



Guidelines for Use of UW Computing and Networking Resources

Included on this page:

- [Summary](#)
- [Appropriate Use Guidelines](#)
 - [Legal](#)
 - [Email](#)
 - [System and Network Integrity](#)
- [Consequences of Illegal or Unethical Actions](#)
- [Enforcement](#)
- [For More Information](#)

Summary

Your use of UW computing and networking resources is governed by:

- Extensive federal and state law and policy
- Internet acceptable use practices
- University of Washington policy
- UW Technology policy

All University of Washington policies regarding the appropriate use of university resources and responsible personal conduct apply to your use of UW computing and networking resources. In addition, your use of UW resources must comply with the restrictions and acceptable practices established specifically for these resources. Faculty/staff use of these systems is subject to Washington state law for employees of state agencies.

Evidence of illegal activities or policy violations will be turned over to the appropriate authorities as soon as possible after detection. Depending upon their nature, violations of law or policy will be met with responses including revocation of access, suspension of accounts, disciplinary actions, and prosecution.

Further, as the computing and networking infrastructure of the University of Washington underlies many crucial activities for the entire University community, including hospitals and clinics, the UW's primary responsibility is to protect and sustain the operation of those facilities. As such, the UW may take whatever steps it feels appropriate to remedy or prevent activities that, in the UW's judgment, endanger the orderly operation of UW networks or systems, and/or which threaten the UW's network connections to the Internet and/or other institutions or networks.

These guidelines are intended as a supplement to the basic [UW policy on ethics in computer use](#) and the University's [software copyright policy](#).

Appropriate Use Guidelines

Guidelines related to the use of UW NetIDs, UW email, and other important University computing resources are described below.

Your UW NetID

For privacy and security reasons:

- You may not share your UW NetID and password with anyone else.
- You may not create a UW NetID for someone else, even if you are their supervisor, parent, or friend.

Legal Guidelines

You must use all UW resources in strict accordance with local, state, and federal laws. These laws cover such areas as illegal access to computer systems, networks, and files; copyright violations; and harassment issues.

The following are prohibited by law and UW policy:

- Copying and/or use of software, images, music, or other intellectual property unless you are certain that you have the right to do so. (See the page on [software copyright policy](#) for more details.)
- Copying of UW software for use on non-UW machines unless explicitly permitted to do so.
- Transmitting to others inappropriate images, sounds, or messages that might reasonably be considered harassing. Harassment is defined as the creation of an intimidating, hostile, or offensive working or educational environment.
- Attempting to break into UW systems, networks, or user accounts.
- Using UW systems or networks as a staging ground for attempts to break into other systems or networks.
- Using UW systems or networks to launch attacks that interfere with or disrupt other systems or networks.
- Using UW computers or networks for personal gain. For example, to sell access to your account or to perform work for profit in a manner not authorized by the university.
- Using UW resources for partisan political purposes, such as using email to circulate advertising for political candidates.

Email Guidelines

UW email is provided as a service to you, as well as to support communication from UW administration. UW administrative email messages will be sent to faculty, staff, students, and affiliates of the UW. Email sent to major groups of UW NetID holders requires the approval of the UW president or vice president.

Your use of UW email should respect others and must not interfere with the operation of the computers and networks. Therefore, you are prohibited from the following:

- Sending email to someone who has requested that you not do so.
- Creating, sending, or forwarding chain letters (messages that are forwarded many times to people who have not solicited the information).
- Flooding another system, network, or user account with email.
- Obscuring the true identity of the sender of email or forging email messages.

It is your responsibility to determine the purpose of an electronic mail list or newsgroup before subscribing or sending messages to the list or group. Persons subscribing to an email list will be viewed as having solicited any material delivered by the list, as long as that material is consistent with the purpose of the list.

The following practices relating to email lists are prohibited:

- Sending to an email list any materials that are not consistent with the purpose of the list. If you send messages not relevant to the purpose of the list, you will be viewed as having sent unsolicited email.
- Continuing to send email to a list if the list owner has requested that you stop sending to the list because you are not following the guidelines or topic established for the list.
- Harvesting email addresses from another email list in order to establish your own list. If a list is closely related to a subject you would like to initiate, it is permissible to post a message to the existing group, inviting people to subscribe to your list.
- Harvesting email addresses from an institution's directory or password file.
- Subscribing anyone to an email list except with the individual's permission.

System and Network Integrity Guidelines

You must respect the integrity of UW systems and networks and other people's systems and networks. You must not access any UW computers or networks nor any computers or networks connected to UW without proper authorization. In no case may you disrupt or harm computers, computer software, computer data or information, or networks regardless of whether the computer, software, data, information, or network in question is owned by the University.

Consider the impact of your action on others, and respect the interests of other computer users and managers.

Report suspected security flaws to *help@u.washington.edu*

The following practices are prohibited:

- Attempting to test security flaws yourself.
- Attempting to disrupt operation of any system or network.
- Altering any data, software, or directories other than your own without proper authorization.
- Probing or connecting to any computers without a legitimate reason to do so.
- Attempting to gain root access on any of the UW systems unless you have been given authorization by the system administrator.
- Using UW systems or networks as a staging ground to crack other systems or networks.
- Installing invasive software, such as worms or viruses, on any UW system over

any network.

Consequences of Illegal or Unethical Actions

Actions that are illegal or against university policy will be referred to the appropriate officials regardless of whether or not a computer was involved in their commission. UW Technology's role is to provide technical assistance to the authorities. Only minor computer and network policy violations will be handled internally by UW Technology.

The UW may monitor user activities and access any files or information in the course of performing normal system and network maintenance or while investigating policy or violations. Anyone using UW resources expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, UW will provide the evidence to law enforcement officials.

Enforcement

If you violate any of the UW computer and network use policies you are subject to loss of access to computing resources as well as to university disciplinary and/or legal action.

If there is evidence of misuse of computing and networking resources through a specific account, the following steps will be taken to protect the systems, networks, and the user community:

1. The suspected UW NetIDs or network ports will be suspended immediately pending the outcome of any investigation.
2. The files and data associated with the UW NetID or computer will be inspected for evidence.
3. The violation will be reported to the appropriate authorities:
 - o UW Technology policy violation to the assistant director for Client Services
 - o University policy violation to Student Affairs, the appropriate instructor, department chair, or supervisor.
 - o Illegal activity to the police, the FBI, the Secret Service, Human Rights, UW and state auditors or the Attorney General's Office.

Violators are subject to any and all of the following:

- Loss of UW NetID (i.e, loss of computing and networking access)
- University disciplinary actions (as prescribed in the "Student Code of Conduct" or "University of Washington Handbook")
- Civil proceedings
- Criminal prosecution

For More Information

Access to the text of applicable laws is available through the UW Law Library.

Examples of improper or excessive use are included in the [Washington State Executive Ethics Board's regulations](#).

If you have any questions or concerns about ethical and legal use of computers and networks, use [Send a question to UW Technology](#).



 [UW Technology](http://uwtechnology.washington.edu)
help@u.washington.edu
Modified: January 25, 2008

 A service provided by
UW Technology