

Policy Title: Data Privacy Policy
Policy Owner: Information Technology Services
Effective Date: 10/01/2026
Last Updated: 09/18/2026
Scheduled Review 01/15/2028
Related Policies:
Related Forms:

I. POLICY STATEMENT

Seattle University is committed to protecting the data entrusted to it. This policy reflects the University's commitment to safeguarding Personal Data and Institutional Data against unauthorized access, use, disclosure, alteration, loss, or destruction; promoting compliance with applicable requirements; and reinforcing integrity and accountability across University activities.

This policy addresses both data privacy and data security. Data privacy governs how data is collected, used, disclosed, retained, and disposed of, while data security concerns the safeguards used to protect that data.

The University shall limit the collection, use, disclosure, or storage of Institutional Data to that which reasonably serves the University's academic, research, or administrative functions, or other legally required purposes. Such collection, use, disclosure, and storage shall comply with applicable federal, state, and local laws and regulations, and University policies, guidelines, and standards.

II. PURPOSE & BACKGROUND

Personal Data (see definition, below) and Institutional Data (see definition, below) are vital to Seattle University's mission. Protecting these assets fosters trust, mitigates risk, and promotes excellence in teaching, research, scholarship, artistic creation, and administration. Additionally, Seattle University is dedicated to ensuring compliance with statutory and contractual requirements applicable to the data it collects, stores, or transmits.

III. APPLICABILITY/RESPONSIBILITY

This policy applies to all Personnel, students, contractors, vendors, alumni, visitors, and other individuals who collect, access, use, disclose, retain, dispose of, or otherwise handle Personal Data or Institutional Data on behalf of Seattle University or through University systems. Individuals subject to this policy must handle data in accordance with its assigned classification and applicable University requirements.

IT Services owns and administers this policy and maintains supporting privacy and security standards and safeguards. The Office of University Counsel advises on applicable legal, regulatory, and contractual requirements. The Data Governance Committee oversees institutional data governance and stewardship.

IV. DEFINITIONS

Data Classification: Standards determined by IT Services to describe the sensitivity of data and govern its access. The levels of classification are:

- **High Risk:**
 - Highly sensitive data is data that, if accessed, disclosed, altered, or destroyed without authorization, could reasonably result in significant harm to an individual or the University, including financial loss, identity theft, personal safety risks, legal liability, or reputational damage. Such data is often, but not always, subject to legal,

- contractual, regulatory, or privacy requirements.
 - Examples include student education records protected by FERPA, payment card information, Social Security numbers and other government-issued identifiers, health and biometric information, and research data containing identifiable or sensitive information.
- Moderate Risk:
 - Data that may not be subject to legal, contractual, or regulatory obligations but should be shared only with Seattle University personnel and authorized partners.
 - Examples include internal communications, internal reports, and internal policies and procedures.
 - Moderate-Risk Data, if disclosed inappropriately or altered, could have adverse effects on the University's operations, reputation, or accreditation or compliance requirements.
- Low Risk:
 - Data that is intended for public consumption and does not contain sensitive or confidential information.
 - Low-Risk Data includes general announcements, event information, publicly accessible websites, publicly available reports, press releases, or general information about the university.

Data Privacy: The principles and practices governing how Personal Data and Institutional Data are collected, used, accessed, disclosed, retained, and disposed of in accordance with applicable law and University policy.

Data Security: The administrative, technical, and physical safeguards used to protect data against unauthorized access, use, disclosure, alteration, loss, or destruction.

Data Steward: A designated University official accountable for decisions concerning the access, use, quality, protection, and management of data within an assigned data domain.

Data Use: Accessing, storing, processing, transmitting, or employing data for a legitimate University purpose.

Disclosure: The release, transfer, or provision of access to data to another person or entity, internally or externally; sharing data.

Family Educational Rights and Privacy Act ("FERPA"): A federal law that protects the privacy of student education records.

Institutional Data: Information that documents, describes, or supports University functions, decisions, or operations, including instruction, research, scholarship, administration, financial management, human resources, and governance.

Personal Data: Information that identifies, relates to, describes, or could reasonably be linked to an individual, alone or in combination with other data. Personal Data includes information treated as personally identifiable information (PII), personal information, or a similar term under applicable law. Examples include names, contact information, identification numbers, education records, health information, financial information, location data, online identifiers, and biometric information.

Personnel: Faculty, staff, fellows, student employees when acting within the scope of their University employment, and other individuals performing work for the University. This term does not include contractors or vendors.

V. POLICY REQUIREMENTS

A. Legal, Regulatory, Contractual, and University Requirements

Seattle University's obligations concerning Personal Data and Institutional Data arise from applicable laws and regulations, contractual commitments, and University policies. The requirements that apply depend on the type of data, the individuals involved, and the purpose and location of the data processing. When an applicable legal, regulatory, or contractual requirement is more protective or restrictive than this policy, that requirement will control.

Seattle University will recognize rights concerning Personal Data when provided by applicable law or University policy. Individuals subject to this policy are responsible for complying with the requirements applicable to the data they collect, access, use, disclose, retain, or dispose of and for seeking guidance from the appropriate Data Steward, IT Services, or the Office of University Counsel when uncertain.

