

Policy on Responsible Use of Union College Computing and Network Resources 6-8-2006

General Statement

As a part of the physical and social learning infrastructure, Union College acquires, develops, and maintains computers, computer systems, and networks. These computing resources are intended for College-related purposes, including direct and indirect support of the College's instruction, research, and service missions; of College administrative functions; of student and campus life activities; and of the free exchange of ideas among members of the College community and between the College community and the wider local, national, and world communities.

The rights of academic freedom and freedom of expression apply to the use of College computing resources. So, too, however, do the responsibilities and limitations associated with those rights. The use of College computing resources, like the use of any other College-provided resource and like any other College-related activity, is subject to the normal requirements of legal and ethical behavior within the Union College community. Thus, legitimate use of a computer, computer system, or network does not extend to whatever is technically possible. Although some limitations are built into computer operating systems and networks, those limitations are not the sole restrictions on what is permissible. Users must abide by all applicable restrictions, whether or not they are built into the operating system or network and whether or not they can be circumvented by technical means.

Applicability

This policy applies to all users of College computing resources, whether affiliated with the College or not, and to all uses of those resources, whether on campus or from remote locations. Additional policies may apply to specific computers, computer systems, or networks provided or operated by specific units of the College or to uses within specific units. Consult the operators or managers of the specific computer, computer system, or network in which you are interested or the management of the unit for further information.

Policy

All users of Union College computing resources must:

Comply with all federal, New York State, and other applicable law; all generally applicable College rules and policies; and all applicable contracts and licenses. Examples of such laws, rules, policies, contracts, and licenses include the laws of libel, privacy, copyright, trademark, obscenity, and child pornography; the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit "hacking", "cracking", and similar activities; the College's Student Conduct Code; the College's harassment and sexual harassment policies; and all applicable software licenses. Users who engage in electronic communications with persons in other states or countries or on other systems or networks should be aware that they may also be subject to the laws of those other states and countries and the rules and policies of those other

systems and networks. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.

Use only those computing resources that they are authorized to use and use them only in the manner and to the extent authorized. Ability to access computing resources does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding. Accounts and passwords may not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned by the College.

Respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected. Again, ability to access other persons' accounts does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding.

Respect the finite capacity of those resources and limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users. The reasonableness of any particular use will be judged in the context of all of the relevant circumstances.

Refrain from using those resources for personal commercial purposes or for personal financial or other gain. Personal use of College computing resources for other purposes is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user's job or other College responsibilities, and is otherwise in compliance with this policy. Further limits may be imposed upon personal use in accordance with normal supervisory procedures.

Refrain from stating or implying that they speak on behalf of the College unless doing so in the performance of legitimate duties on behalf of the College. Affiliation with the College does not, by itself, imply authorization to speak on behalf of the College. The use of suitable disclaimers is encouraged.

Enforcement

Users who violate this policy may be denied access to College computing resources and may be subject to other penalties and disciplinary action, both within and outside of the College. Violations will normally be handled through the College disciplinary procedures applicable to the relevant user. For example, alleged violations by students will normally be investigated, and any penalties or other discipline will normally be imposed, by the Office of the Dean of Students, in accordance with the Student Conduct Code Procedures. However, the College may temporarily suspend or block access to an account, prior to the initiation or completion of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of College or other computing resources or to protect the College from liability. The College may also refer suspected violations of applicable law to appropriate law enforcement agencies.

Security and Privacy

Union College employs various measures to protect the security of its computing resources and of their users' accounts. Users should be aware, however, that the College cannot guarantee such security. Users should therefore engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords, and changing them regularly.

Users should also be aware that their uses of College computing resources are not completely private. While the College does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the College's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, the scanning of systems and network ports for anomalies and vulnerabilities, and other such activities that are necessary for the rendition of service. The College may also specifically monitor the activity and accounts of individual users of College computing resources, including individual login sessions and communications, without notice, when (a) the user has given permission or has voluntarily made them accessible to the public, for example by posting to a publicly-accessible web page or providing publicly-accessible network services; (b) it reasonably appears necessary to do so to protect the integrity, security, or functionality of the College or other computing resources or to protect the College from liability; (c) there is reasonable cause to believe that the user has violated, or is violating, this policy; (d) an account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; or (e) it is otherwise required or permitted by law. Any such individual monitoring, other than that specified in "(a)", required by law, or necessary to respond to perceived emergency situations, must be authorized in advance by the Chief Information Officer or the Chief Information Officer's designees.

Union College, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate College personnel or law enforcement agencies and may use those results in appropriate College disciplinary proceedings.