Information Protection



Policy

**Steward** Director Governance and General Counsel

**Administrator(s)** Manager Information Governance

**TRIM File** F20/1258

Policy Number UP20/2

Approval Date 24 August 2023

Assessment Date 24 August 2026

Approver Senior Deputy Vice-Chancellor

# Purpose

#### The purpose of this **Policy** is to —

##### express the **Information Protection** practices required by the **University**;

##### establish the classification and handling of University Information based on risk and value to the University;

##### establish standards for the management, responsible sharing and governance of **University Information**;

##### promote University Information as an institutional asset for which there is ownership, accountabilities, responsibilities and controls; and

##### contribute to a University culture of integrity.

#### In this Policy —

[1 Purpose 1](#_Toc144284600)

[2 Scope 2](#_Toc144284601)

[2.1 Institutional Scope 2](#_Toc144284602)

[2.2 Individual Scope 2](#_Toc144284603)

[3 Information Protection 2](#_Toc144284604)

[4 Information Governance 3](#_Toc144284605)

[4.1 Information Owner 3](#_Toc144284606)

[4.2 Information Steward 3](#_Toc144284607)

[4.3 Information Custodian 3](#_Toc144284608)

[4.4 Business System Owner 3](#_Toc144284609)

[4.5 Information Power User 4](#_Toc144284610)

[4.6 Information User 4](#_Toc144284611)

[5 Information Classification 4](#_Toc144284612)

[6 Information and Data Handling 4](#_Toc144284613)

[7 Takedown Powers 5](#_Toc144284614)

[8 University Information Management System 5](#_Toc144284615)

[8.1 Data Centre Services 6](#_Toc144284616)

[8.2 Backup and Recovery 6](#_Toc144284617)

#### This Policy is to be read in conjunction with the following —

##### Information Protection Takedown Procedure;

##### Information Protection Classification Guide; and

##### UWA Information Governance Framework.

# Scope

## Institutional Scope

#### The scope of this Policy applies to the entire University.

## Individual Scope

#### The scope of this Policy applies to the entire **University Community**.

# Information Protection

#### Information Protection means providing security for University Information based on its risk, legal requirements and business value.

#### University Information means all data, records and information created, captured, processed, stored, shared and/or disposed of, by the University Community or on behalf of the University, relating to University Business, in any format or medium.

#### The University Community must ensure University Information is —

##### protected from unauthorised access, modification or misuse;

##### prevented from loss or inappropriate disclosure;

##### managed in accordance with its business value to the University; and/or

##### compliant with statutory and/or other legal obligations.

# Information Governance

#### The University will identify members of the University Community to perform information governance roles to ensure University Information is managed in accordance with legislative obligations.

## Information Owner

#### **Information Owner** means the University, as the legal owner of University Information.

#### The Vice-Chancellor must act on behalf of the University as the Information Owner in developing and managing Information Protection.

## Information Steward

#### **Information Steward** means a senior **Employee** identified by Information Governance and approved by their line manager, to be accountable for the University Information within their **Business Capability**.

#### Business Capability means a defined grouping of capacity, resources, processes and expertise used by the University to perform a specific function.

## Information Custodian

#### **Information Custodian** means an Employee identified by an Information Steward who is —

##### a subject matter expert for a specific type of University Information; and

##### responsible for implementing and monitoring the management of and access to University Information.

#### Information Custodians may or may not be a direct report to an Information Steward.

## Business System Owner

#### **Business System Owner** means a senior Employee who is responsible for managing University Information stored within a **University Information Management System** in accordance with University policies.

## Information Power User

#### **Information Power User** means an Employee granted elevated access to University Information.

## Information User

#### **Information User** means a member of the University Community that creates, captures, receives or uses University Information.

# Information Classification

#### Information Stewards will be accountable for the classification and labelling of their University Information as —

##### Public Information intended, or available, for release to the Public; or

##### Confidential Information limited to University Information Users, requires basic access control and where unauthorised access could have a minor negative impact on the University or a third party; or

##### Confidential Restricted Information limited to University Information Users with a business need based on their organisational function, where unauthorised access could have a moderate negative impact on the University or a third party; or

##### Highly Restricted Information limited to University Information Users with a specific business need based on their individual role, where unauthorised access could have a major or catastrophic negative impact on the University or a third party.

