

POLICY CONCEPTS: INSTRUCTIONS AND GUIDELINES

All policy proposals – including new policy concepts, proposed revisions, or suggested repeals – must be submitted via the form on page 2 to the Office of the University Secretary with appropriate supporting information and documents. Completed submissions are forwarded to the University Senate (academic policies) or the President's Policy Advisory Council (PAC), which ensures proper routing through the policy-making process. (See UO Policy I.03.01 for more information.)

Please keep the following definition of a university policy in mind as you develop your concept:

A University Policy ("Policy") is a policy that (1) has broad application or impact throughout the University community, (2) must be implemented to ensure compliance with state or federal law, (3) is necessary to enhance the University's mission, to ensure institutional consistency and operational efficiency, or to mitigate institutional risks; or (4) is otherwise designated by the Board [of Trustees] or the President [of the University] as a University Policy.

A policy establishes rights, requirements or responsibilities. Excluded from this definition are things such as, but not limited to, implementation guides, operating guidelines, internal procedures, and similar management controls and tools.

To help facilitate as smooth a process as possible, please consider the following:

1. Consult as many stakeholders as possible *prior to submitting* your concept. A primary role for the PAC is to ensure that appropriate offices, departments or groups are consulted.
2. Run your concept by the Office of General Counsel (OGC) *prior to submission*. OGC review is a required step in policy-making.
3. Please use the proper template – email uopolicy@uoregon.edu to obtain either (a) the new policy template (new proposals) or (b) the Word version of the existing policy in its proper template (for redlines/revisions).
4. A "redlined" version of your concept in Word is required for proposed revisions. This must be done using the appropriate Word version (see #3, above).
5. Include any appropriate related resources that will be useful to those reviewing the concept. Links are preferred, but supplemental documents are of course acceptable for items not online. Examples of such items include any associated procedures or unit level policies (even if in draft form), or other policies or procedures related to, overridden by, necessary as a result of, or otherwise affiliated with your concept;
6. Please submit all documents as individual files.
7. Someone from the responsible office or proposing unit will need to attend a PAC meeting to explain the concept and answer any questions.

Please email uopolicy@uoregon.edu if you have any questions. Thank you!

POLICY CONCEPT FORM

Name and UO Title/Affiliation:	José A. Domínguez, Chief Information Security Officer
Policy Title & # (if applicable):	Privacy Policy
Submitted on Behalf Of:	Self
Responsible Executive Officer:	Jammie Moffitt, Senior Vice President for Finance and Administration/CFO

SELECT ONE: ☒ **New Policy** ☐ **Revision** ☐ **Repeal**

Click the box to select

HAS THE OFFICE OF GENERAL COUNSEL REVIEWED THIS CONCEPT: ☒ **Yes** ☐ **No**

If yes, which attorney(s): Ryan Hagemann, Jessica Price

GENERAL SUBJECT MATTER

Include the policy name and number of any existing policies associated with this concept.

Here are several policies that cover some elements of privacy for data the university collects and manages:

Student Records – III.05.03

University Records Management – IV.10.01

Faculty Records Policy – OAR 571.030

RELATED STATUTES, REGULATIONS, POLICIES, ETC.

List known statutes, regulations, policies (including unit level policies), or similar related to or impacted by the concept. Include hyperlinks where possible, excerpts when practical (e.g. a short statute), or attachments if necessary. Examples: statute that negates the need for or requires updates to an existing policy; unit level policy(ies) proposed for University-wide enactment; or existing policies used in a new, merged and updated policy.

The following is a list of external statutes and regulations that call for or make references to expectation of privacy for personally identifiable information:

- Family Educational Rights and Privacy Act (FERPA) – <https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>
- Health Insurance Portability and Accountability Act (HIPAA) – <https://www.hhs.gov/hipaa/index.html>
- General Data Protection Regulation (GDPR) – <https://gdpr-info.eu/>
- Oregon Public Records Law – <https://www.doj.state.or.us/oregon-department-of-justice/public-records/attorney-generals-public-records-and-meetings-manual/i-public-records/>
- Oregon Consumer Privacy Act – <https://olis.oregonlegislature.gov/liz/2023R1/Downloads/MeasureDocument/SB619/Enrolled>

STATEMENT OF NEED

What does this concept accomplish and why is it necessary?

