Reason for Policy

The University of Oregon's websites are the public face of the university. For many, these websites are the first point of contact. They must reflect the needs of our audiences and the university, and meet legal requirements for compliance, ensuring equal access for all users, including those who rely on assistive technologies.

This policy ensures that:

- **Websites provide accurate, accessible, and up-to-date information** that reflects the university's priorities
- **Roles and responsibilities are clearly defined**, so accountability is built into every stage of content creation and management
- **Design, content, technical, and records retention standards are followed**
- **The university can respond quickly** to platform, policy, or legal changes
- **Institutional risk is reduced**, and public trust in the university's digital presence is protected

---

Entities Affected by this Policy

- Anyone who creates, edits, or publishes content on a **uoregon.edu** website
- Anyone who designs, develops, or manages a UO website
- Vendors and third-party partners working on UO's websites

Web Site Address for this Policy

[Provided by Office of the University Secretary after policy is posted online]

Responsible Office

For questions about this policy, please contact the Department of Digital Strategy within University Communications: (541) 346-3134, bfh@uoregon.edu.

Enactment & Revision History

Day-Month-Year – [text]

Day-Month-Year – [text]

Policy

Core policy

This policy defines how University of Oregon websites are governed, who is responsible for them, and what rules must be followed to ensure quality, accessibility, and alignment with university standards.

Scope

This policy applies to all University of Oregon websites that use the **uoregon.edu domain or any of its subdomains** (i.e., admissions.uoregon.edu, law.uoregon.edu, blogs.uoregon.edu). It also applies to **websites that receive a redirect from a uoregon.edu domain,** regardless of the domain they ultimately use. This policy does not cover software applications - including learning platforms like Canvas and web applications like Banner - or external domains like goducks.com.

This includes:

- Sites built and maintained in official UO content management systems
- Custom or externally hosted websites representing the university
- Blogs, microsites, landing pages, and websites maintained on behalf of UO units, programs or initiatives

Website ownership

All websites that use the **uoregon.edu domain are the legal property of the University of Oregon, subject to the authority of the Board of Trustees**. This includes any websites created, managed, or funded by individual units, departments, or programs, regardless of where they are hosted or who created them.
While units and individuals may create and maintain these sites, they do so as custodians, not as owners.

Purpose

University of Oregon's websites are the public face of the university. For many, these websites are the first point of contact. They must reflect the needs of our audiences and the university, and meet legal requirements for compliance, ensuring equal access for all users, including those who rely on assistive technologies.

This policy ensures that:

- **Websites provide accurate, accessible, and up-to-date information** that reflects the university's priorities

- **Roles and responsibilities are clearly defined**, so accountability is built into every stage of content creation and management
- **Design, content, technical, and records retention standards are followed**
- **The university can respond quickly** to platform, policy, or legal changes
- **Institutional risk is reduced**, and public trust in the university's digital presence is protected

Goals

- Make UO's websites a strong, effective platform for sharing public information
- Define clear ownership and responsibilities
- Create a governance structure that supports accuracy, accessibility, continuity, and compliance

Procedures

The following procedures outline what units – through their designated Website Stewards and content contributors – must do to ensure their websites meet university standards for quality, accessibility, branding, and security.

Content

Units are responsible for keeping content accurate, timely, and aligned with UO's editorial, records management, and accessibility standards. Content should reflect the university's mission and avoid legal, reputational, security, or accessibility risks.

Prohibited content

Websites may not include:

- Content that implies or promotes endorsement of a political candidate or ballot measure by the university, unless it has been officially sanctioned by the Board of Trustees
- Copyrighted content without legal authorization
- Advertising for outside products or services unless there is a direct, written agreement with the university authorizing it
- Defamation or other unprotected speech

Questions about content may be submitted by emailing [GC office team].

Files

Downloadable files (i.e., PDFs, Word docs) must meet accessibility and records retention requirements. Website Stewards are responsible for ensuring compliance.

Brand alignment

All websites must be compliant with the University of Oregon's branding guidelines, including clear affiliation with the University - including use of standard university page templates, footers, disclaimers and logo masthead - standards for visual design, voice, and content structure, as provided by university communications in its branding guidelines. As these guidelines evolve, websites must be updated accordingly to maintain consistency and alignment with institutional identity.
Any exceptions to the university's branding standards must be approved in writing by University Communications. Contractors performing work that does not comply with brand standards must either obtain written approval from University Communications or will be required to remediate the work at their own expense.
Exception requests may be submitted by emailing [UC brand team].

