Policy on Acceptable Use of Information Technology Resources
8-9-2013

The current version of this policy also resides on the ITS website at https://its.union.edu/policies-forms/policies.

General Statement

As a part of the physical and social learning infrastructure, Union College acquires, develops, and maintains computers, computer systems and networks, telecommunications systems and equipment, fax machines, electronic mail (e-mail), Internet access, removable media, servers, storage devices, handheld devices and other electronic equipment or media ("IT Resources"). These IT 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. In general, all computers, the data stored on them, e-mail messages, facsimiles, voicemail and other communications created by and/or stored on the College's IT Resources are the property of the College, which allows the College to access its IT Resources to locate business information, maintain the system and network, comply with legal requirements, and administer this and other College policy. Accordingly, your use of the College's IT Resources is subject to the privacy limitations set forth below (see Security and Privacy). There are some exceptions to this general rule, including but not limited to materials covered by the College's Intellectual Property policy, located in the Faculty Manual, and materials that are specifically licensed and not owned by the College. In the absence of a specific exception covering the equipment you are using or the data you are accessing, storing, or creating on College-owned equipment, the general rule set forth above applies.

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 IT 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 the College's IT Resources 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 IT 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.

All users of Union College IT 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 Policy Against Unlawful Discrimination, Harassment, Bias Activity and Retaliation; and all applicable software licenses. Discrimination, harassment of others, bias activity and/or retaliation, whether on campus, using the College's IT Resources and/or over the Internet, will not be tolerated. Prohibited conduct includes, but is not limited to, the use of anonymous/forged E-mail, "SPAM", port-scanning and other unsolicited messages or activity. 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 IT Resources that they are authorized to use and use them only in the manner and to the extent authorized. Ability to access the College's IT 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. Users will be held responsible for all activity originating from their registered computer. This includes all actions taken by guests using a connection registered under your name.

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. No user may in any way restrict or interfere with other's access to or use of the network. Abuse (intentional or not) of network resources will not be tolerated. This includes any activities considered detrimental to the network or those that cause excessive traffic. 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. IP Addresses may NOT be registered to domain names outside of Union College (example: registering your IP to something like www.company.com).

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 the College's IT 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 the College's IT 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; revision: (c) an account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; or (d) it is otherwise required or permitted by law. The College may also monitor the activity and accounts of individual users, upon notice to the individual user, if there is reasonable cause to believe that the user has violated, or is violating this or any other College policy. Any 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. It is common practice by the Chief Information Officer to relinquish decision-making responsibility regarding monitoring emails to the appropriate Vice President and/or the President.

Use of the College's IT Resources constitutes consent by the user to all of the terms and conditions of this policy, as well as consent to the College's accessing, intercepting, and monitoring of employee use of the College's IT Resources in accordance with this policy.

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.