Protection of personal and institutional information is critical to maintain the university's operational and social responsibility reputation in addition to compliance adherence to many of the regulatory requirements that apply to the University of Oregon.

Today, the university web templates have a PRIVACY POLICY entry that points to our student records privacy policy published by the University Registrar in accordance with the Student Records policy. That particular statement only applies to student information and does not apply to all data collected and managed by the University.

This policy is the result of work performed by the SERMC privacy working group. During the discovery phaser, we observed that in the absence of a university-wide privacy policy and policy notice, many web sites have created and published their own privacy policy and notice statements. This new privacy policy and the accompanying privacy notice will serve as the baseline to be used by all university entities in the absence of a more stringent privacy policy and privacy notice, as those required by regulatory or contractual requirements.

AFFECTED PARTIES

Who is impacted by this change, and how?

This policy applies to the university as an enterprise, including but not limited to all university offices, units, and departments that collect, store, use, disclose or manage data related to UO employees, students, alumni, retirees, volunteers, visitors, contractors, vendors, customers, certain third parties, and research subjects.

CONSULTED STAKEHOLDERS

Which offices/departments have reviewed your concept and are they confirmed as supportive? (Please do not provide a list of every individual consulted. Remain focused on stakeholders (e.g. ASUO, Office of the Provost, Registrar, Title IX Coordinator, etc.).)

Name	Office	Date
SEE APPENDIX A FOR LIST OF STAKEHOLDERS CONSULTED. WHEN SEVERAL INDIVIDUALS WERE CONSULTED, THE WORD "MULTIPLE" WAS USED UNDER THE NAME HEADING.		

APPENDIX A – STAKEHOLDERS CONSULTED

Name	Office	Date Contacted
Tim Inman	Board of Trustees	5-Oct-2023
Multiple	Business Affairs	13-Mar-2023
Carol Stabile	Clark Honors College	14-Mar-2023
Multiple	College of Arts & Sciences	14-Mar-2023
Adrian Parr	College of Design	14-Mar-2023
Laura Lee McIntyre	College of Education	14-Mar-2023
Kathie Stanley	Division of Student Life	10-Mar-2023
Multiple	Finance & Administration	10-Mar-2023
Multiple	Financial Aid & Scholarships	13-Mar-2023
Krista Chronister	Graduate School	14-Mar-2023
Multiple	Human Resources	10-Mar-2023
Multiple	Information Services	1-Mar-2023
J P Monroe	Institutional Research	13-Mar-2023
Multiple	Intercollegiate Athletics	10-Mar-2023
Moira Kiltie	Knight Campus for Accelerating Scientific Impact	10-Mar-2023
Marcilynn Burke	Law School	14-Mar-2023
Bruce Blonigen	Lundquist College of Business	14-Mar-2023
Multiple	Office of Admissions	13-Mar-2023
Ryan Hagemann and others	Office of General Counsel	10-Mar-2023
Multiple	Office of Internal Audit	13-Mar-2023
Multiple	Office of Research and Innovation	10-Mar-2023
Multiple	Office of the Provost	13-Mar-2023
Multiple	Office of the Registrar	13-Mar-2023
Kassy Fisher	President's Office	10-Mar-2023
Mahnaz Ghaznavi	Public Records Office	14-Mar-2023
Multiple	Safety & Risk Services	14-Mar-2023
Sabrina Madison-Cannon	School of Music and Dance	14-Mar-2023
Juan-Carlos Molleda	Schools of Journalism & Communication	14-Mar-2023
Anna Schmidt-MacKenzie	Student Services & Enrollment Management	10-Mar-2023
Kimberly Johnson	Undergraduate Education and Student Success	14-Mar-2023
Multiple	University Advancement	10-Mar-2023
Multiple	University Communications	10-Mar-2023
Multiple	University Faculty Senate	13-Mar-2023
Multiple	University Faculty Senate	13-Mar-2023
Multiple	University Health Services	13-Mar-2023
Michael Griffel	University Housing	23-Mar-2023

