TITLE: **INFORMATION TECHNOLOGY ACCEPTABLE USAGE POLICY**

DATE(S) OF POLICY AND POLICY REVISION APPROVALS: **February 8, 2011; February 14, 2006**

RESPONSIBILITIES: Users are responsible for their activities while using technology resources and services. By using the College's resources, users agree to abide by all relevant Luzerne County Community College policies and procedures, as well as all federal, state, and local laws. Additionally, each computing facility or service may have specific rules and regulations that govern the use of their systems and users must comply with those rules and regulations. Users are responsible for keeping up to date with this policy and other applicable College technology policies, procedures, and guidelines. Current technology policies are available on the College's web page and from the Information Technology Office.

Access: Use of computing resources may be limited by issues of need, resources, or appropriate use. Access to computing resources is provided to support the daily operations and functions of the College. These activities should relate to the College's educational mission and institutional goals. Some applications may be actively discouraged due to the demand they place on limited resources. Please cooperate with College computing staff if asked to refrain from running applications such as these when resource use is heavy.

Copyright: Luzerne County Community College respects copyright laws and insists that its faculty, staff, and students do likewise. Copying proprietary software is theft and will not be tolerated on campus.
Users should not distribute email document attachments or post information on the College website containing copyrighted material unless evidence exists that the College has the right to copy or distribute such material. Examples of copyrighted materials could include software, database files, documentation, articles, graphic or audio files, or downloaded information.

Electronic Communication, College Network and Internet Usage Guidelines: The College provides a variety of electronic communication and storage channels such as web pages, the Internet, email, voice mail, network folders, messaging, chats, lists and newsgroups for use by students, faculty, and staff. The College encourages the appropriate use of these technologies to enhance its mission and goals. Personal use of email and network storage resources is discouraged. Users should assess the implications of their decision to use College information technology resources for personal use. Data resulting from such personal use may be subject to the archive and record retention requirements of the College. Data is also monitored on a routine basis in order to protect the College from potential problems relating to such things as viruses, storage constraints, and inappropriate content. Users who purposely access sites or distribute electronic messages containing pornographic, lewd, sexually explicit, illegal, or other offensive material may expose the College to liability for sexual harassment or other unlawful discrimination. This includes information that contains sexual implications, racial slurs, gender-specific comments or any comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin, or disability. In addition, intentional access or distribution of such information is not for business purposes and is not necessary for the performance of legitimate job duties and responsibilities. Such use of the Internet is strictly prohibited.

The following set of guidelines define proper and improper use of Luzerne County Community College's Internet services. These guidelines apply to all individuals who use the Internet service (viewing web pages, using Internet e-mail, etc.), or maintaining web pages, through College related systems.
In addition to the guidelines presented below, all other College policies apply to Internet access at Luzerne County Community College. Use of the Internet is a privilege which can be revoked at any time. Any willful violation of this policy may result in suspension of access to the Internet and can result in disciplinary action.

Internet Services - Guidelines:

1. Internet services may not be used for commercial purposes. Selling or advertising services/merchandise by any groups or individuals using College internet resources is not permitted unless pre-written approval is obtained from an appropriate College representative. The only exception to this rule is that the College does allow students and staff to sell personal items on the classifieds section of the student and staff intranet sites.

2. The College's Internet services may not be used to gain, or attempt to gain, unauthorized access to remote computers.
3. Internet access is provided for educational and administrative purposes. Misuse or abuse of Internet access is prohibited.
4. Users may not attempt to uncover or exploit security loopholes in LCCC Internet servers/server software, routers, or other Internet related hardware.
5. Use of Internet services to post or access material of a profane or sexually explicit nature is not permitted.
6. Intentional distribution or acquisition of destructive computer software (for example viruses, etc.) is prohibited.
7. Students may not utilize more than a reasonable amount of space for file storage on the College's Internet servers. If it is determined that a student is utilizing an excessive amount of space, the College reserves the right to limit this space.
8. Unauthorized accessing, monitoring or tampering with another user's electronic communications (files, e-mail messages, etc.), or any attempt to do so, is not permitted. The College reserves the right for the appropriate authorized personnel to access electronic communications for administrative purposes or technical problem resolution.
9. Each user accepts responsibility for his/her use of the Internet. Users should take precautions against the misuse of their account. Selection of a password is an important security issue. Users are advised against selecting a password which may be easily guessed.
10. Luzerne County Community College is the owner of all data stored on all College-owned computers. This includes, but is not limited to, Internet electronic mail and web pages placed on its servers.
11. Backup copies of all data on LCCC Internet servers are created on a regular basis. Luzerne County Community College cannot, however, guarantee data will not be lost in the event of a system failure. Users are advised to keep backup copies of anything placed on the Internet servers.
12. Any activity which violates federal, state, or local laws is not permitted. In addition to the above general guidelines, the following additional guidelines apply to Internet electronic mail and web pages placed on Luzerne County Community College servers.

Guidelines for web pages placed on Luzerne County Community College web servers:
1. All official Luzerne County Community College web pages must adhere to a standard color scheme and layout. This layout and color scheme may be obtained from the Internet system administrator.
2. Luzerne County Community College provides the resources for staff and students to create "Unofficial" web pages (personal home pages, student web pages, etc.) The College, however, does not necessarily endorse these published sites and reserves the right to remove these sites.
3. Web pages may not be used to distribute copyrighted material without the express written consent of the copyright holder. This guideline applies to all copy written material including copy written computer software.
4. Web pages containing material that is offensive, profane, pornographic, or discriminatory are not permitted.

