Information Technology Services Operations Manual - Master Data Management, Data Classification and Usage, and Data Storage

Policy code:	OG2083
Policy owner:	Director, ITS
Approval authority:	Chief Operating Officer
Approval date:	27 August 2024
Next review date:	27 August 2025

Table of Contents

1. Introduction

The Information Technology Services procedural manuals detail the processes that have been developed using previous policies, procedures to provide clear advice to Federation University Staff regarding their responsibilities, actions and accountability in accordance with the Federation University Act, Statute, Regulations and Policies, Procedures and Manuals.

It is an associated document within the Federation Governance document suite and must be used as a tool to assist all stakeholders to fulfil obligations in accordance with university mandates.

The purpose of this manual is to ensure that all members of the Federation community are informed, understand their requirements to perform key tasks and know where to access information as needed to adhere to mandated requirements and enhance their practice.

It is also intended to assist all staff in carrying out their functions and responsibilities with ease and completeness by providing clarity of expectation and responsibilities.

This manual will be revised annually by the owner and/or their nominated delegates to ensure currency of information.

Note: This manual as a pdf document will be located in the Policy Administration System (PAMS) published via Policy Central to ensure users have access to current, update to date information. Wherever possible, editors have cross referenced back to relevant Federation documents and other links.

2. Master Data Management

2.1 Purpose

Federation University Australia is committed to the appropriate storage of information in support of its teaching, administrative and support functions. The University acknowledges its obligation to ensure appropriate security of personal data in relation to all relevant legislation while providing approved data storage solutions to accommodate the varying needs of the University community. University data is recognised as a valuable asset and will be efficiently managed and availed through development of a best practice approach to data management.

This manual mandates a range of associated University policies and procedures developed to ensure the integrity, authenticity, availability, access, confidentiality and security of data produced and/or utilised by the University through minimising duplication and fragmentation and introducing internal controls to mitigate identified risks.

Through its associated procedures the University will:

- define the roles, responsibilities and accountability for different data usage
- ensure best practice processes for effective data management including access, retrieval, reporting, managing and storing
- protect the University's data against internal and external threats.

The University is also required to produce evidence of its activities to external regulators, internal auditors, accreditation and funding bodies. Adherence to this manual will ensure the University is able to meet this requirement.

The University's *Research and Research Training Policy* and *Research Data Management Procedure* governs responsibilities and processes for the ownership, storage, retention, accessibility for use and reuse and/or disposal of research data in accordance with the Australian Code for the Responsible Conduct of Research.

2.2 Scope

This manual applies to all University data produced, collected, stored and/or utilised by members of the University's community. It does not apply to data used for the purpose of academic research.

While partner provider organisations are supported through the use of specific University information technology systems, this manual does not apply to non-University related data created, managed or stored by these organisations.

2.3 Legislative Context

- Federation University Australia Act 2010
- The Higher Education Support Act 2003
- The National Code of Practice for Registration Authorities and Providers of Education and Training to Overseas Students made under the Education Services for Overseas Students Act 2000 (ESOS)
- Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015
- Information Privacy Act 2000 (Victoria)
- Electronic Transactions Act 2000 (Victoria)
- Public Record Act 1973 (Victoria)
- Australian Copyright Act of 1968
- Evidence Act 1958 (Victoria)
- Australian Qualifications Framework AQF Second Edition January 2013
- Australian Skills Quality Authority ASQA
- Higher Education Standards Framework (Threshold Standards) 2011
- Tertiary Education Quality and Standards Agency (TEQSA)
- Higher Education and Skills Group HESG
  - 2014 – 2016 VET Funding Contract

