Policy Title:	Acceptable Technology Use Policy
Policy Owner:	Information Technology Services
Effective Date:	*11/02/2026*
Last Updated:	*09/18/2026*
Scheduled Review	*01/15/2028*
Related Policies:	
Related Forms:	

I. POLICY STATEMENT

Seattle University is committed to the safe, responsible, ethical, and lawful use of its information technology (IT) resources. These resources support the University's mission. All members of the University community are expected to use IT resources in a manner that upholds University values, protects Institutional Data, and preserves the confidentiality, integrity, and availability of information systems.

II. PURPOSE & BACKGROUND

Seattle University relies on technology to advance its mission and support teaching, learning, research, scholarship, administration, and community engagement. Because the University's technology environment is shared, the actions of one User can affect the security, privacy, access, and work of others. This policy promotes a safe, secure, and accountable technology environment; protects members of the University community and Institutional Data; and sustains trust in the systems on which the University depends.

The policy establishes expectations for responsible use while supporting academic inquiry, collaboration, innovation, and the appropriate exchange of information. It defines acceptable and prohibited uses of IT Resources and clarifies the shared responsibilities of Users and the University. The policy ensures that University IT resources are used in a manner consistent with institutional goals, legal requirements, and best practices in higher education. It also reinforces accountability, stewardship, and shared responsibility for safeguarding University data and systems.

III. APPLICABILITY/RESPONSIBILITY

This policy applies to all Users of Seattle University's IT Resources, including current and former members of the University community, contractors, vendors, guests, and other individuals who access or use those resources. It applies regardless of location and whether access occurs through University-owned or personally owned devices.

- **All users** must understand and comply with this policy, applicable laws, and related University policies.
- **Supervisors** are responsible for communicating requirements, supporting training, and addressing known noncompliance through established University processes.
- **Information Technology Services** (IT Services) develops, maintains, and enforces this policy, IT security controls, and operational standards.
- The **Chief Information Officer** (CIO) and **Information Security Officer** (ISO) oversee implementation, interpretation, exceptions, and enforcement of this policy.

IV. DEFINITIONS

Acceptable Use: Use of IT Resources for authorized University purposes or permitted Personal Use, in accordance with applicable law, and University policies..

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

IT Resources: Technology resources owned, managed, licensed, provided, or approved by the University, including networks and internet access; computers and mobile devices; software, applications, systems, accounts, and communication services; classroom, laboratory, and virtual computing environments; Institutional Data; and cloud, storage, collaboration, and artificial intelligence services.

Personal Use*:* Limited, incidental use of IT resources for non-commercial, non-University purposes that does not interfere with University operations.

Users*:* Individuals who use University IT resources, whether or not they are authorized to do so.

V. POLICY REQUIREMENTS

A. Acceptable Use

Users must:

- Use IT Resources for authorized University purposes or permitted Personal Use.
- Safeguard Institutional Data in accordance with the Data Privacy Policy and Data Privacy and Handling Standard.
- Access IT Resources only through University-authorized accounts and access mechanisms.
- Access, store, process, and transmit Institutional Data only through University-authorized systems, applications, and services, including cloud and artificial intelligence services.
- Follow copyright, intellectual property, and software licensing laws.
- Promptly report security incidents or suspected violations to IT Services.

Incidental Personal Use is permitted if it:

- Does not interfere with University operations or duties.
- Does not consume excessive resources.
- Complies with other University policies, including the Human Resources Policies and the Conflict of Interest Policy.

B. Unacceptable Use

Users may not use IT Resources in a manner that:

- Violates applicable law, University policy, contractual obligations, or licensing terms.
- Obtains unauthorized access, uses another person's credentials, circumvents security controls, or compromises the security, privacy, or confidentiality of systems, accounts, or data.

- Damages, disrupts, or interferes with IT Resources or University operations, or modifies shared equipment or connects network equipment without authorization.
- Infringes intellectual property rights.
- Constitutes harassment, threats, discrimination, or other conduct prohibited by law or University policy. This does not restrict legitimate teaching, learning, research, scholarship, artistic expression, or other protected activities.
- Supports personal financial gain, unauthorized commercial or external business activities, or political campaign activities, except as permitted by applicable University policies. See also the Policy on Political Campaign Activities, Human Resources Policies, and Conflict of Interest Policy.

C. Privacy and Monitoring

Seattle University respects reasonable privacy interests and supports academic freedom and an open, collegial environment. However, the University cannot guarantee privacy in information created, stored, transmitted, or processed using IT Resources.

The University may access or monitor IT Resources when reasonably necessary for system administration, cybersecurity, continuity of operations, compliance with applicable law or University policy, investigation of suspected misconduct or policy violations, response to emergencies, or other legitimate University purposes. Such access or monitoring will be conducted by authorized personnel, limited to what is reasonably necessary, and consistent with applicable law and University policy.

VI. Account Security

Users must safeguard their accounts and authentication credentials and promptly report suspected loss, disclosure, misuse, or compromise to IT Services. Accounts and authentication credentials may not be shared with or used by another person unless expressly authorized by IT Services. Users are responsible for activities they knowingly conduct or authorize through their accounts.

VII. VIOLATIONS

The University will determine whether conduct violates this Policy based on the requirements of this Policy, related University policies and standards, applicable law, and the relevant circumstances. Users must cease activity determined to violate this Policy when directed by an authorized University official. Depending on the nature and severity of the violation, the University may restrict or revoke access privileges or take other appropriate action. The University may temporarily suspend access while a matter is investigated when reasonably necessary to prevent ongoing misuse, protect IT Resources, or preserve University operations.

Violators are also subject to disciplinary action/sanctions as prescribed in the codes of student conduct applicable to Law and Non-Law students, Human Resources Policies, the Faculty

Handbook, and other applicable documents. Violators also may be subject to criminal prosecution or civil suit under local, state or federal law.

VIII. RELATED INFORMATION

Item	Description
University Links	Conflict of Interest Policy Policy on Political Campaign Activities Copyright Policy Data Privacy Policy Human Resources Policies
Forms	
Related Links	
Procedures	