Responsible Use of College Computing Resources Policy

Lehigh Carbon Community College

Date of Issue: February 2011

This policy and associated materials are reviewed, evaluated, and revised each year, as appropriate.

Portions which relate to compliance with the Higher Education Opportunity Act (HEOA) are assessed annually. Assessment criteria are process-based: the College assesses the plan and materials through comparison to other colleges' plans and through comparison to "best practices" and guidelines suggested by copyright holders.

A. General Statement

As a part of the physical and social learning infrastructure, the College acquires, develops, deploys, and maintains "computing resources" (computers, computer systems, software, applications, computing services, web services, electronic communications, telecommunications, networks, etc.).

These computing resources are intended for College-related purposes, including direct and indirect support of the College's instruction 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, but so do the responsibilities and limitations associated with those rights. The uses of College computing resources, like the use of any other College-provided resource and like any other College-related activity, are subject to the requirements of proper legal and ethical behavior within the 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 systems and networks, those limitations are not the sole restrictions on what is permissible.

Users must abide by all application restrictions, whether or not they are built into the system or network and whether or not they can be circumvented by technical means.

B. Applicability

This policy applies to all users of College computing resources, whether affiliated with the College or not, and to all 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.

C. Policy

Compliance with Applicable Laws, Rules, Policies, Contracts, and Licenses

During use, all users of College computing resources must comply with all federal, state, and other applicable laws; must comply with all applicable College rules and policies; and must comply with all applicable contracts and licenses. Examples of such laws, rules, policies, contracts, and licenses include, but are not limited to, the following:

a) Laws of libel, privacy, copyright, trademark, obscenity, and child pornography
b) The Electronic Communications Privacy Act of 1986 and the Computer Fraud and Abuse Act of 1986, which prohibit activities such as hacking and cracking
c) The College's code of student conduct, presented in *The Rights, Freedoms and Responsibilities of Students*
d) The College's code of employee conduct, presented in the current *Policies and Procedures Manual*
e) The College's sexual harassment policy, presented in conduct codes for both students and employees
f) All applicable software licenses

Compliance with Copyright Laws

- The following statement clarifies how institutions of higher education might comply with HEOA requirements. It summarizes the civil and criminal penalties for violating federal copyright laws, and users of College computing resources are hereby notified of the nature of copyright and the penalties of violating copyright:

> Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.
>
> Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than $750 and not more than $30,000 per work infringed. For "willful" infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys' fees. For details, see Title 17, United States Code, Sections 504, 505.
>
> Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense.
>
> For more information, please see the Web site of the U.S. Copyright Office at www.copyright.gov, especially their FAQ's at www.copyright.gov/help/faq. (Madzelan)

- EDUCAUSE maintains a list of legal alternatives to illegal downloading and file-sharing: "Legal Sources of Online Content." The URI for this resource is <http://www.educause.edu/legalcontent>.

Compliance with Electronic Communications Laws

Furthermore, users are solely responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses. Users who engage in electronic communications with persons locally or 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 local jurisdictions, states, and countries, and subject to the rules and policies of those other systems and networks.

Obtaining Proper Authorization(s) for Use

Users are solely responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding. Users shall use only those computing resources that are authorized for use and use them only in the manner and to the extent authorized. The ability to access computing resources does not, by itself, imply authorization to do so.

Accounts and Passwords

Accounts and passwords are exclusive to individual users and 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 must respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected.

The ability to access other persons' accounts does not, by itself, imply authorization to do so. Users are solely responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding.

Prioritization of Computing Resources Uses

Resources are Finite

Users must 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 activities of other users. Although there is no set bandwidth, disk space, CPU time, or other activity limit applicable to all uses of College computing resources, the College may require users of those resources to limit or refrain from specific uses in accordance with this principle. The reasonableness of any particular use will be judged in the context of all of the relevant circumstances.

Use of College Computing Resources for Personal Gain

Users shall refrain from using College computing 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.

The College's Right to Limit Use

The College reserves the right to implement technologies to manage computing resources such as disk space, network bandwidth utilization, and print privileges as it sees fit to maintain a cost effective, supportable computing environment or if legally required to do so.

D. 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. The College may refer suspected violations of applicable law to appropriate law enforcement agencies.

Students

Violations by students will be handled through the College conduct administration procedures.

Alleged violations by students are reported to the Dean of Student Development. In accordance with *The Rights, Freedoms and Responsibilities of Students*, the Dean will investigate and determine actions to be taken, including any penalties and/or other action. The Dean of Student Development or the student whose conduct is in question may request that the Conduct Board conduct a formal hearing of the reported violation per the process delineated in Articles 4 and 5.

Article 4.5.3 lists actions the College may take, including notice and warning, probation, suspension, dismissal, restitution, and other actions.

College Employees

If the alleged offender is an employee of LCCC, Human Resources will address the situation per the administrative process delineated in the current *Policies and Procedures Manual*.

All Users

If the alleged incident is determined to be of a criminal nature, local or state police will be contacted, regardless of whether the alleged perpetrator is an employee, student, or visitor. For instance, Article 4.2.2 of *The Rights, Freedoms and Responsibilities of Students* acknowledges the college's "legal duty to act in good faith" when it knows about criminal violations: "Should any criminal violations occur on campus or at College-sponsored activities off-campus, the College upon receiving such information has a legal obligation to report these violations to the appropriate law enforcement agency. In addition to being subject to possible criminal prosecution, a student may be subject to actions set forth in 4.5.3."

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 the College or other computing resources or to protect the College from liability or from a violation of law.

E. Security and Privacy

Security

The 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 does not guarantee such security and that all users are solely at their own risk when using the computer resources.

Therefore, users should engage in “safe computing” practices by establishing appropriate access restrictions for their accounts, guarding their passwords, and changing them regularly. All users are required to safeguard their user IDs and passwords for systems they have given access to. Sharing of passwords of any systems (Banner, Bannerweb, e-mail, the ANGEL Learning Management System [LMS], the Portal, etc.) is strictly prohibited.

Privacy

Users should be aware that their uses of College computing resources are not 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 requires the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the rendering of service.

The College retains the right to specifically monitor the activity and accounts of individual users of College computing resources, including individual login sessions and communications, without notice, when at least one of the following conditions has been met:

a) The user has voluntarily made them accessible to the public, as by posting to a web page
b) It reasonably appears necessary to do so to protect the integrity, security, or functionality of College or other computing resources or to protect the College from liability or an alleged violation of law
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
e) It is otherwise required or permitted by law

The College, at 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 as the College solely deems appropriate.

Works Cited

Computer Fraud and Abuse Act of 1986. Pub. L. 99-474. 100 Stat. 1213. 16 Oct. 1986. Print.

Electronic Communications Privacy Act of 1986. Pub. L. 99-508. 100 Stat. 1848. 21 Oct. 1986. Print.

"Legal Sources of Online Content." *EDUCAUSE*. EDUCAUSE. July 2010. Web. 3 November 2010.

Lehigh Carbon Community College. *The Rights, Freedoms and Responsibilities of Students*. Approved by the Lehigh Carbon Community College Board of Trustees on 3 June 2010. *Lehigh Carbon Community College*. Lehigh Carbon Community College, n.d. Web, PDF file. 3 Nov. 2010.

Madzelan, Daniel T. "Dear Colleague Letter" to US institutions participating in Title IV of the Higher Education Act of 1965. DCL ID: GEN-10-08. n.d. *Information for Financial Aid Professionals (IFAP)*. US Department of Education. 4 June 2010. Web. 3 November 2010.

Lehigh Carbon Community College. *Policies and Procedures Manual.* 2010-2011 ed. PDF file.