Multiple	University Libraries	13-Mar-2023
Multiple	VP for Equity & Inclusion	10-Mar-2023



Policy Concept Form

As part of the University of Oregon Policy development process, all new Policy proposals, as well as proposals for the revision or repeal of existing Policies, must be submitted via this form to the University Secretary (the policy custodian). The Secretary will forward completed concept forms to the President's Policy Advisory Council for consideration pursuant to the University's Policy on University Policies. Please remember:

A "Policy" as defined by the University Policy on Policies (1) has broad application or impact throughout the University community, (2) must be implemented to ensure compliance with state or federal law, (3) is necessary to enhance the University's mission, to ensure institutional consistency and operational efficiency, or to mitigate institutional risks; or (4) is otherwise designated by the Board or the President as a University Policy subject to the Policy-Making Process authorized in Section 4. A policy establishes rights, requirements or responsibilities. Excluded from this definition are things such as, but not limited to, implementation guides, operating guidelines, internal procedures, and similar management controls and tools.

[Complete the following information as thoroughly as possible; response boxes will expand as filled.]

CONCEPT SUBMITTED BY:

NAME:	
PHONE:	
EMAIL:	
ORGANIZATION:	

POLICY CONCEPT SUBJECT MATTER (including existing policy number if appropriate):

--

STATEMENT OF NEED FOR THIS POLICY CONCEPT (i.e. What is the problem this concept seeks to address, and how does this proposal do so?):

WHO OR WHAT MIGHT BE AFFECTED BY THIS POLICY CONCEPT, AND HOW? *List all individuals, groups, etc. that would be impacted by this concept and the nature of any possible impacts (both positive and negative).*

WHAT COSTS MIGHT BE ASSOCIATED WITH THIS CONCEPT, BOTH IMPLEMENTATION AND RECURRING?

WHAT OTHER RESOURCES (HUMAN, PHYSICAL, OPERATIONAL, FINANCIAL, TECHNOLOGICAL, ETC.), WILL BE NEEDED TO IMPLEMENT AND MAINTAIN COMPLIANCE WITH THIS POLICY?

--

DOES THE PROPOSED CONCEPT IMPACT EXISTING POLICIES, GUIDELINES OR PROCEDURES? DOES THE PROPOSED CONCEPT RELATE TO A MATTER WITHIN A UNION CONTRACT? IF SO, PLEASE LIST.

--

ADDITIONAL INFORMATION YOU WISH TO SHARE?

--

PLEASE PROVIDE ANY SUGGESTED LANGUAGE AS AN ATTACHMENT TO THIS FORM.

FOR OFFICE USE ONLY
Date Received:

University of Oregon Privacy Notice

The University of Oregon (“university” or “UO”) Privacy Notice applies to university conduct or activities involving the collection, use, storage, disclosure or management of personal information including but not limited to conduct or activities described in the university’s Privacy Policy. This notice provides the minimum baseline guidance for the reasonable expectation of privacy in personal information in the absence of more specific legal, policy, or contractual requirements. It also presents a broad overview of the range of conduct or activities that require the processing of personal information and the university’s general approach to safeguarding personal information. However, schools, colleges, and departments at the UO may have additional privacy notices, practices and requirements that are related to their specific collection and practices regarding the processing of personal information. Likewise, different individuals or groups of people (e.g., students, faculty, patients, research subjects) may be entitled to heightened privacy protections by virtue of their relationship to the university and specific privacy laws and university policies.

The university values the reasonable privacy expectations of members of the university community and strives to protect the reasonable expectation of privacy by:

- Informing individuals about our information and privacy policies, procedures and practices;
- Collecting the minimum amount of personal information necessary for legitimate business purposes and legal compliance;
- Limiting access to personal information to appropriate and authorized individuals;
- Using appropriate physical and technical security measures to protect personal information, and
- Integrating privacy principles in the design of projects that involve use of personal information.

This document is for notice purposes only and it is not intended to create new or additional rights or a contractual relationship with any party or person.

Definitions

In this notice, “*personal information*” means any recorded information or data that is about an individual person and from which that person can be identified. It does not include information where an individual person's identity has been removed (e.g., anonymous or redacted information).

