

## Privacy Policy

### I. Policy Statement

Portland State University (sometimes referred to in this policy as “PSU” or “the University”) respects personal privacy and is committed to protecting it. A set of [privacy principles](#), underpin this commitment, and shape this policy. All members of the PSU Community must familiarize themselves with PSU’s privacy principles and abide by them, particularly those members who interact with or collect personal data. All members of the PSU Community should also read and reference PSU’s [privacy notice](#), a public statement of PSU’s current data practices.

### II. Reason for Policy/Purpose

- This policy establishes the ways in which PSU Community members are required to protect the privacy of information — particularly identifiable information — in any form.
- In addition, it contains rules on how PSU Community members collect, use and share personal information in accordance with all applicable laws.
- To support the implementation of PSU’s [privacy principles](#).

### III. Applicability

- This policy is applicable to all members of the PSU Community and others with access to the PSU campus and PSU’s data.
- This policy applies to the personal data in the custody and control of PSU.

### IV. Definitions

- **Breach of Information** — Breach of Information means any technical or physical incident or set of circumstances that leads to the unauthorized, accidental, or unlawful access to, or destruction, loss, alteration, or disclosure of personal information.

- **Data Stewards** — Data stewards are employees who oversee the use and protection of data in their designated area of responsibility, including the authorization of the release of data for internal use, and also with third party vendors. For a more detailed description, see the [Information Security Policy](#).
- **Data Subject Access Request** — A data subject access request (DSAR) is a request from an individual to Portland State University asking, for example, for access to or modification of Personally Identifiable Information (PII), or changes in how the university processes such data. An individual may have additional rights under applicable data privacy regulations, such as, without limitation, the European Union’s General Data Protection Regulation (GDPR), or similar regulations.
- **Disclosure** — Disclosure means the release of, transfer of, provision of access to, or other communication or dissemination of PII within or outside of the PSU Community.
- **Personally Identifiable Information (PII)** — PII is any representation of data that can be used to identify a specific individual either directly (e.g., name, ssn, address) or indirectly (using a combination of data elements such as gender, race, birthdate, etc.). Technology has expanded the scope of PII considerably and data elements such as IP address, login IDs, social media posts, digital images, geolocation, and biometric can also be classified as PII.
- **Processing** — Processing means any operation or set of operations performed on PII or on sets of PII, whether or not by automated means, such as collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, combination, restriction, erasure, or destruction.
- **PSU Community** — The PSU Community includes students, faculty, staff, units, departments, schools, colleges, third-party vendors and advisors.
- **Privacy Standards** - The standards, rules, and/or guidelines adopted by Chief Information Security Officer (CISO) and Data Privacy Officer (DPO) pursuant to this policy.

## V. Policy

### ○ Limit Collection and Storage

1. Portland State University will limit the processing of personal data to that which reasonably serves the University's academic, research, or administrative functions, or other legally required purposes. Such data processing should comply with applicable Federal, State and International laws and regulations, and University policies.

### ○ Protection of PII

1. All systems that house information classified as "Restricted," such as PII, are subject to the [Oregon Data Security Breach Notification](#) Laws, and/or other applicable data breach notification laws.
- **Vendor Contracts**
  1. In the event that a unit, department, or individual seeks to enter into a contract that involves PII, such unit, department, or individual shall work with the Office of Information Technology and the appropriate designated data steward to ensure that adequate and appropriate safeguards and contractual provisions are in place relating to the processing of this PII before entering the contract.
- **Special Categories of Information**
  1. Prohibited Information
    - a) The University prohibits the collection and Processing of tax identifiers (Social Security Numbers and Individual Taxpayer Identification Numbers), drivers license numbers and financial account information, except in specific circumstances and by the written approval of the Data Protection Officer.
    - b) Examples of where the university collects tax identifiers are:
      - (1) The University must maintain a record of tax identifiers for those students who have been or are being awarded financial aid, for students who are seeking loan deferrals, and for federal tax reporting compliance. More information on collection and use of student tax identifiers can be found in the [Student Records Privacy & Policy webpage](#).
      - (2) The University maintains a record of tax identifiers for contracting and processing vendor payments when an Employer Identification Number (EIN) is not available.
      - (3) The University maintains a record of tax identifiers for employees ID verification, payroll processing and for federal tax reporting compliance.
  2. Student Records (FERPA)
    - a) Students have rights with respect to access to their education records under the Family Educational Rights and Privacy Act of 1974 ("FERPA"). These rights are outlined in the [Student Records & Privacy Policy webpage](#).

