

Website Governance Policy (DRAFT)

Objectives

1.1. The objectives of this policy are to:

- a) Protect the University, partner and stakeholder reputations by ensuring that University websites are of a consistent professional standard; meet accessibility standards; offer a seamless, digital experience; are protected against cyber attack and that the capture, storage and usage of data is secure and compliant.
- b) Support Advancing Melbourne by ensuring that the University digital experience for stakeholders is appropriate for a leading global University through adherence to digital best practice, including information architecture, navigation, and web design.
- c) Provide clear guidance for website owners on website management across the digital asset lifecycle.

2. Scope

2.1. This policy applies to all existing and new externally facing websites, and student-facing services that meet one or more of the following criteria:

- a) University branded and co-branded websites, including sub-brands; for avoidance of doubt, this applies to research initiatives where the University logo is used.
- b) Use the unimelb.edu.au domain
- c) Represent University “business”. (e.g. where content on a site is seeking research collaborations for a faculty, or soliciting of prospective graduate researcher enquiries.)
- d) Is hosted on University operated or indirectly financed services. (e.g. expensed to the University.)

3. Authority

3.1. This policy is made under the [University of Melbourne Act 2009 \(Vic\)](#) and the Vice-Chancellor [Regulation](#) and supports compliance with applicable standards, as set out in section 5.2 of this policy.

4. Policy

4.1. Website Owners are responsible for managing their website/s in compliance with this policy

4.2. Website Platform Owners are responsible for managing their University Website Platform/s in compliance with this policy.

4.3. A Website Owner is the nominated owner in the Website Register. In absence of a nominated owner, the default owner is the Faculty Executive Director and/or Head of Division.

4.4. Website Owners must remediate or decommission their site if it is in breach of this policy.

4.5. This policy is used in alignment and in conjunction with the University’s [Information Security Policy \(MPF1270\)](#), [Risk Management Policy \(MPF1194\)](#), [Provision and Acceptable Use of IT Policy \(MPF1314\)](#), and their supporting processes, standards and frameworks.

4.6. Websites are classified as Information Assets under the Information Security Policy (MPF1270) and must have asset and/or service owners assigned, to ensure:

- a) information captured, processed, and stored in websites are classified based on the University's information system and assets classification;

- b) websites are provisioned, modified, operated and decommissioned securely in accordance with this policy;
- c) information security risks relevant to the websites are managed and governed; and
- d) website security vulnerabilities are remediated in timely manner in accordance with The University Risk Management Policy.

5. Procedural principles

5.1. Websites must be assigned an owner and tracked in the Website Register.

5.2. To be compliant with this policy, Website Owners and Website Platform Owners must meet the mandatory requirements specified within the standards listed below.

Standard: Maintain website currency

Standard: Website platform

Standard: Website design

Standard: Website content

Standard: Personal data collection

Standard: Website accessibility

Standard: Website performance standard

5.3. For websites that do not meet the requirements of this policy and the Website Owner cannot be contacted to remediate, the site will be decommissioned.

5.4. For websites that do not meet the requirements of this policy and the Website Owner does not agree to remediate, the Website Owner has 30 days to gain approval for an exception from their Faculty Executive Director or equivalent via the Website Register. Failure to comply will result in decommissioning.

5.5. Website Owners are responsible for maintaining the security of the website and complying with the University's [Information Security Policy \(MPF1270\)](#).

6. Roles and responsibilities

<i>Role/Decision/Action</i>	<i>Responsibility</i>	<i>Conditions and limitations</i>
Maintain website policy, standards and procedures.	Director, Digital Experience & Marketing	Specialist teams to provide advice on their respective standards and procedures (including Cybersecurity, Accessibility and Brand)
Maintain services to support policy implementation.	Director, Digital Experience & Marketing	

Approve University Website Platform providers.	Chief Information Officer	
Maintain website/s to meet the mandatory requirements.	Website Owner	
Maintain Website Platform/s to meet the mandatory requirements.	Website Platform Owner	
Decide to decommission websites.	Website Owner	
Decide to decommission websites which do not comply with this policy, the owner cannot be contacted, and 30 days have passed without exception approval.	Associate Director, Digital Product Management	

7. Definitions

Accessibility: The practice of making websites usable by as many people as possible, including those with disabilities or impairments.

Collaboration Platform: A digital workspace where University members can work together on projects, share information, and communicate – e.g. github.com, SharePoint.

Decommission: The process of planning for and implementing the removal of a website from active service.

Hub: A central digital platform or website that aggregates and organises content, services, or information related to a specific topic, department, or function within the University. Hubs are designed to provide a unified and coherent user experience for accessing related resources and information.

Personal Data: Any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly.

University Website: Any website that meets one or more of the following criteria:

- Uses the unimelb.edu.au domain
- Is branded or co-branded with University of Melbourne identifiers
- Represents University "business" (e.g., research collaborations, faculty information)
- Is hosted on University operated or indirectly financed services

University Website Platform: The centralised, officially sanctioned web server hosting environments managed by the University. These platforms comply with University policies, standards, and security requirements, providing a consistent and reliable user experience across all digital properties associated with the University.

Website: A collection of related web pages, including multimedia content, typically identified with a common domain name, and published on at least one web server.

Website Owner: (note: this is known as Asset Owner in related policy [Information Security Policy MPF1270](#)) The person or entity responsible for managing the website in compliance with this policy. In the absence of a nominated owner, the default owner is the Faculty Executive Director and/or Head of Division.

Website Platform: Web server hosting instance for serving web pages to the Internet or Intranet.

Website Platform Owner: (note: this is known as Service Owner in related policy [Information Security Policy MPF1270](#)) An entity or function of the University that provides a service for members of the University community to publish web content.

Website Register: The official University record of all websites, their owners, and their compliance status.

POLICY APPROVER

VP Advancement, Comms & Marketing

POLICY STEWARD

Director, Digital Experience & Marketing

REVIEW

This policy is due to be reviewed by [insert date not more than **1 year** from date of approval].

VERSION HISTORY

Version	Approved By	Approval Date	Effective Date	Sections Modified
	Vice-President Advancement, Comms & Marketing			N/A