2.4 Definitions

Term	Definition
Authorised person	An individual or group of people who have been authorised to use and/or store data on the University's approved data storage system/s
Copyright	Intellectual property right that protects a body of work, not for ideas or information, but for the form in which they are expressed, from unauthorised use and is applied automatically when a work is created without the need to register or comply with formalities
Data	Data and records collected, created and/or maintained by the University including digital and non-digital information.
Data dictionary	Centralised repository of information about data such as meaning, relationships to other data, origin, usage and format
Data management	Defines the access rights, roles and responsibilities in relation to the management and protection of University data
Data integrity	Data accuracy and consistency over its entire lifecycle
Data owner	An individual or group of people accountable for specific data that is created, transmitted, used and stored on a system within the University
Data quality	Data currency, validity and relevance
School	Federation University Australia has a number of Academic Organisational Units

Intellectual property (IP)(including patents and trademarks)	IP is the application of the mind to develop something new or original, existing in various forms – a new invention, brand, design or artistic creation A patent is a legally enforceable right that is granted for any device, substance, method or process that is new, inventive and useful A registered trade mark is a legally enforceable right that is granted for a letter, number, work, phrase, sound, smell, shape, logo, picture and/or aspect of packaging
Metadata	Describes information about data, such that data can be discovered, understood, re-used and integrated with other data; information described in a metadata record includes where and when the data was collected, created, organised, transmitted (where applicable) and last updated and who is responsible, allowing correct attribution to the creators of the work
Record	Any record that is created or received by the University in the transaction of its business functions or resulting from research activities and retained as evidence of that activity which can include, but is not limited to, hard copy documents, electronic or digital records including email and information maintained as part of a database or business information system
Scholarly works	Any article, book, musical composition, creative writing or like publication or any digital or electronic version of these works that contains material written by academic staff or student based on that person's scholarship, learning or research but does not include work that is teaching material
Security	Safety of University data in relation to access control, authentication, effective incident detection, reporting and solution, physical and virtual security, change management and version control
University data	All data owned or licensed by the University
Users	Persons who use information resources and have responsibility for ensuring that such data is used properly in compliance with this manual

2.5 Manual Statement

This manual provides the following set of guiding principles to maximise the University's data management capabilities to manage the needs of students, staff and other members of the University's community who create, receive, store, access, transmit, use, or dispose of data as part of their relationship to the University noting that both the types of data and requirements will differ:

Principle	**Demonstrated by:**
Any record generated as a result of University activities is an official record under the Public Records Act 1973 (Victoria) and must be created, captured, stored and effectively managed within the	• utilising secure and reliable storage platform/s to manage data centrally – refer Section 4: Data Storage; data stored on local PCs and laptops is the responsibility of the user and should be transferred to University's sanctioned storage • capturing the activities and functions of the University to adequately represent institutional memory

University's approved data storage and records management systems	
The University's data classification scheme standardises records' structures and descriptions by contextualising the records within functions and activities	• classifying data utilising the University's information security classification so that it may be managed and secured in a manner appropriate with its sensitivity and importance - refer Section 4: Data Storage • categorising and using files consistently within the established classification scheme – refer Section 3: Data Classification and Usage
The University protects the confidentiality of personal and health information it collects for both its own operations and the conduct of research	• complying with the University's *Information Privacy Procedure* and *Study Adjustment and Course Flexibility Guidelines* • ensuring that all personal and health data is stored in accordance with the Australian Privacy Principles, Ethical Conduct and other standards related to health records, as appropriate • storing completed participant consent forms required in the conduct of researchprojects, clinical trials or other approved University activities eg Open Days in accordance with National Guidelines and Standards
Ownership and rights associated with data created, collected and stored is clarified and managed appropriately	• facilitating appropriate management of all data created or collected • determining inclusion of appropriate/sufficient details to ensure storage and access to records in accordance with any contractual agreements or sponsorship • ensuring that scholarly works and data created by staff or students is owned by their creator/s unless the status is otherwise altered giving intellectual property rights to the University
The legal context for the collection, management, storage and use of data is considered and addressed	• identifying data which is likely to pose legal issues to ensure storage and access options are suitably managed • ensuring that any legal issues relevant to the collection, management and storage of data are addressed
Extensive metadata is built around the data to ensure quality information about its provenance, legal and technical framework, access rights, publication and disposal in line with relevant metadata standards	• collecting and publishing metadata related to the data • keeping good records and contextual information to ensure data is easy to locate and accessible into the future • incorporating structured metadata eg properties which include title, author, subject, keywords, version control information, dates and additional comments within agreed standardised vocabularies and ontologies
Long term storage, archiving and disposal requirements are identified and implemented	• managing appropriately the transition of data along the curation continuum eg private to public domain • considering and implementing solutions for storing and accessing data, including language recordings • retaining data in compliance with minimum regulatory or funding retention periods eg five years to perpetuity and within legal and ethical requirements • disposing of data in an appropriate manner in accordance with the University's *Records Management Procedure*
Data disaster recovery and activity continuity planning is in place	• ensuring each organisational unit has created and continues to maintain a current business continuity plan