B. University Privacy and Stewardship Principles

The University's approach to data privacy and protection is guided by the following principles:

- **Lawfulness and Fairness** – Data shall be collected, processed, and maintained in compliance with applicable laws and university values.
- **Accountability and Governance** – Responsibility for data management is assigned at all levels of the institution.
- **Data Minimization and Purpose Limitation** – Collect, use, and retain only data necessary for legitimate purposes.
- **Integrity and Confidentiality** – Protect data against unauthorized access, alteration, and loss through administrative, technical, and physical safeguards.
- **Transparency and Notice** – Where required by law, inform individuals about how their Personal Data is collected, used, and disclosed.
- **Security by Design and Default** – Integrate privacy and security protections into the design of computing environments, applications, and research projects.
- **Shared Responsibility** – Every member of the University community is accountable for safeguarding Personal and Institutional Data.

C. Data Collection and Use

Seattle University will collect, use, and retain Personal Data and Institutional Data only as reasonably necessary for legitimate academic, research, administrative, or legal purposes. Data must be handled according to its classification and applicable legal, regulatory, contractual, and University requirements. Notice or consent must be provided or obtained when required.

High-Risk Data may be stored or processed only in Seattle University-maintained or contracted computing environments unless approved in advance by the Chief Information Officer.

D. Assessment of Data Privacy and Data Protection

Before implementing a new technology, program, or material change that processes Personal Data or Institutional Data, the individual or University unit responsible for the initiative must conduct a privacy and security assessment proportionate to the sensitivity of the data and the nature of the proposed processing. Initiatives involving High-Risk Data require review and approval in accordance with the Data Privacy and Handling Standard.

- For Low-Risk and Moderate-Risk Data, individuals must conduct their own assessment and attest to the sufficiency of their plans.
- For High-Risk Data, individuals must consult and obtain the approval of the Information

Security Officer and the Chief Information Officer.

E. Institutional Data Governance, Access, and Disclosure

Institutional data governance will include the following.

- Institutional Data must be classified by risk in accordance with the definitions above for High, Moderate, and Low Risk.
- Institutional Data and University records must remain subject to appropriate University governance and stewardship.
- Research data must be managed and shared in accordance with applicable law, University policy, approved research protocols, funding agreements, data-use agreements, and other applicable obligations. External or public sharing must include appropriate safeguards for Personal Data and confidential or restricted information.
- Institutional Data may not be sold, transferred, or disclosed without proper authorization.
- The Data Governance Committee oversees the University's institutional data governance framework. Within that framework, Data Stewards are accountable for access, use, and sharing decisions concerning High-Risk Data within their assigned data domains.
- Access to and sharing of data must be limited to authorized individuals based on job responsibilities and the principle of least privilege. Authorization for High-Risk Data may be granted by role when appropriate.

F. Third-Party and Vendor Management

The following requirements apply when Seattle University shares Personal Data or Institutional Data with a third party or engages a third party to access, process, store, transmit, or otherwise handle such data:

- Contracts with third parties that process Personal Data or Institutional Data must address authorized uses, confidentiality, data security, incident notification, retention, return or deletion of data, and the use of subcontractors.
- Third parties must meet the applicable privacy and security requirements established in the Data Privacy and Handling Standards and their agreements with the University.
- Third parties may process Personal Data or Institutional Data only for purposes expressly authorized by the University. Contracts must prohibit use of University data for advertising, product development, service improvement, model training, or other secondary purposes unless such use has been approved in writing by the Chief Information Officer and the Office of University Counsel.

G. Retention and Disposal

Personal Data and Institutional Data must be retained and disposed of in accordance with applicable law, contractual obligations, University records-retention schedules, and standards established by the appropriate Data Steward. When retention is no longer authorized or required, data must be securely disposed of using University-approved methods.

H. Monitoring, Incident Response, and Reporting

Monitoring of University systems will be conducted in accordance with the Acceptable Technology Use Policy and applicable law.

Suspected or confirmed data incidents, data loss, or unauthorized disclosures, including those

involving lost or stolen devices, must be reported to IT Services immediately and no later than 24 hours after discovery. Lost or stolen physical devices must also be reported to the Department of Public Safety.

I. Implementation Standards and Procedures

IT Services, in coordination with the Data Governance Committee, University Technology Committee, Academic Technology Committee, and Office of University Counsel, will maintain a Data Privacy and Handling Standard that establishes requirements for data classification, collection, use, access, storage, transmission, privacy and security assessments, retention, and secure disposal. All individuals subject to this policy must comply with the applicable requirements of that standard.

J. Exception Process

Exceptions to this policy must be documented, time-limited, and approved by the Chief Information Officer in consultation, as appropriate, with the Information Security Officer, the responsible University leader, the relevant Data Steward, and the Office of University Counsel. Approved exceptions must include reasonable safeguards and may not waive applicable legal, regulatory, or contractual requirements.

VI. VIOLATIONS

Violations of this policy may result in restriction or revocation of access, required training, disciplinary action, or other appropriate measures in accordance with applicable student, faculty, employment, and University policies and established processes. Violations may also result in civil or criminal consequences when provided by law.

VII. RELATED INFORMATION

Item	Description
University Links	Acceptable Technology Use Policy Seattle University Public Safety: Call (206) 296-5990 Seattle University IT Services Information Security: Email infosec@seattleu.edu or call (206) 220-8300 Human Resources Policies Faculty Handbook Code of Student Conduct Law Student Code of Student Conduct Data Privacy and Handling Standards
Forms	Security exception request form
Related Links	
Procedures	