##### Unclassified (Non UWA) information does not relate to the University, or concerns University Business, is unclassified and there is no negative impact to the University if accessed or disclosed. Such information may result from the permitted limited personal use of University Information Management Systems.

#### Information Users must not prevent collaboration and knowledge exchange by applying an incorrect classification on University Information.

# Information and Data Handling

#### Access to and use of University Information will be in accordance with its classification.

#### Business System Owners and Information Power Users must apply appropriate access controls and security models to University Information in accordance with its classification and business function.

#### Information Users must classify University Information when they create, capture, process, store, share and/or dispose of University Information in accordance with —

##### the Information Protection Classification Guide;

##### the requirements of any contractual, commercial and/or **Intellectual Property** obligations.

#### University Information which is Confidential Restricted or Highly Restricted must only be shared under an —

##### information sharing agreement;

##### confidentiality agreement;

##### contract or by prior agreement of contractual obligations; or

##### where required by law.

# Takedown Powers

#### The University may be required to take action to remove University Information from **IT Assets**.

#### The University must exercise takedown powers where the University receives an appropriately authorised request to remove University Information from an IT Asset from —

##### A **Copyright** owner, or entity acting on behalf of a Copyright owner, where the takedown request relates to a potential infringement of third party Copyright;

##### Australian Communications and Media Authority; or

##### Australian Federal Police; or

##### Western Australian Police.

#### The University may exercise takedown powers where an IT Asset is —

##### found to be in breach of the University’s Acceptable Use of IT policy; or

##### alleged to contain University Information or other material which is illegal or contravenes their Copyright.

#### The University will exercise these takedown powers in accordance with the Information Protection Takedown Procedure.

# University Information Management System

#### University Information Management System means any system used for creating, capturing, processing, storing and/or sharing University Information, endorsed by University IT.

#### University Information must be stored in a University Information Management System.

#### Information Users must store University Information only in a University Information Management System.

#### University Information created, processed, stored or managed outside of a University Information Management System may constitute a breach of this Policy.

#### The University and University IT will not be responsible for the protection of University Information stored outside of a University Information Management System.

## Data Centre Services

#### University IT will be accountable for physical and environmental controls for the University Information stored within University IT infrastructure such as the Institutional Data Centre (IDC).

#### University Information stored or hosted outside the IDC in an endorsed University Information Management System managed by a contracted provider, will be in accordance with the Information Retention Policy and Cyber Security Policy.

#### University IT will ensure appropriate physical and environmental controls are implemented by any contracted provider who provides data centre services to the University for the storage of University Information.

## Backup and Recovery

#### University IT will be responsible for University Information being adequately protected by being backed up by —

##### University IT for information stored within the IDC; and

##### the supplier, hosting organisation or other responsible agency for University Information stored in University Information Management Systems hosted outside the IDC.

#### Business System Owners are accountable so that backup scopes and schedules implemented by University IT meet —

##### the business requirements and criticality of their University Information Management Systems; and

##### the requirements for the specific information assets as required by the appropriate Information Steward and/or Information Custodian.

#### University IT will perform periodic checks and proper maintenance of backup media so that University Information held on backup is viable and can be restored if required.

#### The University and University IT will not be responsible for the backup of University Information or other materials stored outside of the Institutional Data Centre, or endorsed University Information Management System.

Definitions

**Business Capability** is defined in section 4.2

**Business System Owner** is defined in section 4.4

**Copyright** is defined in the Intellectual Property Policy.

**Employee** is defined in the Policy Framework Policy.

**Information Custodian** is defined in section 4.3

**Information Owner** is defined in section 4.1

**Information Power User** is defined in section 4.5

**Information Protection** is defined in section 3

**Information Steward** is defined in section 4.2

**Information User** is defined in section 4.6

**Intellectual Property** is defined in the Intellectual Property Policy.

**IT Assets** is defined in the Cyber Security Policy.

**University** is defined in the Policy Framework Policy.

**University Business** is defined in the Policy Framework Policy.

**University Community** is defined in the Policy Framework Policy.

**University Information** is defined in section 3

**University Information Management System** is defined in section 8

End