	• backing up on premise and cloud storage data in accordance with the defined schedules and server cloud agreements • ensuring adequate measures are in place to prepare for and manage in the event of a disaster or disruption to facilitate the resumption of University activities and minimise threats to the University's information assets

3. Data Classification

3.1 Purpose

This manual establishes a framework for classifying Federation University Australia (the University) information based on its confidentiality and potential business impact on the University's operations, reputation, and legal obligations. It presents a consistent approach for evaluating University information and applying data classifications to ensure appropriate management and security protections. It should be read in conjunction with the Information Governance and Management Framework.

3.2 Scope

All information created, collected or stored by the University in electronic or physical formats, must be classified into one of the five data classifications. All parties creating or accessing University information must comply with the manual, including (but not limited to) students, staff, contractors, partners and third parties.

3.3 Definitions

Term	Definition
Data Classification	A categorisation which indicates the sensitivity of a set of information based on its confidentiality. Interchangeable with 'protective markings' or 'sensitivity labels'.
Business Information Steward	A subject matter expert who approves internal access requests, classifies, registers, and maintains an information asset, ensures its security, quality, and compliance, and provides advice on its use and interpretation.
Executive Information Steward	A senior leader who oversees one or more information assets and ensures they are secure, accurate, available and shared where appropriate. They also approve and champion information governance policies and procedures, and authorise the release of information assets to external parties.
Technical Information Steward	A person who has technical expertise and skills to oversee and maintain the quality, security and availability of an information asset, such as a database, a document or a report.
Information Asset IA	An Information Asset (or Data Asset) is a definable piece of information that can be in the form of an information sub-domain, collection of datasets, or data elements. Information Assets have recognisable and manageable value, risks, content and lifecycles.

Information Owner	The person or entity that has enterprise-wide authority and accountability for the collection and management of the University's information. The Vice-Chancellor and President is the Information Owner for Federation University Australia and can delegate responsibilities as needed.

3.4 Data Classification Procedure

Information should be classified by the University community at the point of creation or capture. The stipulated classification should be endorsed by the relevant information stewards.

Data classifications are ensure that appropriate management controls are enacted on information assets to minimise their risk of inappropriate or unauthorised disclosure. Data classifications are based on the confidentiality of the information and assigned accordingly.

When classifying an information asset, consider the most confidential information held within the asset and classify based on the highest relevant classification. All information of the University should be assigned a data classification based on the below table:

3.4.1 Data Classification Scheme

Data Classification	Description	Potential Impact
Public	Information that is authorised for public release, however, may not be provided to the public. Examples include: • Annual report • Published course information • Public website • Published research data • Policies and procedures • University strategy	**Insignificant impact** to the University if lost, accessed or disclosed without authorisation.
Official	Information that has a restricted, yet potentially broad audience based on academic, research or business needs. Official is the purposes as determined by its default data classification, where none has previously been applied. Examples include: • Contact information accessible by standard communicationstechnology (Name, email, phone, title, etc) • Administrative documentation • Aggregated information for planning and analysis	**Unlikely to cause harm** to the University or an individual if publicly released or subject to a data breach.