3. Human Subjects Research (Common Rule)
    - a) PSU's human subjects protection program safeguards the rights and well-being of individuals involved in research at PSU by reviewing proposed Research protocols and managing the process for securing approval from PSU's Institutional Research Board (IRB). More detail is available in our [Research Integrity and Compliance Program](#).
  4. Social Security numbers (SSN), driver's license numbers, and financial account numbers are restricted information and shall not be collected, used, or disclosed unless allowed under a generally applicable University policy (e.g., the Social Security Number Standard). Exceptions or amendments to the applicable University policy must be reviewed and endorsed by the relevant data steward(s) before being submitted by the relevant data steward(s) to the University Privacy Official and University Chief Information Security Officer for final approval.
- **Records of Processing Activities (ROPA)**
    1. The DPO will facilitate the creation of a ROPA for high risk processing activities by department. The DPO maintains a list of departments which require a ROPA to be documented. For more information, contact the DPO.
    2. If you are part of an activity that collects large amounts of PII, collects sensitive PII, or you feel is high risk contact the DPO. The DPO will evaluate the activity/collection and determine if a ROPA is needed.
  - **Data Privacy Impact Assessments (DPIA)**
    1. After creation of a ROPA the DPO may recommend or require a DPIA to be created for high risk processing activities.
    2. The DPO will facilitate the DPIA creation process and may recommend additional controls based on any potential negative impact to data subjects.
  - **Expectation of Privacy on Campus**
    1. PSU respects and values the privacy of its faculty, students and staff, and will not monitor network access, or its community members, without cause except as needed to improve service, safety, or as required by law or as permitted by these exceptions or other university policies:
      - a) [Acceptable Use Policy](#)
        - (1) Access to computers, computing systems, and networks owned by PSU is a privilege which

imposes certain responsibilities and obligations on users. Use of these resources is subject to University policies and regulations, and local, state, and federal laws.

b) University Housing

(1) See the [Housing and Dining Contract](#) for limited circumstances in which student residences may be accessed.

c) Photography and Class Recording

(1) FERPA restricts the sharing of student records information, including student class-activities. To maintain FERPA compliance with classroom recording, it's imperative that any class recordings which include any student activity are shared only with students, TAs, and instructors who are in the same class as the recording. Class recordings may not be reused across classes or sections. Student class activities can include student names, voices, photo or video, and chat activities. Class recording content cannot be shared outside of the class without a FERPA release from all parties. More information on recording is available in the [Conferencing, Web Recording and FERPA](#) documentation published by the Office of Academic Innovation.

○ **Restrictions on Unsolicited Emails**

1. Overview -- The Can-Spam Act applies to not just bulk emails but all commercial communications the "primary purpose of which is the commercial advertisement or promotion of a commercial product or service." If you or your department is sending out bulk emails you must comply with the regulations. The Federal Trade Commission has provided the following list of the main requirements:

- a) Don't use false or misleading information;
- b) Don't use deceptive subject lines;
- c) Identify the message as an ad;
- d) Tell recipients where you are located;
- e) Tell Recipients how to opt out of receiving future email from you;
- f) Honor opt-out request promptly; and
- g) Monitor what others are doing on your behalf.

2. Departments shall use platforms which comply with the [Can-Spam Act](#). For more information and access to university supported email tools, email [ucomm@pdx.edu](mailto:ucomm@pdx.edu).
- **Our Privacy Notice**
    1. [The PSU Privacy Notice](#) serves a variety of important functions, including informing all users of University websites about the processing and disclosure of your information. University websites, including, but not limited to, websites for education, research and service areas, shall have clearly visible links on their websites to our notice.
    2. Depending upon the web page content or users, the PSU Privacy Notice may be amended or supplemented to meet legal or policy requirements associated with the web page content or users. Visitors are advised to review it periodically for any changes. Changes to the privacy notice are effective when they are posted.
    3. When the University permits third parties to use a University-owned domain, they shall ensure that the third party is contractually obligated to have an online privacy statement that complies with all applicable laws and regulations and is reviewed by the Data Protection Officer for consistency with the PSU Privacy Notice.
    4. Please refer to the PSU Privacy Notice for information related to Data Subject Access Requests (DSAR).
  - **Examples of Policy Violations**
    1. Violations of this policy may include but are not limited to:
      - a) A collection or disclosure of information in violation of the [Privacy Notice](#);
      - b) Collecting tax identifiers improperly and without approval;
      - c) Emailing improperly or with the use of an unauthorized platform;
      - d) Failure to disclose a breach to the DPO;
      - e) Collecting more personal identifiable information than is needed for the stated task;
      - f) Using personally identifiable information for a purpose other than the one stated at collection;
      - g) Not securing personally identifiable information; and
      - h) Sharing personally identifiable information with unauthorized individuals or third parties.

