821

ACCEPTABLE USE OF CLIU ELECTRONIC EQUIPMENT POLICY

NOVEMBER 18, 2013

821 ACCEPTABLE USE OF CLIU ELECTRONIC EQUIPMENT POLICY

A. PURPOSE

1. To provide acceptable access and uses of the Carbon Lehigh Intermediate Unit's ("CLIU") computer hardware, network systems, computer software, or electronic equipment.

B. AUTHORITY

1. The Board directs the Management Information Systems ("MIS") Department to provide and maintain CLIU electronic equipment, computer hardware, software, and/or network that facilitate CLIU business.

2. The Board directs the Executive Director and/or his/her designee to implement, carryout, and enforce all provisions of this policy.

C. DEFINITIONS

1. **Electronic Equipment and Computer Hardware** includes but is not limited to servers, personal computers, printers, scanners, routers, hubs, storage media tape drives, flash drives, floppy diskettes, diskettes, hard drives, modems, network cards, laptops, cell phones, tablets, and all hardware accessories.

2. **Computer Software** includes but is not limited to all software applications, operating systems, network operating systems, and all backup utility software, e-mail, web-sites, firewall, and all software applications purchased and/or authorized for use on CLIU hardware and/or network. **Network** includes but is not limited to CLIU Network, Protocol, IP, IPX, SPX, TCP/IP, NT, UNIX, firewall network licenses, Internet, private public domain, e-mail, web-site, and all network browsers.

3. **Authorized Software** is a software application that has been submitted to and reviewed by the MIS department and deemed to be compatible with current systems and authorized by MIS to be installed, copied, downloaded, loaded, or ran on CLIU electronic equipment, computer hardware, and/or network.

821

ACCEPTABLE USE OF CLIU ELECTRONIC EQUIPMENT POLICY

NOVEMBER 18, 2013

D. ACCESS TO CLIU ELECTRONIC EQUIPMENT, COMPUTER HARDWARE, SOFTWARE, AND/OR NETWORK

1. Access to and/or use of CLIU electronic equipment, computer hardware, software, and/or network is a privilege granted solely to Employees who receive an authorized account or individuals who are provided permission by MIS Department.

2. The CLIU reserves the right to disable, revoke, and/or remove user accounts and/or privileges permanently or temporarily.

E. ACCEPTABLE USE

1. Employees will choose a password to use when accessing the network. The password will be reported to the MIS department. The password is not private and is the property of the CLIU.

2. An Employee who is provided an authorized account or other individual given permission by a CLIU Administrator is granted access to utilize CLIU electronic equipment, computer hardware, software, and/or network for official CLIU business. The Employee or Authorized User's utilization is acceptable as long as it:

   a. Is performed in a professional and ethical manner as deemed by the CLIU in its absolute discretion;
   b. Does not violate state or federal law;
   c. Does not violate Board Policy;
   d. Does not result in personal use involving significant use of CLIU resources, direct costs, or any interference with the performance of CLIU duties, work, responsibilities, or data communication networks as deemed by the CLIU;
   e. Does not result in commercial gain, private profit, or local market competition with the CLIU (This includes but is not limited to chain letters, solicitation of business or services, sales of personal property, etc.);
   f. Does not result in offering or providing goods or services or purchasing goods or services for personal use;
   g. Does not result in political lobbying, as defined by the state statute covering political lobbying (CLIU Employees may use the system to communicate with their elected representatives and to express their opinion on political issues.);
   h. Does not result in the sharing of confidential information about students, patients, clients, CLIU staff, and/or CLIU business;
   i. Does not result in the accessing, creating, displaying, uploading, downloading, copying, sending, storing, transmitting or distributing pornographic, obscene, sexually explicit, abusive, harassing, lewd, offensive or threatening language, images, and/or other materials.
   j. Does not result in annoying or harassing another;

k. Does not result in using another's individual's account or identity;
l. Does not result in allowing an unauthorized individual to use an assigned account;
m. Does not result in damage to or destruction of computer hardware or software;
n. Does not result in copying of software in violation of commercial law;
o. Does not result in spreading computer viruses;
p. Does not result in the copying of CLIU forms, policies, guidelines for personal use, personal gain, or commercial use;
q. Does not result in downloading, loading, installing, copying, running unauthorized software on CLIU hardware and/or network; and/or
r. Does not result in activity that the CLIU determines in its absolute discretion to be unacceptable or inappropriate.

F. STATUS OF CLIU ELECTRONIC EQUIPMENT, COMPUTER HARDWARE, SOFTWARE, AND/OR NETWORK

1. CLIU electronic equipment, computer hardware, software, and/or network and the files, communications, data, images, material, literature, and/or information accessed, created, displayed, saved, sent, received, downloaded, uploaded, copied, stored, distributed, and/or transmitted using the CLIU electronic equipment, computer hardware, software and/or network are the property of the CLIU and are not to be considered private. Employees have no property interest or expectation of privacy when accessing or utilizing CLIU electronic equipment, computer hardware, software, and/or network.

G. USER RESPONSIBILITIES

1. A user, an Employee or authorized individual as defined above, must report the loss or theft of any CLIU electronic devices and/or equipment immediately to an administrator.

2. Users, an Employee or authorized individual as defined above, must keep electronic equipment in a physically secure location such as not in open view in a vehicle or unattended in public location.

H. CONSEQUENCES OF VIOLATION OF POLICY

1. CLIU reserves the right to view and monitor all applications, files, communications, messages, data, images, material, literature, and/or information that is maintained on CLIU electronic equipment, computer hardware, software, and/or network to ascertain compliance with acceptable use policies. The MIS Department may delete files deemed to be beyond managerial storage levels.

2. Use of CLIU electronic equipment, computer hardware, software, and/or network for anything other than the permissible use stated in this policy whether through ignorance, negligence, or deliberate disregard, may result in the disciplinary action up to and including termination. In addition, illegal use of CLIU electronic equipment, computer hardware, software, and/or network will be reported to the appropriate legal authorities.