed asset	Data is an asset that has value to the organisation, and as such is managed accordingly. Each data set has a custodian and steward that ensures the data is fit for purpose.	Data has a real measurable value. Data supports decision-making so accurate and timely data is critical to accurate and timely decisions. The Data Custodian has management responsibility while the data steward manages data at a day-to-day level; ensuring data quality.	• Create an Information Management Strategy to identify opportunities, reduce business risk and align information investment to the business strategy. • Need to educate users to appreciate the value in accurate data that is fit for purpose. • Sources of data need to be identified, classified and assigned a Data Custodian. • Data Custodians must have the authority and means to manage the data for which they are accountable. • Data Stewards are essential because incorrect on inconsistent data could be used in decision making. • Procedures need to be developed to prevent and correct errors.
Data is shared	Users have access to the necessary data to perform their duties; therefore data is shared across enterprise functions and applications while maintaining security and data integrity.	Data is shared across the University to improve the quality and efficiency of decision-making. It is more cost effective to maintain data in a single application and then share it to multiple applications.	• To enable this we must develop and abide by a common set of policies, procedures and standards governing data management and access. • Need to document our data including data models and metadata and make it accessible. • Need to develop common methods and tools for sharing data e.g. application integration. • Under no circumstances will sharing data cause confidential data to be compromised.
Data is accessible	Users are able to use the data to perform their functions.	Data is available to the widest range of users for the widest range of purposes. Access to data leads to efficiency	• Accessibility includes the ease with which users can access the data and obtain information. • It must be sufficiently adaptable to meet a wide range of users.

[1] Based on the data principles from the Open Group (2013). *TOGAF Version 9.1.* Van Haren Publishing

Name	Statement	Rationale (the value)	Implications (the resources)
		and effectiveness in decision-making. Staff time is saved and consistency of data is improved.	• Users need to take responsibility to understand the data and caution not to misinterpret it. • Access does not mean privileges to modify or disclose the data.
Data is understood	Data is defined consistently and the definitions are understandable and available to all users.	Data used in applications must have a common definition to facilitate communications and sharing of data.	• Critical to improving information. • All data needs to be defined and the definitions need to be available to all users. • When a new data definition is required the effort is co-ordinated and reconciled with the University's metadata repository, which includes the glossary of terms.
Data is secure	Data is protected from unauthorised access, use and disclosure.	Restrict availability of information, where required, via privacy rules and relevant legislation.	• All data needs to be classified, including duplicated, aggregated and/or transformed data, and indicate if it contains personal information. • In order to adequately provide access to open information while maintaining secure information, security must be identified and developed at the data level, not the application level while ensuring that data is shared and available as required. • Security needs to be designed at the beginning. Applications, data and technologies must be protected from unauthorised access. • Data sources containing personal identifiable information (PII) and/or private information must be inventoried.

Policy:

All corporate data must be managed and as such have representation by all the groups mentioned below. These are delegated responsibilities and ownership of data is retained by the Senior Leadership Team (SLT) of Massey University. The Data Governance Committee will sponsor and oversee the implementation of the Data Management Framework.

The Information Technology Services department is responsible for:

- promoting the value of University data for enterprise use while facilitating sharing, integration and security
- providing data architecture services that leverage a data reference model, manage an enterprise data classification and create an inventory of corporate data assets

- documenting, managing and distributing data models (conceptual, logical and/or physical) of University data including relevant metadata and data integration
- designing and managing processes for maintaining the integrity, accuracy, timeliness, consistency, standardisation and value of data including master data management
- providing advice and support for the data stewards, data custodians and the data governance committee members
- designing, managing and implementing data management policies, standards and frameworks in consultation with relevant key stakeholders
- creating and/or reviewing database designs that align with relevant standards ensuring the principles are applied e.g. access and security
- providing storage infrastructure and operational database support including managing the database management system platform, backing up databases and monitor/improve database performance
- providing guidance on use and implications of the different storage options to ensure it is fit-for-purpose
- ensuring appropriate procedures and systems are in place to support business continuity and disaster recovery.