Internet Electronic Mail Guidelines:
1. Every Internet e-mail account is password protected and intended for use by a single individual unless prior approval is obtained. E-mail users should not share accounts or disclose their passwords to others.
2. While all electronic mail is considered private and confidential, Luzerne County Community College reserves the right to access electronic mail for administrative or other purposes.
3. Internet users may not employ a false identity through sending messages, which give the illusion the messages were sent by another party.
4. Electronic mail messages containing material that is offensive, profane, pornographic, or discriminatory are not permitted.

Luzerne County Community College reserves the right to make changes to this policy. The latest version is available on the College's website at http://www.luzerne.edu/internetpolicy.

Security: Owners of technology system accounts are responsible for safeguarding their User IDs and passwords and are responsible for all activity generated from their accounts. Accounts should never be shared with others. Misuse of access rights should be reported to the appropriate department or division supervisor. Users should exercise good password management by always changing an initial password assigned by IT staff immediately upon receipt; changing passwords, where possible, at least every ninety days or when required to do so by the system

being used; and never writing down a password and posting nearby a computer.
Users should create secure, hard-to-guess passwords. Secure passwords are at least eight (8) characters in length; contain a combination of upper and lower-case letters, numbers, and symbols; and do NOT consist of common names or words. Specific procedures to assist users on changing passwords on College systems are available from the office of Information Technology.

Misuse of Technology Resources: The College provides information technology resources for users to engage in activities that support the mission of the institution. Use of the College's resources for personal profit, non-College related fund-raising, or illegal purposes is not acceptable. Non-authorized solicitations on behalf of individuals, groups, or organizations are also prohibited. Examples of misuse include, but are not limited to:

- attempting to defeat or circumvent any security measures, controls, accounts, or record-keeping systems
- using systems for unauthorized access
- intentionally altering, misappropriating, dismantling, disfiguring, disabling, or destroying any computing information and/or services
- using information technology resources in any way or purpose that could cause, either directly or indirectly, excessive strain on computing facilities or cause interference with others' use of information technology resources
- disrupting or attempt to disrupt system operations
- using technology resources or services for workplace violence of any kind.
- using technology resources or services for unlawful purposes including fraudulent, threatening, defamatory, harassing, or obscene communications
- invading the privacy rights of anyone
- disclosing or using non-public information for unauthorized purposes
- disclosing student records in violation of FERPA
- violating copyright law
- using another person's user ID, password, files or data without permission
- removing any college hardware, software, or data without permission

PRIVACY: Users should be aware that although the College takes reasonable measures to protect the security of its information technology resources and accounts assigned to individuals, the College does not guarantee absolute security and privacy. Information stored electronically may be made available in administrative or judicial proceedings. Users communicating data containing personal information or student record information must comply with Family Educational Rights and Privacy Act (FERPA) and the Heath Insurance Portability and Accountability Act (HIPPA) guidelines. All student information must be treated as confidential. Release of information contained in a student's record without the student's consent is a violation of Sec. 438 Public Law 90-247. Any requests for disclosure of student information, especially from outside the College, should be referred to the Registrar's office or Student Development Office.
The College has the ability to access and monitor any electronic data that is stored or transmitted on College systems. The College reserves the right to monitor these College systems at any time and is currently doing so on a regular basis. This is necessary in order to protect the College from potential intrusions, viruses, or disruptive activity.
Information Technology staff have the ability to remote control the majority of personal computers that are owned by the College. This is primarily used for support and/or training purposes. It is an IT Policy that the IT staff member must first alert the end user that they will be connecting to and remote controlling their PC.
Data and files containing sensitive or confidential information should be destroyed securely. Media or documents with sensitive or confidential information should NOT be simply thrown into the trash. "Hard" copies such as paper, microfiche, microfilm, etc. should be shredded. Computer media such as floppies, zip disks, CD-ROMs etc. should be destroyed or reformatted to remove data.
Physical security of Information Technology resources is also very important. Users should always log-off or use some type of workstation lock method such as a password-enabled screen saver when stepping away from their computers for more than a moment. Media such as floppies, zip disks, and CD-ROMs should be stored in a lockable, secure area. Portables such as laptops, PDAs, cell phones, etc. should never be left unattended for any amount of time and should be stored in a lockable, secure area.
In general, the practice is to treat electronic data with as much privacy as possible. However, situations may arise where employees with legitimate business purposes may have the need to view information created by another staff member or monitor user activity on the network. The College will do so when it believes it is appropriate to prevent or correct improper use, satisfy a legal obligation, or insure proper operation of the electronic resources.
The President or his/her designee may authorize access to employee or student email or computer files in a number

of circumstances including, but not limited to:

- situations involving the health or safety of people or property
- possible violations of College codes of conduct, regulations, policies, or laws
- termination of an employee
- other legal responsibilities or obligations of the College
- the need to locate information required for College business

SANCTIONS: Violations of the Acceptable Use Policy are treated like any other violation of College policy. The College reserves the right to discipline a user if it is determined, after an investigation by the appropriate Vice President or the President's designee, that the user violated College policy and/or federal, state or local statutes by misusing technology resources or services. Procedures contained in the faculty, professional, support, and student handbooks will determine disciplinary action, up to and including termination and/or legal action.

The effective implementation of this policy will be assessed on a periodic basis.