

# Digital Environment Policy

## Table of Contents

1. Purpose
2. Scope
3. Definitions
4. Policy statement
  - 4.1. Management and governance
  - 4.2. Digital security
  - 4.3. Digital assets
  - 4.4. Responsibilities of Flinders University community members
5. Supporting procedures

## 1. Purpose

The purpose of this policy is to provide the overarching framework for how the Flinders University digital environment and related digital assets are governed, managed and protected.

## 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

<b>Digital asset</b>	Includes any hardware, software, data or information object or digital 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.
<b>Digital environment</b>	The complete, integrated digital communication and technology ecosystem that is provided for all Flinders University community members to interact, interconnect and digitally operate.
<b>Flinders University community members</b>	<p>Includes:</p> <ul style="list-style-type: none"><li>• enrolled Flinders students, including cross-institutional students and students on exchange from another institution</li><li>• employees and exchange staff</li><li>• employees of controlled entities, Centres and Institutes, and affiliated clubs and associations</li><li>• contractors and consultants performing work on University sites or on behalf of the University</li><li>• visiting academics or persons with academic status</li><li>• the Council and its committees</li><li>• any volunteer in the workplace and study environment.</li></ul>

<b>Information and Digital Services (IDS)</b>	The division within Flinders University responsible for the management and oversight of the digital environment and digital assets.
<b>Information asset</b>	A type of digital asset comprised of data or a collection of data that is processed, analysed, interpreted, classified, or communicated in order to serve a useful purpose, present fact or represent knowledge in any medium or form.

## 4. Policy statement

### 4.1. Management and governance

- a. The University manages its digital environment and digital assets through:
  - i. this policy and related policies and supporting procedures
  - ii. the IDS Risk, Security and Compliance Committee, responsible for the oversight of effective management of risk, security and compliance of the Flinders University digital environment
  - iii. the Digital Governance Committee (and sub-committees), responsible for the recommendation and oversight of capital investments in the Flinders University digital environment and digital assets.
- b. IDS maintains authority over the management and governance of the Flinders University digital environment and all digital assets owned and/or managed by Flinders University.

### 4.2. Digital security

- a. The University manages the security of its digital environment and digital assets as outlined in the [Digital Security Policy](#).
- b. In accordance with the Digital Security Policy, IDS may take immediate action to remove digital asset(s), or the access of a Flinders University community member, at its discretion.

### 4.3. Digital assets

- a. The University manages its digital assets as outlined in the [Digital Assets Policy](#).
- b. All University digital assets must conform to IDS standards, security baselines, periodic testing requirements and configuration guidelines.

### 4.4. Responsibilities of Flinders University community members

- a. Flinders University community members connect, interact and utilise digital assets and services within the digital environment for varied purpose and/or outcomes. When doing so, Flinders University community members must:
  - i. connect, interact and utilise digital assets and services for the betterment of the community and the development of teaching, learning and research purposes
  - ii. interoperate in an acceptable, appropriate and permitted manner as outlined within the [Acceptable Use of Digital Assets Policy](#)
  - iii. value and respectfully utilise their digital identities in a manner that will not bring the University into disrepute.

## 5. Supporting procedures

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

[Digital Security Policy](#)

[Digital Assets Policy](#)

[Acceptable Use of Digital Assets Policy](#)

[Email and Electronic Data Access Procedures](#)

[Information Classification and Handling Procedures](#)

[Digital Hardware Asset Management Procedures](#)

[Digital Software Asset Management Procedures](#)

<b>Approval Authority</b>	Vice-President (Corporate Services)
<b>Responsible Officer</b>	Chief Information Officer
<b>Approval Date</b>	31 July 2024
<b>Effective Date</b>	31 July 2024
<b>Review Date*</b>	2027
<b>Last amended</b>	Chief Information Officer, 19 February 2025
<b>CM file number</b>	CF18/16

\* 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.