The Data Custodians are responsible for:

- assigning Data Stewards for data in their area of responsibility and allowing time for them to complete relevant tasks
- managing and resolving data related issues that cannot be resolved by the Data Steward
- authorising security classification of assigned data, e.g. public, restricted
- authorising access to assigned data and its usage in other systems
- identifying and registering personally identifiable information (PII) contained in data sources
- applying and managing the ethical processes (where required)
- ensuring that data is fit-for-purpose including defining data quality levels, metrics, business rules and facilitating data integration.

The Data Stewards are responsible for:

- implementing and monitoring access to corporate data in accordance to approved business rules and processes
- developing business terms and definitions (metadata) for assigned data sets and attributes, and ensuring that they are properly reviewed and approved in alignment with the Data Governance Framework
- implementing and maintaining data quality requirements and business rules for assigned data sets
- identifying and helping to resolve data issues, risks and errors (escalating to Data Custodian when required)
- arranging appropriate training for staff to ensure that data is captured and used accurately and appropriately
- providing input into data policies, standards and procedures
- managing, mitigating and, where necessary, escalating data related risks
- providing advice and permission for data when it is republished, duplicated or integrated with other systems
- assisting users to ensure relevant data complies with the Records Management Policy
- ensuring that all data that is not a record has an appropriate retention and disposal schedule
- championing the implementation of data management standards and processes.

The Data Governance Committee members are responsible for:

- defining the strategic enterprise data priorities
- reviewing, approving and applying architecture practises
- approving and endorsing any data policies, processes, standards and guidelines
- planning and sponsoring data management projects and services

- communicating and promoting the value of data assets
- managing and resolving data related issues that cannot be resolved by the data custodian
- monitoring compliance to policies, standards and regulatory legislation.

Users are responsible for:

- complying with data management policies, processes and standards
- ensuring that all data access and usage is relevant and appropriate to the work being undertaken
- observing any access controls or security restrictions that apply to the data to which they have access, and only working within the data access boundaries that they have been permitted
- preventing any unauthorised access to data to which they have access rights, and ensuring that confidential or restricted data is always protected without disclosure to any unauthorised persons.

Retention and Disposal:

The University's corporate data may often reside in University records or may of itself be a University record. The retention and disposal of this type of institutional data must be managed in accordance with the Records Management Policy and the approved Retention and Disposal schedule. The responsibility for retention and archiving of research data lies primarily with the Principal Investigator of a research project.

Definitions:

Business intelligence is a set of theories, methodologies, architectures, and technologies that transform and integrate raw data into meaningful and useful information that provides the business community easy access to data that supports decision making.

Data (corporate) is facts, figures or individual pieces of information that is captured through the operation of the University and can be words, numbers or images etc. Data is the raw detail that can be used to represent information or, from which, information can be derived. All data needs to be managed regardless of what type it is. The types are: structured or unstructured.

Data Custodian is an individual who is a Senior University staff member who has planning and policy-making responsibilities for data within their functional areas and management responsibility for defined segments of corporate data. They are expected to undertake any strategic work on data management.

Data governance is the formal management of data assets through the establishment of processes, maintenance of common standards and exercising positive control; it includes managing, improving, monitoring and protecting an organisation's data and information. This then supports business intelligence and master data management initiatives, facilitates migration of legacy data, meets compliance and legislative requirements and improves corporate flexibility and business agility.

Data Governance Committee is the strategic decision making body for data governance and oversees the implementation of the Data Management Framework. It is the cross-functional team that makes policy decisions and includes senior representation for core services, records management, privacy officer and technical stakeholders.

Data management is the function that develops, manages and executes policies, processes, standards and frameworks that collect, protect, deliver, and enhance the value of data and information assets to meet the data availability, quality and security needs of the University.

Data quality includes accuracy, completeness, timeliness, trustworthiness, business rules compliance, consistency and ability to integrate.

Data reference model is a data architecture framework to enable information sharing and reuse by standard description and identification of common data. It promotes good data management practises. The reference model at Massey leverages the framework developed by the American Federal Government.

Data Steward is an individual who is a subject matter expert that does the day-to-day management of the operational requirements, data quality, compliance with requirements, conformance to policies and standards, security controls, and identifying and resolving data issues. They undertake any operational work on data management.