	• Organisational unit processes and procedures	
Official: Sensitive	Information that has a restricted audience and access based on **strict** academic, research or business needs. Examples include: • Personal information of staff, students, applicants or others. • Academic assessment and performance data (exams, results, etc) • Financial data • Unpublished research outputs	If released publicly or subjected to data breach could reasonably be **expected to cause harm** to the University or an individual.
Protected	Information that has a restricted audience and access based on **very strict** academic, research or business needs. Examples include: • Health information • Personal financial information • Personally Identifiable Information (PII) • Identifiable equity and minority group data • Legal information • Information related to minors • National security related research data • Sensitive personnel records	If released publicly or subjected to data breach could reasonably be **expected to cause serious harm** to the University or an individual.

3.5 Responsibilities

Information Stewards are responsible for:

- Classification of information assets under their management in accordance with the University's Data Classification procedure.
- Ensuring the management of information assets is in accordance with the below responsibilities table.

3.5.1 Responsibilities

Classification	Access	Storage	Disposal
Public	Records may be accessible by external parties from any location	Storage must be as per Section 4: Data Storage	Disposal must be as per *Records Management Procedure*

Official	Information is classified as official by default unless reclassified by the creator; access to official records and files is limited to University staff or other authorised personnel	Storage must be as per Section 4: Data Storage	Disposal must be as per *Records Management Procedure*
Official: Sensitive	Access to records and files requires authentication and password protection. Records accessible by only a limited number of authorised people. Records and portable storage devices should be stored in a secured (locked) location	Storage must be as per Section 4: Data Storage	Disposal must be as per *Records Management Procedure*
Protected	Access to records and files requires authentication and password protection Record and file access must be protected and accessible by appropriate parties in the University Devices and records must be stored in a secured (locked) location	Storage must be as per Section 4: Data Storage If data is to be moved, it must be encrypted	Disposal must be as per *Records Management Procedure*

3.6 Associated Documents

- Information Governance and Management Framework
- Information Technology Services Operations Manual- Use of Computing and Communication Facilities and, Information Security
- OVIC - Practitioner Guide: Protective Markings
- Risk Management Framework Procedure

4. Data Storage

4.1 Purpose

This manual supports and mandates the implementation of Section 2: Master Data Management and *Research Data Management Procedure*. It expands on the principles outlined in the procedures as they relate to data management and provides guidance on the implementation and practical application of data storage solutions.

4.2 Scope

This manual applies to all digital and digitised data produced, stored and/or utilised by members of the University's community.

While partner provider organisations are supported through the use of specific University information technology systems, this manual **does not apply** to electronic data created, managed or stored by these organisations.

4.3 Legislative Context

- Federation University Australia Act 2010
- Information Privacy Act 2000 (Victoria)
- Electronic Transactions Act 2000 (Victoria)
- Public Record Act 1973 (Victoria)
- Privacy and Data Protection Act 2014
- Australian Copyright Act of 1968
- Evidence Act 1958 (Victoria)
- Australian Code for the Responsible Conduct of Research (2007)
- OECD Principles and Guidelines for Access to Research Data from Public Funding (2007)
- Australian Skills Quality Authority ASQA
- Higher Education Standards Framework (Threshold Standards) 2011
- Tertiary Education Quality and Standards Agency (TEQSA)

4.4 Definitions

A complete list of definitions relevant to this manual is contained within Section 2: Master Data Management.

A further list of definitions **specifically** relevant to this manual is included below:

Term	Definition
Cloud computing	The delivery of on-demand computing resources over the internet with four options in terms of access and security: **Private cloud** – services and infrastructure maintained and managed by self or a third party which reduces potential security and control risks particularly in relation to sensitive data requirements e.g. data and applications are a core part of your business