Domains and web addresses

Sites must use **uoregon.edu** or an approved subdomain. Using the university's domain ensures greater security, brand alignment, and user trust.

- **Subdomain requests** must be submitted for review [insert link to form] and approval by the Web Governance Board
- **Third-party domains** (i.e., .org, .com) may not be used without written approval from University Communications and the Web Governance Board
- **Vanity URLs or redirects** must follow university standards and be coordinated through approved channels
- **University funds may not be used** to purchase or maintain non-approved domains

Use of unapproved domains may result in removal of redirects, exclusion from university systems, or other enforcement actions.
Exception requests may be submitted by emailing [insert email address].

Fundraising

Only University of Oregon-approved fundraising activities are permitted on university websites. This includes campaigns and giving opportunities that are coordinated with or approved by University Advancement.
All donation-related content must:

- Clearly identify the official university program or initiative it supports
- Be reviewed for compliance with university branding, accessibility, and legal standards

Fundraising efforts that are not explicitly approved may be removed.
Questions or requests for approval can be directed to [insert email address].

Licensing and assets

Images, fonts, and other assets must follow copyright laws. Use only licensed, public domain, or UO-owned content.

Outsourcing

External vendors may not design, host, or maintain UO websites without prior review and approval by the Web Governance Board.
This applies to outsourced web services, including:

- Website design or development
- Content Management System (CMS) setup or customization
- Hosting outside of university-managed environments
- Ongoing website maintenance and support

Approval ensures that vendor work complies with university standards for branding, accessibility, security, and governance.
Units currently working with external vendors must confirm that vendor work aligns with this policy or seek review from the Web Governance Board.
Requests for review can be submitted to [insert email address].

Non-university-related uses

The **uoregon.edu** domain and its subdomains – including any UO-affiliated blogs - may not be used for commercial or non-university-related purposes.
Content that reflects an individual's academic, research, or instructional role may be appropriate–including content protected under the principles of academic freedom–but must still comply with university policies for accessibility, acceptable use, and other applicable standards.
Student organizations and course-related or student portfolio websites should be hosted on designated subdomains [insert link here]. These spaces are designed to support student and instructional use while maintaining separation from official university web properties.

Unauthorized use

Non-university organizations may not use UO's hosting, CMS, theme, or domains without written approval from the Web Governance Board.

Source code

All source code used on university websites must follow recognized best practices for security, accessibility, and maintainability. This includes:

- Avoiding deprecated or unsupported frameworks and libraries
- Ensuring code is regularly updated and patched
- Following security standards, such as those published by OWASP
- Follow web development standards and approaches, ensuring source code is compliant with applicable standards related to security, performance, continuity, and accessibility

Code that introduces vulnerabilities, violates accessibility standards, or overuses infrastructure resources may result in the Web Governance Board, or delegated authority, taking appropriate actions to mitigate risk to the university. This includes, but is not limited to, disabling or blocking traffic to the website.

Website hosting

All university websites must be hosted on the university's official, sponsored hosting platforms. These platforms are managed and approved by Information Services in coordination with the Web Governance Board to ensure security, performance, continuity, and compliance.

- Private website hosting—including use of personal web servers, devices, or third-party platforms not approved by the university—is not permitted
- Hosting websites on other university-owned servers outside the sponsored environments is also prohibited, unless explicitly approved by the Web Governance Board

Use of unapproved hosting may result in the site being taken offline or removed from university systems.

Monitoring and enforcement

The Web Governance Board is responsible for monitoring university websites for compliance with this policy. It has the authority to enforce the policy, including the disabling of websites, individual content, or access to university web systems when necessary.

Attestation

Each website must have a designated Website Steward—who must be a current full-time staff or faculty member—who completes an annual compliance attestation.

Sanctions

Non-compliance may result in content removal, revoked access, or disabling of the site. Issues will be escalated as needed.
To appeal any sanction, email [sanction email address].

Related Resources

The website policy builds on many existing policies in the organization. These include but may not be limited to the following:

- Information and Communications Technology Accessibility
- Acceptable Use (in review)
- Information Asset Classification & Management | University of Oregon Policy Library
- Purchasing and Contracts for Goods and Services
- Academic Policies, Procedures, and Guidance
- Academic Freedom, Freedom of Inquiry, and Free Speech

- Political Activities
- Fund Raising
- Oregon Brand Guide
- University Records Management | University of Oregon Policy Library
- Data Security Incident Response | University of Oregon Policy Library
- Intellectual Property Policies & Guidelines

UNIVERSITY OF OREGON

University Websites Policy

Stakeholder Consultation

60+ STAKEHOLDERS. 17+ SESSIONS. MARCH 2025–FEBRUARY 2026.

