

Seattle University Information Technology Acceptable Use Policy

Last updated: May 25, 2012

General Principles

Seattle University supports an extensive information-technology environment for faculty, staff, students, and other members of the university community. Our ambition is that information technology is a significant tool that can be used to further the university's mission and strategic priorities.

Acceptable use of information technology is always ethical, reflects academic honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property rights, ownership and confidentiality of information, system security mechanisms, and freedom from intimidation and harassment.

Information technology resources may only be used when their use advances the university's educational, research, and service mission, is necessary for the performance of the duties and obligations of the faculty, staff and students, and complies with all applicable university policies. These duties and obligations generally comprise university work, academic study, research and publication, professional development, and service.

Incidental personal use of university Information Technology resources is, however, permitted when it does not compromise the security of the university's technology infrastructure and is consistent with the acceptable uses described above. Examples of such personal use include personal email correspondence with family and friends, informing oneself about news and current events, and, in the case of campus residents, participation in recreation such as game playing. Should demand for computing resources exceed available capacity, priorities for their use will be established and enforced.

Access to Information Technology resources imposes certain responsibilities and obligations and is granted subject to compliance with university policies, and local, state, and federal laws. Users of Information Technology resources are urged in their own interest to review and understand the contents of this policy.

Scope

This Policy applies to anyone who accesses or uses the university's information technology resources, including without limitation the faculty, staff, students, alumni, and registered guests.

This Policy applies to all information technology and other electronic resources of the university, including:

- All computers, systems, equipment, software, networks, databases and other electronic information resources, and computer facilities owned, managed, or maintained on behalf of

the university for the handling of data, voice, television, telephone, or related signals or information;

- Any access or use of the university's electronic resources, including the university's Internet connection, from a computer, device or other system not controlled or maintained by the university.

Guidelines

Behaviors that are consistent with Acceptable Use include:

- Using technology resources only for authorized purposes in accord with the General Principles outlined above.
- Accessing only information that is your own, is publicly available, or with the permission of the information owner. Each user is expected to know and follow the university's Data Privacy Policy.
- Using only appropriately licensed software, including open source and shareware, in compliance with vendor's/owner's license terms of use.
- Checking your seattleu.edu email account regularly. Many official university communications are sent only via email.
- Conducting university business through appropriate channels. Any business that is confidential should be done through secure technology channels, such as university email. (For a definition of confidential information, please refer to the Seattle University Data Privacy Policy.) Only information appropriate for public dissemination (such as marketing, public communications and announcements) may be done through non-secure channels such as social networks, texting, blogs, messaging services or chat rooms.
- Contacting the University's Chief Information Officer (CIO@SeattleU.edu) or using the confidential EthicsPoint reporting system if you observe or suspect a significant violation of this Acceptable Use Policy. It is available at:
<https://secure.ethicspoint.com/domain/media/en/gui/23241/index.html>.

Behaviors that are inconsistent with Acceptable Use include:

- Using any university technology to engage in behavior or communications that violate the law or university policy, including but not limited to hate speech, threats of violence or harm, obscenity, child pornography or sexual or other forms of impermissible harassment.
- Intentionally engaging in any activity that might be harmful to university systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, damaging files or making unauthorized modifications to university data.
- Using a privileged position at the university (such as a system administrator) to access, alter, remove, or disclose a user's communications or other data without proper authorization.
- Attempting to circumvent or subvert system or network security measures. Examples include:
 - Using another person's User ID and password.
 - Sharing your User ID and password with others.
 - Using a computer program to decode passwords or access control information.
 - Altering, removing, or forging email headers, addresses, or messages, or otherwise impersonating or attempting to pass oneself off as someone else.
- Making or using illegal copies of copyrighted materials (such as software, books, journal

articles, movies or music), storing such copies on university systems, or transmitting them over university networks. Users are expected to know and follow the university's Copyright Policy. It is available here: <http://www.seattleu.edu/policies/copyright.aspx>.

