Use of Computing Resources

This section does not cover every situation involving the proper or improper use of college computing resources; however, it does set forth some of the responsibilities that a person
accepts if he or she chooses to use those resources. The purpose of this section is to establish rules for the benefit of all users and encourage responsible use of computing resources.

The computer resources at Orangeburg-Calhoun Technical College are primarily to be used to support and further the academic pursuits of its students. Any use of the computing resources for personal gain or to conduct a private or personal business is strictly prohibited, except for scholarly pursuits such as faculty publishing activities or students applying for financial aid. The following section will outline some of the other potential misuses of the computing system that are prohibited.

A. Authorized Use
    1. No one shall
        a. connect with or otherwise use any college computer, network, or other computing resource without proper authorization
        b. assist in, encourage, or conceal any unauthorized use, or attempted unauthorized use, of any college computer, network, or other computing resource; or
        c. misrepresent his or her identity or relationship to the college to obtain access to computing resources.
    2. Users shall use only those computing and network resources that have been authorized for their use and must identify computing work with their own names or an approved means of identification so that responsibility for the work can be determined and users contacted, if necessary.
    3. Users shall not install any software on any college computer without authorization from Information Technology Services or authority from other controlling entities. This includes but is not limited to shareware and/or freeware.
B. User Accounts
    1. Users shall not subvert restrictions associated with their accounts, such as quotas and levels of access.
    2. Users should follow the procedures for accessing college computing systems as outlined in this document.
    3. No one shall give any password for any college computer or network to any unauthorized person, nor obtain any other person's password by any unauthorized means. Users are responsible for the use of their computer accounts and shall not allow others access to their accounts, through sharing passwords or otherwise. Users should take advantage of system-provided protection measures to prevent such access.
    4. When a user ceases being a member of the campus community within the college (i.e. no longer is a student or employee), his or her account and access authorization shall be terminated. A user shall not use facilities, accounts, access codes, privileges, or information for which he or she is not authorized.
C. Security and Other Related Matters
    1. No one shall
        1. knowingly endanger or compromise the security of any college
            a. computer, network facility, or other computing resource or willfully interfere with others' authorized computer usage
            b. attempt to circumvent data protection schemes, uncover security loopholes,or decrypt secure data
            c. modify or reconfigure or attempt to modify or reconfigure any software or hardware of any college computer or network facility in any way, unless specific authorization has been obtained

d. use college computer resources and communication facilities to attempt unauthorized access to or use of any computer or network facility, no matter where located, or to interfere with others' legitimate use of any such computing resource. This includes the use of network sniffing and discovery tools.

2. No one shall attempt to access, copy, or destroy programs or files that belong to other users or to the college without prior authorization, nor shall anyone use college computing resources for unauthorized monitoring of electronic communications.
3. No one shall create, run, install, or knowingly distribute a computer virus, Trojan Horse, Worm, or other surreptitiously destructive program, e-mail, or data via any college computer or network facility, regardless of whether demonstrable harm results.
4. Users shall not place confidential information in computers without protecting it appropriately. The college cannot guarantee the privacy of computer files, e-mail, or other information stored or transmitted by computer; moreover, the college may access such information. Persons who have access to confidential or sensitive information shall disclose it only to the extent authorized by the Family Educational Rights & Privacy Act, the South Carolina Freedom of Information Act, and other applicable laws, and only in connection with official college business.
5. Users shall not knowingly or recklessly perform any act that will interfere with the normal operation of computers, terminals, peripherals, or networks and shall not intentionally waste or overload computing resources.

D. Intellectual Property
1. No one shall copy, install, use, download, view, or distribute through college computing resources any photographs, logos, images, graphics, graphic elements,
audio, video, software, html markup, data files, or other information in violation of U.S. copyright, trademark, patent laws, federal or state laws (Higher Education
Opportunity Act (HEOA), or applicable licensing agreements, or college policy (OCtech Policy # 3.010.01). It is the user's responsibility to become familiar with the terms and requirements of any such laws or agreements. This subsection does not apply to any material that is in the public domain.
2. Illegal file sharing is often accomplished using Peer-to-Peer (P2P) software like KaZaA, Gnutella, Napster, BitTorrent, etc. P2P files sharing software is not allowed on college owned computers and bandwidth for these applications on the college network will be minimized. Most copyright infringement involves music and movie files. Alternatives exist today to provide users with easy and inexpensive ways to purchase, listen to or watch without violating copyright. These include: Apple iTunes, Amazon Music Store, Google Music, Pandora, Youtube, Netflix. The college may minimize or cap bandwidth for movie and music services to provide sufficient resources for it’s educational mission.

E. Communications
1. Users assume full responsibility for messages that they transmit through college computers and network facilities.
2. No one shall use the college's computing resources to transmit fraudulent, defamatory, or obscene messages, or any material prohibited by law.
3. No one shall use the college's computing and network resources to:
   a. annoy, harass, threaten, intimidate, terrify, or offend another person by conveying offensive language or images or threats of bodily harm to the recipient or the recipient's immediate family
   b. repeatedly contact another person to annoy or harass, whether or not any actual message is communicated, and the recipient has expressed a desire for the contact to cease;
   c. repeatedly contact another person regarding a matter for which one does not have a legal right to communicate (such as debt collection), once the recipient has provided reasonable notice that he or she desires such contact to cease
   d. disrupt or damage the academic, research, administrative, or related pursuits of another person; or
   e. invade the privacy, academic or otherwise, of another person or threaten such an invasion.
4. Users shall comply with this code as well as the regulations and policies of newsgroups, lists, and other public forums through which they disseminate messages.

5. Users shall not
    a. initiate or propagate electronic chain letters
    b. engage in spamming or other indiscriminate mass mailings to newsgroups, mailing lists, or individuals
    c. forge communications to make them appear to originate from another person, e.g., spoofing or phishing; or
    d. engage in resource-intensive activities unrelated to college functions, e.g., multi-user dungeon ("MUD") activities, online gaming, IRCing, accessing
    Adult Chat sites, or extended use of online audio and/or video programs and chat sessions not related to academic pursuits.
6. Users shall conduct all communications in an ethical way and comply with the Internet and computing standards of etiquette.

F. Priorities for Computer Lab Usage
1. In college libraries and general-access computer labs, or in any other environment in which users must share computing resources, priority shall be given to users engaged in activities directly related to the college's mission, e.g., completing course assignments or engaging in research.
2. Each departmental area that maintains computer labs may adopt policies to regulate the use of online chatting or instant messaging, gaming, or recreational
use.
3. Printer use is restricted to academic or departmental purposes only.

G. Pornography
The viewing, printing, or distribution of pornographic or obscene images is prohibited to all users of the college computing system. Images, graphics, and
language associated with the Arts and medical disciplines are excluded.

Enforcement and Sanctions

A. System administrators are responsible for protecting the system and users from abuses of this code. Pursuant to this duty, system administrators may
1. formally or informally discuss the matter with the offending party
2. temporarily revoke or modify access privileges
3. refer the matter to the appropriate disciplinary authority.

B. Any violation of this code may result in the revocation or suspension of access privileges. Imposition of such a sanction is within the discretion of the Information Technology Department or the appropriate academic or administrative unit.

C. Any offense that violates local, state, or federal laws may result in the immediate loss of all college computing and network privileges, may cause student or employee to be placed on disciplinary probation, suspended or expelled, and may be referred to the appropriate law enforcement agencies.