“*Personal information processing*” means anything that any individual acting on behalf of the university does with the personal information – including, but not limited to collection, use, storage, disclosure, conversion, migration, deletion, or retention.

Types of Personal Information We May Collect

UO may collect personal information from individuals directly, through information that individuals provide and/or automated processes (e.g., learning management tools or UO websites), or from third

party entities. Examples of personal information that might be collected for different groups of people at an institutional level include:

- *Prospective Students*: to facilitate admission and provide higher education services, UO collects personal and family information related to the application and financial aid process (including supporting documentation), identification and contact information, education history, demographic information (e.g., race, gender, and age) as volunteered, testing history, personal information and history, employment history, and payment information.
- *Students*: to register, administer financial aid, provide housing, track academic progress, and provide academic advising and other services, UO uses information submitted as prospective students, information related to academic record and performance, subscription data for online courses, and video images recorded by our video security systems for the purposes of ensuring physical security and to protect university individuals and property. The university also uses photos for photo identification and identification at the time of accessing services for validation (e.g., academic advising).
- *Faculty and staff*: to administer an employment relationship with the university, the university collects identification, contact information, demographic information as volunteered, access to protected environments, biographic information, employment and education history, payment and tax information, family and health information related to benefits, information related to performance at work (e.g., for health, safety, and compliance purposes) and video images recorded by our video security systems for the purposes of ensuring physical security and to protect university individuals and property. The university also uses photos for photo identification and identification at the time of accessing services for validation.
- *Visiting scholars and exchange students*: to facilitate their time at the university, UO may collect identification, contact information, demographic information as volunteered, biographic information, and possibly data related to health as relevant.
- *Donors and Alumni*: to manage their relationship and engagement with the university, the university collects identification, contact information, and donor information.
- *Research subjects*: in the exercise of scientific, historical research, or for statistical purposes, the university collects identification and contact information and all information that is produced and observed in relation to the subject as part of a research project.
- *Participants in conferences, symposia, and other campus events*: to register, track payment, and support participation, the university collects identification, contact information, payment information, demographic information as volunteered, and possibly data related to health for accommodation.
- *Website visitors*: to understand and save their preferences for future visits and compile aggregate data about site traffic and site interaction so that we can offer better site experiences, the university may collect IP address, browser type, internet service provider, operating system, date and time of visit, location information, pages visited, pages interactions, such as link clicks, scroll depth, and other information submitted directly via a web form or collected through or stored in web cookies.

- *Campus visitors:* To facilitate their visit, the university collects contact information, payment information, and video images recorded by our video security systems to ensure physical safety and security and to protect university property.

The university occasionally processes other types of personal information for various legitimate and specific purposes. When these situations occur, the university endeavors to inform covered subjects of such occasional processing activities.

How We Use Your Personal Information

UO uses the personal information it collects to facilitate and discharge administrative, educational, and research activities and operations of the university. UO only uses your personal information for the lawful and appropriate purposes for which the personal information was collected unless the university reasonably concludes that it is needed for and may be used for another legitimate reason.

Sharing Your Information with Third Parties

The university may share or disclose your personal information with third parties who contract with the university to help it operate and/or administer and discharge its obligations. The university permits third parties to process your information only for specified purposes in accordance with the UO's instructions or contracts, and UO seeks to share necessary and pertinent information only.

UO may also share your personal information with third parties to comply with certain legal obligations, administer a contract, and/or assist university-affiliated programs regarding contacting you about goods, services, charitable giving, or experiences that may be of personal interest.

Other circumstances where the university may need to share your personal information with third parties include when the university has consent to do so or when it is necessary to protect the health and safety of you or others.

How We Secure Your Information

UO recognizes the importance of securing the information it collects and maintains. While the university cannot guarantee that information submitted over the internet is completely secure, it is committed to protecting the privacy of individuals who access our systems. The university deploys reasonable security measures, including but not limited to physical, administrative, and technical safeguards, to protect personal information.

Notice and Consent

Where required by applicable law, prior to collection of personal information, the university will make available a notice that describes the personal information that will be collected, how it will be processed, and with whom the personal information will be shared. The university will also seek individual consent when it is required by applicable law.