2. If you have questions about whether a violation has occurred, or if a process or activity may violate this policy, contact the DPO at [dpo@pdx.edu](mailto:dpo@pdx.edu).
3. Suspected policy violations should be reported to [dpo@pdx.edu](mailto:dpo@pdx.edu).

## **VI. Roles and Responsibilities**

- The CISO and DPO shall be responsible for the implementation and administration of this policy.
- The CISO and the DPO shall, in cooperation with relevant stakeholders, develop and adopt necessary and appropriate Privacy Standards. All relevant stakeholders shall cooperate with the CISO and the DPO in the development and implementation of the Privacy Standards. The Privacy Standards are not required to be made through the process outlined in the Policy on Policies. The CISO and the DPO may, in consultation with relevant stakeholders, add, revise, or modify the Privacy Standards as necessary to incorporate changes to the applicable data privacy laws and regulations or to improve the University's privacy program.
- All members of the PSU Community are responsible for understanding the Privacy Standards and complying with their respective obligations thereunder.
- The DPO will be responsible for monitoring compliance with this policy and should be notified of violations. The DPO is the primary contact for questions regarding this policy or other privacy issues.
- The CISO is responsible for the confidentiality, integrity, and availability of PSU's data and infrastructure and should be notified of any threat to PSU data or infrastructure. The CISO is the primary contact for questions regarding data integrity and other security issues.
- PSU shall establish a Data Governance Advisory Committee to assist with the governance of the University Privacy Program. The DPO will advise and facilitate the governance committee. The CISO will chair the committee and nominate its members.

## **VII. Enforcement**

- Any employee found to have violated this Policy may be subject to disciplinary action, up to and including termination. This action may be taken in accordance with applicable PSU policies and procedures and

- collective bargaining agreements. Additional accountability for the financial penalties and remediation costs associated with a resulting privacy violation may be applicable to the responsible school or department. Any student found to have violated this Policy may be subject to disciplinary action in accordance with applicable PSU policies and procedures, up to and including expulsion from the University. Student employees may be disciplined as an employee and as a student, resulting in both professional and educational consequences. Any vendor, contractor, or affiliate found to have violated this Policy may be subject to disciplinary action, including termination of contract or affiliation. Additional financial liabilities, civil, and/or criminal punishments may be applicable in addition to termination of contract. Violations may also result in network or system access revocation.
- Suspected policy violations should be reported to [dpo@pdx.edu](mailto:dpo@pdx.edu).

## **VIII. Links To Related Policies, Procedures or Information**

[PSU Privacy Notice](#)  
[Information Security Policy](#)  
[Acceptable Use Policy](#)

## **IX. Contacts**

If you have any questions regarding this policy, please contact the Information Security Team at (503) 725-6246 or [help-security@pdx.edu](mailto:help-security@pdx.edu).

If you have any questions regarding this policy, please contact [department name] at 503-725-[main department number] or [department]@pdx.edu.

## **X. History/Revision Dates**

**Adoption Date:** [date policy first approved by UPC and is in effect]

**Reaffirmation Date:** [date UPC concurs with responsible officer that an existing policy requires no change, and remains in effect]

**Revision Date:** [date policy has been changed and reapproved]

**Next Review Date:** Month, Day, Year [at least every five years, sooner as needed]

---

## **XI. Policy Adoption/Reaffirmation/Revision Approvals**

---

### **Approved by Portland State University President**

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

### **Approved by Portland State University General Counsel**

Signature: \_\_\_\_\_ Date: \_\_\_\_\_