Duplicate source means a copy of the primary source often used for integration and/or reporting. The duplicated data may have been changed or aggregated through a managed extract, transform and load process.

Ethical processes apply to all research and relate to how data is collected, stored, accessed and managed. The ethical requirements for data may differ, and supersede, from that stipulated in the data management policy document.

Enterprise Data Classification provides a framework with definitions and diagram conventions for data models. It is a hierarchy that is also used to recognise the different data types, apply master data management and data governance. There is only one enterprise data classification that is then used for multiple conceptual and physical data models.

Information is data that has been interpreted so that it has meaning for the user.

Institutional Data is defined as all data created, captured, or managed by the University during its course of operation. It includes data used for planning, managing, operating, or auditing an administrative function of the university.

Metadata is structured data that describes and/or enables finding, managing, controlling, understanding or preserving other information over time. Metadata includes, but is not restricted to, characteristics such as the content, context, structure, access, and availability of the data.

Personally Identifiable Information (PII) is data contained in University systems that is private information as defined by the Privacy Act.

Primary source means the official University record for the relevant data.

Record means information, in its original form or otherwise, including (without limitation) documents, signatures, seals, text, images, sound, speech, or data created, received and/or maintained by, or on behalf of, Massey University in the conduct of its affairs. Records can be compiled, recorded or stored in written form on any material, including film, negative, tape, or any other reproducible medium, or by means of recording devices, computers or any other electronic device or process which makes them machine-readable.

Structured Data is data that resides in a fixed field or file e.g. data contained in databases and spreadsheets. This data is often generated during business transactions and is stored in a business information system e.g. student data which is stored in a student management system (SMS) or financial data which is stored in a financial management system (TechnologyOne).

Unstructured Data is data that does not have a pre-defined data structure that is easily readable by machines e.g. audio, video and unstructured text. Unstructured data may have structured elements e.g. metadata associated with an email, xml document.

Audience:

All Massey staff and its affiliated organisations, including its business enterprises such as wholly owned subsidiary companies, joint venture companies, partnerships, trusts and research centres.

Relevant legislation:

- Privacy Act 1983
- Electronic Transactions Act 2002
- Public Records Act 2005
- Official Information Act 1982
- Public Finance Act 1989
- Copyright Act 1994

Legal compliance:

- *Privacy Act 1983*
  Establishes a set of privacy principles to ensure the protection of personal privacy in respect of both public and private sector organisations. The Act is of prime importance and should be clearly understood by all information management professionals.
- *Electronic Transactions Act 2002*
  This act addresses the legal implications and requirements for the use of information in electronic form or communicated electronically.
- *Public Records Act 2005*
  Provides for the selection of public records and archives for creation, maintenance and retention. Directs that public records and archives may only be destroyed or disposed of with the authority of the Chief Archivist. Provides for the deposit of public archives with the Archives of New Zealand and describes conditions for the management of material so deposited. Sets out the powers of the Chief Archivist in respect of current public records.
- *Official Information Act 1982*
  Provides for access to official information, except where specific reasons for withholding it exist, such as national security or the protection of personal privacy.
- *Public Finance Act 1989*
  Covers the reporting requirements of the Crown, Government Departments and Crown Entities, including requirements for Audit Office issuing of Audit Opinions.
- *Copyright Act 1994*
  Contains references to the requirements for documenting copyright in original works, transferring copyright and licensing for use/copying. Includes documentation requirements for hearings of the Copyright Tribunal. Copyright Regulations also apply.

Related procedures / documents:

- Data Management Framework
- Internet Use and Digital Communications Policy
- Records Management Policy
- Official Information Policy
- Privacy Policy
- Use of Copyright Materials for Educational Purposes Policy

References:

- Open Group (2013). *TOGAF Version 9.1.* Van Haren Publishing.
- DAMA International (2009). *The DAMA Guide to The Data Management Body of Knowledge.* Technics Publications.
- American Federal Government (2005). *The Data Reference Model Version 2.0.* http://www.whitehouse.gov/omb/e-gov/fea.

Document Management Control:

Prepared by: Data Management Specialist
Authorised by: Chief Information Officer
Approved by: SLTWH 24/11/2014 Item 2C
Date issued: November 2014
Next review: July 2017
Effective Date: July 2015