CLARION UNIVERSITY

COURAGEOUS. *confident.* CLARION.

Acceptable Use of Technology Resources Policy

Date Effective: May 05, 2010
Issued By: Academic Affairs
Contact: Office of Computing Services, 814-393-2280
Procedure No. 53.002

Purpose:
The purpose of this policy is to establish parameters for the use and operation of Clarion University's computing systems, telecommunications facilities and network resources.

Policy:
The Clarion University computing, telecommunications and networking resources are provided for the support of the instructional, research and administrative activities of the institution. Use of these resources is a privilege granted by the University and it reserves the right to limit, restrict or extend access to these electronic resources.

Users are expected to conduct their activities within the restrictions and overall policies of Clarion University, the laws of the Commonwealth of Pennsylvania and federal statutes. Agreement to abide by this policy is a condition of acceptance to use the University's electronic resources and violators are subject to suspension of computer privileges and possible referral to the appropriate judicial or disciplinary process.

While the university recognizes the role of privacy in an institution of higher learning and every attempt will be made to honor that ideal, there should be no expectation of privacy of information stored on or sent through university-owned information technology, except as required by state or federal law. For example, the university may be required to provide information stored in its information technology resources to someone other than the user as a result of court order, investigatory process, or in response to a request authorized under Pennsylvania's Right-to-Know statute (65 P.S. §67.101 et seq.). Information stored by the university may also be viewed by technical staff working to resolve technical issues.

A. **General Policy:** The use of computer systems, telecommunications facilities, networks or other electronic resources of the institution for the following purposes is deemed unacceptable:

1. Non-University related political or charitable activities;

2. Commercial uses including (but not limited to) the promotion of "for profit" and/or privately owned businesses or sale of private property;

3. To abuse, defame, harass or threaten another individual or group;

4. To commit fraud or distribute any unlawful messages;

5. Excessive use for frivolous, non-productive and/or non-University related purposes, such as (but not limited to) entering chat rooms; and

6. Other unauthorized acts or actions not in accordance with University policies, or not in the best interests of Clarion University.

B. **Protection of Resources and Data:** University data and resources must be protected to ensure the University's ability to meet its educational goals. Therefore, the following actions are prohibited:

1. Theft, damage or destruction of computing facilities, programs or data,

2. Access or use of computing facilities, programs or data that are not authorized to the user's account,

3. Sharing usernames, passwords, pin numbers or any other security related procedures, files or accounts with other individuals, such as faculty, staff or administrators sharing passwords with work study students. This is a serious security breach, especially in light of the enhanced accessibility to privileged data via the iClarion portal and other web based products.

4. Inhibiting or disrupting the operability of computer systems, telecommunications facilities, networks or other electronic resources.

5. Intentionally introducing viruses, Trojan horses, worms or similar programs onto any University systems or networks.

C. **Copying and copyright infringement:** Clarion University of Pennsylvania respects and upholds the rights of holders of copyrights, their agents and representatives. It is the responsibility of employees and students to be aware of the rights of copyright owners. Legal use of copyrighted material can include, but is not limited to, ownership, license or permission, and fair use under the US Copyright Act. Illegal use includes:

1. Reproducing or allowing others to reproduce copyrighted software material in any form without proper authorization, or not in keeping with the University's copyright regulations or federal and state laws,

2. The use of software applications that allow for the direct sharing of music, movies, games, and software over the Internet when such peer-to-peer file sharing contains copyrighted works without the permission of the copyright holder.

D. **Viruses and Security Updates:** Computing Services has implemented automated distribution procedures for virus and security updates to standard, University owned servers, desktop and laptop computers. However, Computing Services does not have the personnel or expertise to support the myriad specialty systems that need to be connected to the network or to support residential students' systems. Therefore, to protect the viability of the University's electronic resources:

1. It is the responsibility of the end user of any specialty electronic system that utilizes a computer based operating system, such as a copier, document imaging system or ITV system, to ensure that virus protection and security updates are provided by their maintenance contractors.

2. It is the responsibility of residence hall students to install all security patches and to maintain up-to-date anti-virus software on their systems, if they are connected to the residence hall network or to CNet via wireless. If students do not maintain their systems properly and adversely affect the University's system(s), they will be disconnected from the network and may be subject to a reconnect fee.

E. **Email Communication:** The Clarion University email system is considered an official means of communication and all students and employees are responsible for information sent to them via their Clarion account. All students, employees and retirees are given a Clarion University email account. With respect to those email accounts:

1. It is the responsibility of the email account owner to delete unwanted messages and attachments, and to otherwise maintain their account.

2. Email can easily be forwarded to non-University accounts by the account owner; however, the account owner is responsible for the receipt of all information, including attachments, forwarded to another account.

3. It is expected that students and employees will check their Clarion email accounts and the iClarion portal on a frequent and consistent basis.

4. Faculty should expect that students are accessing official electronic communications for the purposes of coursework.

In addition to the iClarion portal, the University maintains mass email distribution capabilities to facilitate communication within the University community. These consist of the ALL-L listserv, the ANNOUNCE email distribution list, and their student equivalents, S_ALL-L and S_ANNOUNCE. Students and employees have the ability to sign off of the ALL-L lists; however, no one can remove themselves from the ANNOUNCE email distribution lists.

Messages sent via the two ALL-L listservs should contain information relevant to the University community such as student support services, event announcements and cancellations, or the availability of excess supplies or furniture. All employees subscribed to ALL-L have the ability to send messages to ALL-L; however, the ability to send messages to S_ALL-L is restricted to specific individuals.

Messages sent via the two ANNOUNCE email distribution lists contain important information that must be seen by all employees or students, i.e., official dates or deadlines, emergency situations, computer or building shutdowns, or critical health announcements. The ability to send messages via ANNOUNCE is restricted to specific individuals.

F. **Data Communication:** The physical data communication system (CNet) at Clarion University provides switched 10Mb or 10/100Mb Ethernet service to all computers and other network devices. All connections to this system are provided through standard RJ-45 outlets that connect to network equipment using standard Category 5, 5E, or 6 cabling. Any entity wishing to utilize the communication system must do so through the provided connections and must obtain permission from Computing Services. If other cabling or communication systems are required then the entity may install additional wiring, subject to approval by Computing Services. In this case, the entity will be responsible for the installation and maintenance of their installed communication system.