Seattle University Policy on the Acceptable Use of Computing Resources

Last Updated: July 7, 2021

Introduction

In support of its mission of education, research and service, Seattle University provides technology hardware, software, computing, networking and other electronic information resources ("Computing Resources") to its community of students, faculty, staff, alumni and registered guests.

Computing 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.

Scope

This Seattle University Policy on the Acceptable Use of Computing Resources (the "Policy) applies to all users who access or use the University's Computing Resources, including faculty, staff, students, alumni, and registered guests.

Rights and Responsibilities

Access to Computing Resources is a privilege and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of the systems and related physical resources, comply with all relevant laws, regulations, and contractual obligations, and use Computing Resources to advance the University's mission of education, research and service.

The right to access data and systems will vary by user type and role. For example, students and employees may have rights of access to information about themselves contained in computer files. Files may be subject to search under court order. In addition, the University may access user files as required to protect the integrity of computer systems.

Examples of Misuse

Examples of misuse of Computing Resources under this Policy include, but are not limited to, the following:

- Using a computer account that you are not authorized to use. Obtaining a password for a generic account without the consent of the account owner.

- Revealing or sharing a user account without authorization.
- Using the Seattle University network to gain unauthorized access to any computer systems.
- Performing an act which will interfere with the normal operation of computers, terminals, peripherals, or networks.
- Running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network. This includes programs known as computer viruses, Trojan horses, and worms.
- Attempting to circumvent data protection schemes or uncover security loopholes.
- Violating terms of applicable software licensing agreements
- Violating copyright laws.
- Wasting Computing Resources.
- Using electronic mail to harass others.
- Masking the identity of an account or machine.
- Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.

Activities will not be considered ‘misuse’ when authorized by the Chief Information Officer for security operations or performance testing.

Examples of Acceptable Use

Examples of acceptable use of Computing Resources under this Policy include, but are not limited to, the following:

- Connecting a gaming console up to dormitory WiFi for recreational use.
- Using Computing Resources only for authorized purposes in accordance with the general principles outlined in this Policy.
- 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 Policy.

Incidental personal use of Computing Resources is permitted when it does not compromise the security of the University's technology infrastructure and is consistent with the acceptable uses described above

If a user's computing usage causes issues, such as using up too much network bandwidth or causes slow-downs, ITS has authorization to terminate the activity, even if the activity is considered acceptable.

Additional Policies

Additional computer and network use policies and terms and conditions may be adopted for specific electronic services provided by the University, along with specific Information Technology standards (e.g. Password Standard) and procedures (e.g. New User Account Request Procedure). Users must comply with all policies, terms, conditions, standards and procedures.

IT Services is responsible for creating and publishing these documents, which are found on the IT Services website (https://www.seattleu.edu/its/). While IT Services will send out notification regarding updates to standards, it is the responsibility of each person to read the standards listed on the IT Services website.

Exceptions

All exceptions to this Policy must be approved in advance. To initiate an exception, contact informationsecurity@seattleu.edu.

Enforcement

Violations of this 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, users are required to cease an activity that is 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.

Minor infractions of this policy or those that appear accidental in nature may be handled informally, with more serious infractions addressed through formal procedures. In some situations, it may be necessary to suspend account privileges to prevent ongoing misuse while the situation is under investigation.

Violators are also subject to disciplinary action as prescribed in the Code of Student Conduct, Human Resources Policy Manual, Faculty Handbook, and other applicable

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

Information Disclaimer

Seattle 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 students, faculty, or staff.

General Information

For clarification of policies and guidelines applying to Seattle University Computing Resources, including this Policy, contact the ITS Service Desk. Policies and Standards are available online at the Seattle University policies and IT Services websites.

Reporting Misuse

Report misuse of computing resources to informationsecurity@seattleu.edu.