Digital Assets Policy

Table of Contents

1. Purpose

a. The purpose of this policy is to outline the principles, approach and responsibilities for effective and efficient management of University-owned and/or managed digital assets throughout the asset lifecycle, and to preserve the security and integrity of the University's digital environment.

b. This policy and its supporting procedures aim to:

i. ensure appropriate management of University-owned digital assets

ii. support improved experiences related to the provisioning for, access to, use and maintenance of university digital assets

iii. maintain visibility of University digital assets via an up-to-date central asset repository

iv. identify, manage and mitigate digital security risks

v. facilitate ongoing asset management process improvements

vi. ensure license compliance.

2. Scope

This policy applies to all Flinders University community members who have reason to access the Flinders' digital environment, or any digital asset owned or controlled by the University.

3. Definitions

Digital asset	Includes any hardware, software, data or information object or resource which has an identified, intrinsic value. The value may be in terms of security value, knowledge value, financial value or any other measurement of value as determined by the University.
Digital environment	The complete, integrated digital communication and technology ecosystem that is provided for all Flinders University community members to interact, interconnect and digitally operate.

Flinders University community members	Includes: • enrolled Flinders students, including cross-institutional students and students on exchange from another institution • employees and exchange staff • employees of controlled entities, Centres and Institutes, and affiliated clubs and associations • contractors and consultants performing work on University sites or on behalf of the University • visiting academics or persons with academic status • the Council and its committees • any volunteer in the workplace and study environment.
Information and Digital Services (IDS)	The division within Flinders University responsible for the management and oversight of the digital environment and digital assets.
University Owned Digital Asset	Any digital asset purchased, acquired or contracted by Flinders University using University funds.
University Managed Digital Asset	Any digital asset used within the University's digital environment which has not been purchased, acquired or contracted using University funds. This includes (but is not limited to) digital assets purchased via grant or research funding agreements/partnerships.
Personal digital asset	Any digital asset not purchased, acquired, owned or contracted by the University or managed by the University. This includes (but is not limited to) personal laptop computers and portable storage devices, such as USB flash drives.

4. Policy statement

4.1. Ownership and authority

a. University Owned Digital Assets remain the property of Flinders University.

b. IDS maintains authority over the security and management of all University digital assets.

c. IDS may assign custodianship/stewardship of University Owned and/or University Managed Digital Assets to members of Flinders University community where appropriate.

d. Flinders University community members are responsible for any digital assets for which they use and/or operate.

4.2. Management

a. IDS manages and secures all University digital assets to ensure that the operations of the University's digital environment is maintained.

b. The acquisition of all University-owned and/or managed digital assets is undertaken in accordance with this policy and its supporting procedures.

c. All University managed digital assets will be tracked in a central repository.

d. All University digital assets must conform to IDS standards, security baselines, periodic testing requirements and configuration guidelines.

e. University digital assets will be periodically subject to audit and review. University digital assets that do not conform to IDS standards, security requirements and periodic testing may be removed, deleted or decommissioned.

f. Quality standards and classifications of University digital assets will be allocated to individual assets. Processes, security controls and accessibility will be aligned in accordance with those assigned quality standards and/or classifications.

g. All integration of University owned and/or managed digital assets onto the University's network will be done in compliance with this policy.

4.3. Personal digital assets

Where personal digital assets are used in the manipulation or use of University digital assets, the University digital asset must be operated in compliance with this policy.

5. Authorities

Chief Information Officer (CIO)	a. Remove university digital assets from the digital environment, revoke access or decommission a digital asset that is non-compliant with this policy.
Chief Information Security Officer (CISO)	b. Remove university digital assets from the digital environment, revoke access or decommission a digital asset that is non-compliant with this policy.

6. Supporting procedures

Supporting procedures are part of this policy and provide additional detail to give practical effect to the policy principles.

Digital Hardware Asset Management Procedures

Digital Software Asset Management Procedures

Other related documents include:

Digital Environment Policy

Digital Security Policy

Acceptable Use of Digital Assets Policy

Procurement Policy

Approval Authority	Vice-President (Corporate Services)
Responsible Officer	Chief Information Officer
Approval Date	31 July 2024
Effective Date	31 July 2024
Review Date*	2027
Last amended	
CM file number	CF24/509
* Unless otherwise indicated, this policy or procedures still apply beyond the review date.	

Printed versions of this document are not controlled. Please refer to the Flinders Policy Library for the latest version.