- Conducting university business, especially confidential matters, through inappropriate channels such as texting, instant messaging, and posting to blogs or other social media such as Facebook because they are neither confidential nor secure. Users should be familiar with and follow the university's Social Media Policy, which allows public communication between the University and its stakeholders. It is available here: <http://www.seattleu.edu/marcom/Inner.aspx?id=53083>
- Using any university technology or resources to engage in political activities, except as allowed by the Guidelines for Political Campaign Activities: <http://www.seattleu.edu/policies/>
- Using any university technology or resources for lobbying activities except as approved by the university's Offices of the President, Executive Vice President or Provost.
- Using the university's systems or networks for personal financial gain or benefit, for example, by engaging in a commercial enterprise or selling access to your User ID, university systems, or networks. Faculty may engage in work such as consulting only in accordance with the Faculty Handbook and university policy.
- Overloading networks with excessive data, degrading services, or wasting information technology resources. Information technology is a shared and limited resource. Users should be considerate in their consumption of it. One individual can consume the majority of available WiFi bandwidth in a location (by downloading a hi-def movie, for example) and degrade connection quality for all other users at that location.
- Engaging in other activities that are inconsistent with the General Principles presented above.

Confidentiality and Privacy

According to the university's Data Privacy Policy, information managed by and stored using university technology is 'Confidential' and may be 'High Risk Confidential.' In either case, this requires the university and users to protect its confidentiality. Using university information technology is a privilege, not a right, for the university community. Although the university does not routinely monitor email, data, software, or other online activity of users, it reserves the right to do so to assure acceptable use of its technology and as may be deemed necessary as set forth below.

The university may be compelled by law to gather and/or disclose digital information of its users, such as pursuant to a subpoena, civil discovery hold or request, request of a governmental agency, or court order. If a significant breach of this Acceptable Use Policy is alleged or suspected, user(s) may be asked to cooperate with our investigation. Upon approval of University Counsel and one of the following: President, Executive Vice President, Provost, or CFO; the university may access, monitor, remove, or disclose a user's communications or other data on university systems or personal devices. User(s) are required to cooperate in an investigation. In the event a user fails to cooperate, their user account credentials may be revoked and they may be subject to other action or discipline. See "Enforcement" below.

Electronic communications, software, and other data are backed up for disaster recovery and business continuity reasons. Such back-ups are stored long after they are created or last accessed. Information you delete is still preserved in back-up storage and may be retrieved when deemed necessary, as set forth above. Activity on computers, servers, and networking systems may be logged by administrative software included on such equipment, and these logs may be monitored and reviewed by system administrators or discovered in legal proceedings. These copies, backups, activity logs, and other records may persist after a user's affiliation with the university ends.

Enforcement

Violations of this Acceptable Use Policy will vary in seriousness from accidental to illegal. Where acceptable use comes into question, the university reserves the right to determine what is appropriate and acceptable and what is not. When requested, you are required to cease an activity in violation of this policy. Failure to comply may result in revocation of user account credentials or other action depending on the nature and severity of the offense.

Violators are also subject to disciplinary action as prescribed in the Student Handbook, Human Resources Policy Manual, Faculty Handbook, and other applicable documents. Offenders also may be subject to criminal prosecution or civil suit under laws including, but not limited to the Communications Act of 1934 (as amended), the Computer Fraud and Abuse Act of 1986, The Computer Virus Eradication Act of 1989, Interstate Transportation of Stolen Property, the Electronic Communications Privacy Act, the U.S. Copyright Act, and state and federal child pornography laws.

Information Disclaimer

Individuals using computer systems owned by the university do so subject to applicable laws and university policies. The university disclaims any responsibility and/or warranties for information and materials residing on non-university systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions, or values of the university, its faculty, staff, or students.

Further Information

As technology evolves, questions will arise about how to interpret the general guidelines expressed in this policy. For further information about the University Information Technology policies or protocols, contact the Chief Information Officer by sending an e-mail to: CIO@SeattleU.edu.