

Authorized Use Policy – Webster University Vienna Campus

Access and use

Access to some University computer systems requires that each user have a unique identity, protected by a password. A computer identity represents the user in various system activities, to provide access to software and data, and to associate the user's own software and data with the identity. As such, this computer identity is a University instrument of identification, and its misuse constitutes forgery or misrepresentation and is subject to University disciplinary action.

In particular:

- No Webster system is to be used for any illegal or criminal purpose.
- Unauthorized attempts to gain root access or access to any account not belonging to the user on any Webster system are prohibited.
- DO NOT share your logon credentials with anyone else.
- Unauthorized access to restricted databases is prohibited.
- Any user who finds a possible security hole on any Webster system is obliged to report it to the system administrators.
- Password sharing is prohibited. Users shall be held responsible for choosing safe passwords, ensuring file protections are set correctly, and for all use of accounts and user-ids assigned to them.
- No food allowed in computer labs. Drinks only allowed in spill proof containers.

Civility and liberty

The University seeks to protect the civil, personal, and property rights of those actually using its computing resources and seeks to protect the confidentiality of University records stored on its computer systems. Conduct which involves use of University computer resources to violate another's rights is subject to University disciplinary action.

As an academic institution, we are committed to supporting the academic freedom of all members of the University community; as a social institution, we are committed to respecting the dignity of all members of our community. The standards and principles of intellectual and academic freedom developed for university libraries apply to material received via computer news networks and by similar means. The standards of intellectual and academic freedom developed for faculty and student publication in traditional media apply to computer-mediated publication.

There will be situations in which what one person understands to be free expression another person takes to be harassment, personal assault, or an assault on prevailing standards of decency. The Report of the Committee on Freedom of Expression at Yale University (January 8, 1975), states:

Shock, hurt, and anger are not consequences to be weighed lightly. No member of a community with a decent respect for others should use, or encourage others to use, slurs and epithets intended to discredit another's race, ethnic group, religion, or sex. It may sometimes be necessary in a university for civility and mutual respect to be superseded by the need to guarantee free expression. The values superseded are nevertheless important, and every member of the university community should consider them in exercising the fundamental right to free expression.

We have considered the opposing argument that behavior which violates these social and ethical considerations should be made subject to formal sanctions, and the argument that such behavior

entitles others to prevent speech they might regard as offensive. Our conviction that the central purpose of the university is to foster the free access of knowledge compels us to reject both of these arguments. They assert a right to prevent free expression. They rest upon the assumption that speech can be suppressed by anyone who deems it false or offensive. . . . They make the majority, or any willful minority, the arbiters of truth for all. If expression may be prevented, censored, or punished, because of its content or because of the motives attributed to those who promote it, then it is no longer free. It will be subordinated to other values that we believe to be of lower priority in a university.

The conclusions that we draw, then, are these: even when some members of the university community fail to meet their social and ethical responsibilities, the paramount obligation of the university is to protect their right to free expression. . . . If a university's overriding commitment to free expression is to be sustained, secondary social and ethical responsibilities must be left to the informal processes of suasion, example, and argument.

Just as nothing in the present policy is to be understood as excusing users of University computing facilities from compliance with federal or state law, nothing in this policy should be understood as withdrawing the University's affirmation of statements in faculty and student policy handbooks in support of academic and intellectual freedom.

None of this, though, denies that harassment on the basis of sex is a violation of Section 703 of Title VII of The Civil Rights Act of 1964 and is also prohibited under Title IX of the Education Amendments of 1972. Webster University's Sexual Offense Policy defines sexual harassment (following Section 703 and the EEOC's 1980 Sex Discrimination Guidelines):

Unwelcome sexual advances, requests for sexual favors, and other verbal or physical contact of a sexual nature constitutes sexual harassment when 1) submission to such conduct is made either explicitly or implicitly a term or a condition of an individual's employment or education or 2) submission to or rejection of such conduct is used as a basis for employment or academic decisions affecting that individual or 3) such conduct has the purpose or effect of unreasonably interfering with an individual's work or academic performance or of creating an intimidating, hostile, or offensive educational or employment environment.

The mere fact of computer-mediation by no means excuses contact that otherwise counts as sexual harassment under the reasonable person standard adopted by the University. Furthermore, users of public terminals or similar facilities at the University should be aware of the public nature of shared facilities and should take care not to display images or play sounds that could create an atmosphere of harassment for others. Similar considerations apply to electronic mail exchanges.

Electronic mail on Webster systems should be as private as the system administrators can make it. Users are prohibited from trying to read the electronic mail of others. System administrators are not to read mail or non-world-readable files unless truly required in the course of their duties. System administrators are to treat mail and non-world-readable files as private at all times. Whenever feasible, systems should be administered so that bounced mail is directed to the system administrators in the form of headers only to protect privacy while ensuring reliable e-mail service.

The University is not responsible for unofficial uses of computer resources. In particular, e-mail and personal Web pages often express private opinions which do not reflect University positions.

Property

Webster University computing and information resources are made available to individuals to assist in the pursuit of educational and other academic goals. It is expected that users will cooperate with each other and respect the ownership of work and information even though it is in electronic--rather than more immediately tangible--form. Individuals and organizations will be held no less accountable for their actions in situations involving computers and information resources than they would be in dealing with other media. Rules prohibiting theft and vandalism apply to software and data as well as to physical equipment.

In particular:

- No Webster system is to be used as a staging ground to crack other systems.
- No one shall alter or delete software, hardware, communications, or data belonging to someone else without authorization.
- Users may not browse, access, copy, or change private files without authorization. Users may not attempt to modify the computer system or software in any unauthorized manner.
- Use of Webster systems for non-Webster purposes, such as running an independent business, or volunteer work for some other organization, absent written authorization, may constitute theft of computer time. Activities by students related to their coursework or to the work of chartered student organizations, and by faculty or staff related to their contractual obligations are explicitly authorized by this policy.
- Users ought to adhere to posted lab and system policies, procedures, or protocols, such as time or storage limits, where those policies, procedures, or protocols are consistent with this policy. Refusal may constitute failure to comply as defined in the Code of Student Conduct.
- The use of invasive software, such as "worms" and "viruses" destructive to computer systems, is unethical and illegal.
- Copyrighted software must only be used in accordance with its license or purchase agreement. Users do not have the right to receive or use unauthorized copies of software, nor to make unauthorized copies for themselves or others.
- Attempting to damage or disrupt operation of computer equipment, data communications equipment, or data communications lines is prohibited.
- Gratuitous consumption of system resources (disk space, CPU time, and bandwidth) will not be tolerated.

Adjudication

This policy establishes no new governance or disciplinary structures. Alleged violations of this policy are to be treated like other allegations of wrongdoing at the University. For example, allegations of misconduct by students should be adjudicated according to established procedures regarding student conduct.

Above policy approved in this form by the Faculty Senate, Webster University, July 18, 1996, and by the Technology Coordinating Committee, August 21, 1996, following previous deliberations by the Senate, as well as deliberations by the Technology Coordinating Committee of the University, it's AUP Subcommittee, and the Faculty Executive Committee (precursor to the Senate). Adopted by the Administrative Council of the University on August 27, 1996.