Exceptions to this notice and consent requirement are permitted to the extent allowed under law.

Regulations Informing Our Privacy Practices

UO's practices are informed by various legal and regulatory requirements, university policies, and industry best practices. In addition, different groups within the university are subject to more specific privacy regulatory requirements. Below is a nonexclusive list of some of the most frequently implicated regulatory provisions impacting privacy at the UO:

Family Educational Rights and Privacy Act (FERPA)

The university is required to comply with the federal [Family Educational Rights and Privacy Act of 1974](#). The university has a policy that outlines the requirements that must be followed with regard to student education records: <https://policies.uoregon.edu/student-records-1>.

Health Insurance Portability and Accountability Act (HIPAA)

In some cases, the university is required to comply with the [Health Insurance Portability and Accountability Act](#). Additional information about the university's compliance information can be found here: <https://safety.uoregon.edu/university-oregon-hipaa-privacy-team>.

General Data Protection Regulation (GDPR)

In addition to the general privacy information above, the [GDPR](#) outlines the collection, use and disclosure of certain personal data provided to the UO. Additional information about GDPR and the university's compliance requirements can be found here: <https://service.uoregon.edu/TDClient/2030/Portal/KB/ArticleDet?!ID=127175>.

Oregon Public Records Law

Information collected, used, disclosed and stored by the university is generally subject to the Oregon Public Records Law and therefore subject to inspection by the general public unless an applicable exemption applies. More information about the Oregon Public Records law can be found in the [Oregon Attorney General Public Records and Meetings Manual](#) and the [Oregon Public Records Advocate](#).

Records Retention Schedule

For information on how long the university retains records, please visit the university's Records Retention Schedule: <https://rrs.uoregon.edu/>.

Collection of Data about Children or Minors

The University of Oregon does not knowingly collect personal information from children or minors as defined by the Children's Online Privacy Protection Act (COPPA) on its general websites. The collection and use of personal information from children or minors for other purposes is subject to supplemental and more specific notification or consent terms.

Links to and References from Third-party Websites and Services

University websites (e.g., uoregon.edu) contain links to, and may be linked from, sites outside of the University of Oregon. The university is not responsible for the privacy practices, terms of use, or the content of such platforms, websites, and services. A link to an outside platform, website, service or



embed of content on uoregon.edu does not constitute an endorsement or sponsorship of the site, service, or its contents. In addition, the University of Oregon may embed content, such as video, social media feeds or tracking mechanisms such as pixels, that allow for collection of data by third parties to provide visitors with services.

Privacy Notice Changes

This privacy notice may be updated from time to time. The notice will include the date of the latest update.

Contact

If you have any questions about our practices around the use of personal information, contact privacyofficer@uoregon.edu.

Last Updated: May 5, 2025

Reason for Policy

The University of Oregon (“university” or “UO”) values our community’s right to privacy, safeguards personal information, and ensures the appropriate institutional use of personal information provided to or maintained by the university. This policy defines some common terms and outlines the reasonable expectations of privacy throughout the collection, storage, use, and disclosure of personal information provided to or maintained by the university.

Entities Affected by this Policy

This policy applies to the university as an enterprise, including but not limited to all university offices, units, and departments that collect, store, use, disclose or manage data related to UO employees, students, alumni, retirees, volunteers, visitors, contractors, vendors, customers, certain third parties, and research subjects. This policy provides the minimum baseline guidance regarding the reasonable expectation of privacy in the absence of more detailed legal, policy, or contractual requirements.

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 Office of the Chief Information Security Officer, (541) 346-1701, or ciso@uoregon.edu.

Enactment & Revision History

Day-Month-Year – [text]

Day-Month-Year – [text]

Definitions

In this policy, unless otherwise defined by applicable law, the following definitions apply:

"Disclosure" means the release, transfer, provision of, access to, or divulging in any other manner, of information outside the UO office, unit, or department storing, or maintaining the personal information. “Disclose” has the corresponding meaning.

"Personal information" means any recorded information or data that is about an individual person and from which that person can be identified. It does not include information where an individual person's identity has been removed (e.g. anonymous or redacted information).

"Personal information processing" means anything that any individual acting on behalf of the university does with the personal information – including but not limited to collection, use, storage, disclosure, conversion, migration, deletion, or retention.