	Community cloud – several organisations with similar security considerations share access to a private cloud e.g. a group of franchises who have their own private clouds which are hosted remotely in a private environment **Public cloud** – services are stored off-site, managed by an external organisation such as Google or Microsoft and accessed over the internet which offers the greatest level of flexibility and cost saving but more vulnerable than private clouds **Hybrid cloud** – takes advantage of both public and private cloud services and gain benefits by spreading options across different cloud models e.g. use public cloud for emails to save on large storage costs while keeping highly sensitive data safe and secure behind the firewall in a private cloud
Cloud-based applications	Software as a Service (SaaS), run on cloud computers that are owned and operated by others and connect to users' computers via the internet and a web browser
Cloud-based environment	Platform as a service (PaaS) provides everything required to support the complete lifecycle of building and delivering web-based (cloud) applications, without the cost and complexity of buying and managing the underlying hardware, software, provisioning and hosting
Metadata	Describes information about data, such that data can be discovered, understood, re-used and integrated with other data; information described in a metadata record includes where and when the data was collected, created, organised, transmitted (where applicable) and last updated and who is responsible, allowing correct attribution to the creators of the work
On-premise Storage	Refers to locations inside the University network which is controlled and managed by University Information Technology Services ITS staff and remains within the University network and security infrastructure

4.5 Actions

4.5.1 Determining data storage compliance requirements

	Activity	Responsibility	Steps
A.	Checking data classification	Data Steward	1. Apply data classification scheme to determine if the data can be stored on University sanctioned cloud storage services – if not, refer Action 4.5.3: Accessing on-premise Storage
B.	Determine compliance requirements	Data Steward	1. In context of the data to be stored refer to 4.3: Legislative Context to determine the compliance requirements that apply.

			2. Compare compliance requirements against provided data storage options compliance certifications.
C.	Determining suitability of cloud storage	Data Steward	1. Staffing and financial data may be stored in university sanctioned cloud services.

4.5.2 Providing data storage options

	Activity	**Responsibility**	**Steps**
A.	Protecting data	ITS	1. Provide options for the storage of digital data, including those housed on-premise and in the cloud including approved corporate business systems, network drives and approved cloud-based applications • Business information systems Use business information systems to store data that relates to a specific business function (i.e. student data should be stored in the Student Management System) • SharePoint may be used to store other types of data – refer Section 3: Data Classification and Usage • Cloud storage solutions deployed for the storage of University data must comply with all legislative requirements; may not be appropriate for all applications and classifications of data – the service must be fit for purpose and used appropriately
B.	Undertaking a risk assessment for prospective data storage	ITS	1. Ensure the cloud solution meets the legislative requirements of the Public Records Act 1973 (Victoria) and associated mandatory standards issued by PROV

			2. Identify risks in the proposed cloud environment 3. Complete a Risk Assessment

4.5.3 Accessing on-premise storage

	Activity	Responsibility	Steps
A.	Storing Protected data	Data Steward	1. Use of on-premise storage for any data classified as Protected or Restricted – Refer Section 3: Data Classification and Usage – may only be done by way of a University sanctioned information system. NOTE: On-premise can be used to store data of any type, but the preference will be to store public data in University sanctioned cloud storage services – refer Action 4.5.1 Determining data storage compliance requirements 2. Input information into relevant on-premise information system or storage location 3. Save with suitable data classification tags 4. Complete all metadata fields

4.5.4 Using cloud storage services

	Activity	Responsibility	Steps
A.	Accessing cloud storage services	Data Steward	1. Determine suitable storage location. 2. Save with suitable data classification tags 3. Complete all metadata fields

5. Responsibility

- Chief Operating Officer, Chief Operating Office is responsible for monitoring the implementation, outcomes and scheduled review of this manual.
- Director, Information Technology Services is responsible for maintaining the content of this manual as delegated by the Chief Operating Officer, Chief Operating Office.

6. Records Management

Document Title	Location	Responsible Officer	Minimum Retention Period
Completed Risk Assessments	The University's approved records management system	Information Technology Services	7 years after administrative use has concluded
Agreements with Cloud Service	The University's approved records management system	ITS / Legal	7 years after expiry of agreement

7. Rescinded Documents

This manual replaces the following documents that have been rescinded when this Manual was issued.

- Master Data Management Policy IM1972
- Data Classification and Usage Procedure IM1974
- Data Storage Procedure IM1981

Glossary