DATA MANAGEMENT POLICY

Section	Information Technology Services
Contact	Chief Information Officer
Last Review	September 2022
Next Review	September 2025
Approval	SLT 22/09/124
Effective Date	September 2022

Purpose:

To establish uniform data management standards and identify the roles accountable and responsible for the management of the data so that it efficiently and effectively serves the needs of the University. Massey University values access to, and the timeliness, accuracy, and consistency of data, so that decision-makers have confidence and trust in the information they rely on.

Scope:

This policy applies to all institutional data, including data outside of Massey University stored in a cloud service. It applies to creators and/or users of such data and also applies to third parties who access and use University systems and IT equipment or who create, process, or store data owned by the University.

Policy Statements:

1. The University asserts its rights in respect of all institutional data that is created and captured during the operation of the University. Institutional data are the property of the University and are to be managed as a key asset.

2. In accordance with the Information Security Classification Policy and Framework all sources of data must be identified, documented, and classified commensurate with its sensitivity and value to ensure appropriate protection throughout its lifecycle.

3. Sharing data between University departments is facilitated where appropriate. Personally Identifiable Information (PII) will be deidentified wherever possible prior to such sharing unless the department has a genuine need to access the data in an identifiable manner. Under no circumstances will sharing data cause confidential data to be compromised generating a Privacy Breach.

4. Data must be safeguarded and managed at all points and across all systems, from creation, to use, to archive, through coordinated efforts and shared responsibilities to ensure its accuracy. Each functional area will develop and implement processes for identifying and correcting erroneous or inconsistent data. When and if erroneous or inconsistent data has been identified, the Data Steward from the corresponding functional area shall either correct the data or escalate the issue to the appropriate Data Custodian. All Data Breaches must be notified to the university's Privacy Officer.

5. Access to data is on the basis of the business needs of the University to enable the University to achieve its mission. Employees will have access to the data needed to perform their responsibilities. Access to Personally Identifiable Information (PII) will have all required access controls applied and managed. Access does not mean privileges to modify or disclose the data.

6. The University's institutional 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. Before decisions are made concerning data retention and data archiving, the appropriate Data Stewards must be consulted.

7. All institutional data must be managed and as such must have representation by all the groups mentioned below. These are delegated responsibilities.

   Data Leaders are representative of the University's Senior Leadership Team (SLT) and are accountable and responsible for:

   - providing strategic guidance for the institutional data in their area of responsibility
   - acting as a champion for data management and data-related initiatives
   - approving the policies associated with managing the University's data specific to a functional area
   - assigning Data Custodians.

   The Data Custodian is the authoritative head of the respective Faculty, School, Division or Unit within the University and is accountable and responsible for:

   - assigning Data Stewards for data in their area of responsibility and allowing time for them to complete relevant tasks
   - the business use of the data asset, and is given the authority to collect, create, retain, and maintain the data within their assigned area of control, coupled with the responsibility to protect it on behalf of the University
   - authorising and reviewing the security classification of Information
   - authorising access to assigned data and its usage in other systems
   - identifying and registering Personally Identifiable Information (PII) contained in data sources
   - ensuring that data is fit-for-purpose including defining data quality levels, metrics, business rules and facilitating data integration.

   The Data Steward(s) are individuals responsible for the day-to-day management of the data, including operational requirements of data quality, data definitions, compliance with requirements, conformance to policies and standards, security controls, and identifying and resolving data issues. The Data Steward is required to:

   - provide direction regarding the quality, security, integrity, accuracy, consistency, privacy confidentiality, and accessibility of information across its lifecycle
   - assign an appropriate information classification
   - implement, monitor and authorise access to the data in accordance to approved business rules and processes
   - specify any additional handling controls needed to ensure the confidentiality, integrity, and availability of the data
   - communicate the control requirements to the Data Custodian and to users of the data.

The IT Services department is responsible for:

- providing a sustained data administration function that will review data models and reinforce a set of definitions for commonly consumed data, with the understanding that there may be multiple valid definitions. The definitions shall be available to all data users
- approving and applying the data architecture and ensuring integration across the University is supported to foster data accuracy and uniformity, and demonstrate an understanding of the University's institutional complexity, various data systems, and differing data formats
- ensuring data is safeguarded to maintain the confidentiality and privacy of Personally Identifiable Information (PII). Data sources containing personally identifiable information and/or private information must be inventoried.

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.

Definitions:

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 d ata availability, quality and security needs of the University.

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

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 but does not include research data.

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

Privacy Breach in relation to Personally Identifiable Information (PII) held at the University:

(i) means unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, the personal information; or

(ii) an action that prevents the university from accessing the information on either a temporary or permanent basis.

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.

Relevant legislation:

- Contract and Commercial Law Act 2017
- Privacy Act 2020
- Public Records Act 2005
- Official Information Act 1982
- Public Finance Act 1989
- Copyright Act 1994

Related procedures / documents:

- Information Security Classification Policy and Framework
- Information and Records Management Policy
- Official Information Policy
- Privacy Policy

Document Management Control:

Prepared by: Chief Information Officer
Authorised by: Deputy Vice-Chancellor, University Services
Approved by: SLT 22/09/124
Date issued: November 2014
Last review: September 2022
Next review: September 2025