“Information Technology (IT) System” means an information system, a communications system, or, more specifically, a computer system — including but not limited to all hardware, software, and peripheral equipment — operated by a limited group of IT users.

“(IT) System Maintenance” means a set of actions to ensure that an IT system remains secure and operational. It typically involves three main maintenance types: preventive, corrective, and proactive. Preventive maintenance focuses on routine tasks to prevent system issues (e.g., software updates and security patches). Corrective maintenance addresses problems as they arise, such as repairing or replacing parts. Proactive maintenance seeks to improve system performance and longevity by upgrading software or hardware when necessary, ensuring systems continue to run efficiently.

“University Privacy Officer Representative” means the function of a university employee in the Information Security Office who is responsible for responding to inquiries about data privacy. The University Privacy Officer Representative can be reached at privacyofficer@uoregon.edu.

Policy

The University of Oregon is committed to protecting personal information and the reasonable expectation of privacy to the extent possible, subject to state and federal law. The university limits the collection, use, sharing, and storage of personal information except where reasonably necessary to serve the institution’s academic, research, or administrative functions, including but not limited non-UO external third parties who contract with the university to help administer its operations, or other legally permitted purposes. Such collection, use, sharing, and storage must comply with applicable laws, rules and regulations, as well as the policies, standards, and procedures of the university. Other than as stated above, or as required by legal or regulatory requirements that guarantee public access to certain types of information (e.g., laws, regulations, valid subpoenas, applicable legal instruments), personal information is not actively disclosed to non-UO external third parties.

Reasonable Expectations of Privacy of Personal Information

While information collected, used, disclosed, and stored by the university is UO’s public property and may reasonably be subject to the Oregon Public Records Law outlined at ORS Chapter 192 without a reasonable expectation of privacy, the university recognizes a reasonable expectation of privacy may exist for some personal information subject to applicable laws and university policies and procedures. While the university strives to protect personal information and uses reasonable technical, organizational, and administrative efforts to do so, it cannot guarantee absolute privacy of all such information. In addition to the above-mentioned institutional purposes, individuals can expect personal information to be used by the institution under the following circumstances:

- System maintenance or administrative, academic, and research operations, including but not limited to security measures;
- valid consent from the individual to share their information;
- provision of university services internally or by non-UO third parties;

- disclosure to protect the health, safety, or property of any individual or in the event of an emergency facing the university;
- investigation of suspected violations of legal requirements or institutional policy;
- fulfillment of legal obligations under Oregon Public Records Law or other applicable laws, regulations, subpoenas, orders, or institutional policies, rules, or guidelines; and
- as permitted by applicable law or policy.

Privacy Notice

The university will maintain and publish a privacy notice to describe, at a minimum, the type of information the university collects, how the information is used, and to whom the information is or may be disclosed. This applies to the collection of general information and personal information. The notice will be posted in conspicuous locations including but not limited to the university's websites.

Responsibilities

- a. Data and information privacy are the shared responsibility of all members of the university community. All members of the university community are expected to follow and support the university's privacy policy and associated procedures.
- b. The provost and vice presidents are responsible to ensure implementation and enforcement of this policy in all IT systems and services within their respective portfolios.
- c. All administrators, deans, department heads, directors, supervisors and/or principal investigators are directly accountable for maintaining the privacy of personal information that is collected in areas for which they are responsible. This includes but is not limited to the establishment and management of data privacy procedures as well as ongoing support by each unit for data privacy, including but not limited to appropriate training on data protection strategies and tools.
- d. The Information Security Office is responsible for providing training, technical expertise and assistance to campus partners regarding compliance with laws, regulations, and policies associated with the protection of personal and other protected data.
- e. All employees are responsible for reporting all data disclosures and incidents, unintended or otherwise, involving unauthorized access to personal information. Such a report shall be made to an immediate supervisor who shall report the situation to the appropriate person or office for action. Additionally, it can be directly reported to the University Privacy Officer Representative.

Related Resources

[University of Oregon Privacy Notice](#)

[Information Asset Classification & Management Policy](#)

[Data Security Incident Response Policy](#)