Over the last nine months, we have engaged executive leadership, faculty, governance, technical teams, communications professionals, and legal counsel to ensure the policy works for the people who'll implement it.

These groups and individuals were engaged at varying levels—some helped us define what we should and shouldn't govern about university sites, others reviewed working drafts to refine language and identify gaps, and still others provided technical or legal review to ensure the policy aligns with existing requirements.

Working Group

- Carol Keese, VP for Communications & Marketing
- Abhijit Pandit, VP for Information Technology
- Brian Hawkins, AVP for Digital Strategy
- Melody Riley Ralphs, AVP for Enterprise Systems (retired 2025)

Executive Leadership

The following table summarizes the consultations held with Executive Leadership:

Group/Individual	Date(s)	Key Participants
President	June 18, 2025	Karl Scholz, Kassy Fisher, Carol Keese
General Counsel	See Legal and Risk	Kevin Reed
President's Executive Team	July 14, 2025, Dec 15, 2025	Full team (two sessions)
Vice President for Enrollment Management	July 11, 2025	Derek Kindle, Carol Keese
Provost	July 8, 2025	Chris Long, Carol Keese
Provost's Office	Dec 3, 2025; Jan 7, 2026	Chris Long, Allison Blade, Saul Hubbard
Senior Vice President for Finance and Administration	February 20, 2026	Jamie Moffitt

Governance & Faculty

Consultations with Governance and Faculty groups are detailed below:

Group/Individual	Date(s)	Key Participants
SERMC	August 13, 2025	Committee-level review
SERMC web Working Group	April 24, June 26, 2025	Melody Riley Ralphs, Abhijit Pandit, Brian Hawkins, Carol Keese
Faculty Advisory Committee	January 12, 2026	Committee-level review
Special Provost's Council on Web Governance	February 18, 2026	Chris Long, Abhijit Pandit, Hal Sadofsky, Kate McLaughlin, Carol Stabile, Brian Fox, Alicia Salaz, Jen Reynolds, Kate Morris, Bruce Blonigen, Adrian Elisheva Parr Zaretsky, Allison Blade, Dennis Galvan, Emily Tanner-Smith, Grant

Group/Individual	Date(s)	Key Participants
SERMC	August 13, 2025	Committee-level review
SERMC web Working Group	April 24, June 26, 2025	Melody Riley Ralphs, Abhijit Pandit, Brian Hawkins, Carol Keese
		Schoonover, Regina Lawrence, Renee Irvin, Sabrina Madison-Cannon, Carol Keese, Brian Hawkins, Krista Chronister

Technical & Accessibility

The following technical and accessibility groups provided feedback:

Group/Individual	Date(s)	Key Participants
Information Services	July 17, 2025 Aug 27, 2025	Melody Riley Ralphs, Abhijit Pandit, Carol Keese, Derek Wormdahl
Accessibility Architect	October 10, 2025	Grey Pierce
Records Management	November 13, 2025	Mahnaz Ghaznavi

Legal & Risk

Group/Individual	Date(s)	Key Participants
General Counsel	June 30, 2025	Kevin Reed, Carol Keese
Risk & Safety	July 1, 2025	Andre LeDuc, Brian Hawkins, Carol Keese

Chiefs of Staff

July 17, 2025: Allison Blade, Anna Schmidt, Christy Long, Deborah Butler, Jason Kovac, Julia Cohalan, Kaia Rogers, Kassy Fisher, Anna Shamble, Keith Frazee, Kelly Pembleton, Krista Dillon, Kristyn Elton, Moira Kiltie, Lauren Crockett, Kate Petcosky

This group helped us understand how the policy would interact with existing unit processes and where operational concerns might create friction.

Communications Leads

August 14, 2025: Andra Brichacek Roe, Dave Austin, Lewis Taylor, Nick Noyes, Cathy Kralik, Sara Ellis, Heidi Hiaasen, Jim Engelhardt, Juls Davis, Nikki Harris, Josh Green

This group was consulted on what a web policy should and shouldn't do—helping us understand where central governance adds value and where it would create unnecessary friction.