| Policy Title: | General Usage- Networking and Computing |
|---|---|
| Policy Number: | UNIV-450 |
| Revision Date: | February 2023 |
| Policies Superseded: | FINA-602 |
| Policy Management Area(s): | Information Technology Services |

## SUMMARY:

It is the mission of Information Technology Services (ITS) at Coastal Carolina University to provide emerging, reliable, and cost-effective technology resources and services to enhance student learning and improve teaching, as well as to augment the research and administrative functions of the University. Coastal Carolina University maintains policies for the use and security of its information technology resources to ensure that all use of Coastal Carolina University's information technology resources support the University's mission as a public comprehensive liberal arts institution.

ITS is responsible for securing the University's network and computing systems in a reasonable and economically feasible manner against unauthorized access and/or abuse, while making information technology resources accessible for authorized and legitimate users. Information technology resources are defined as computer systems, networks, and data and information resources including software, data, files, and all associated content regardless of the form or the location, as well as computers, devices and telephones. These policies apply to all electronic records of the University, regardless of their form or location. All users of University information technology resources are required to adhere to these policies.

## POLICY:

I. GENERAL COMPUTING POLICY

A. All computer systems that are the property of Coastal Carolina University and/or the state of South Carolina should be used only for University-related business.

B. Any unauthorized, deliberate action that violates posted policy, damages or disrupts a computing system, alters its normal performance, or causes it to malfunction is prohibited, regardless of system location or time duration.

C. Only software approved/relevant to the user's University-related duties should be installed on a computer system. A list of ITS-supported/approved software is available on the ITS website.

D. The copying or sharing of copyrighted materials, software, video and audio files (including MPEG files) without the express written permission of the owner or the proper licensing authority is prohibited.

E. Due to the increased risk of electronically transmitted viruses, it is suggested that software upgrades, installation files and other executable files (.exe files) should only be downloaded and installed from the internet after consultation with ITS staff.

F. Students must have antivirus software on their computers and must update their antivirus program definitions regularly.

G. Unless advised otherwise, students must update their operating system regularly to ensure system integrity and security.

H. The use of University technology resources (e.g., computers, computer systems, facilities and/or services) for commercial purposes is prohibited.

I. The installation of University wired and/or wireless routers, bridges and similar equipment without the expressed consent of ITS is prohibited.

## II. NETWORK ACCOUNTS AND SECURITY

A. Once a user receives an ID to access network and computer systems, the user is responsible for all actions taken while using that ID. Because users of the network may be allowed to access other networks (and/or the computer systems attached to those networks):

1. Applying for a user ID under false pretenses is prohibited.
2. Sharing user credentials with any other person is prohibited. If someone else uses your user credentials, you will be responsible for the actions that other person performed. Sharing of user credentials may result in the loss of all University computer accounts.
3. Using your computer as a server on the network (or any directory or file on your computer) is prohibited unless access is password-protected. Any files considered public should be copied to an appropriate directory that is accessible from the network.
4. Deletion, examination, copying, or modification of files and/or data belonging to other users without their prior consent is prohibited.
5. Attempts to evade or change resource quotas are prohibited.

6. Continued impedance of other users through mass consumption of system resources/bandwidth, after receipt of a request to cease such activity, is prohibited.
7. Use of systems and/or networks to gain unauthorized access to remote systems is prohibited.
8. Use of systems and/or networks to connect to other systems, in evasion of the physical limitations of the remote/local system, is prohibited.
9. Use of systems and/or networks to copy or share copyrighted materials, software, audio and video files (including MPEG files) is prohibited.
10. Decryption of system or user passwords is prohibited.
11. The copying and/or modification of system files is prohibited.
12. Any intentional attempt to "crash" network systems or programs is prohibited.
13. Any attempt to secure a higher level of privilege on network systems is prohibited.
14. The willful introduction of computer "viruses" or other disruptive or destructive programs into University or external networks is prohibited.
15. Any attempt to intercept and/or monitor network traffic is prohibited.

## III. ELECTRONIC MAIL (EMAIL)

A. The use of email on the University network system is contingent upon the following:

1. The email system is University property and should be used primarily for University-related purposes.
2. The University reserves the right to monitor email and internet usage.
3. FERPA applies to University email and its use.
    a. The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. (To learn more about FERPA, visit https://studentprivacy.ed.gov/)
    b. If you are sending an email that includes FERPA-protected information (see https://studentprivacy.ed.gov/ferpa#0.1_se34.1.99_12 for definitions of FERPA-protected information) to a student or to approved parties, encrypt the email before sending (see https://www.coastal.edu/its/security/encryption/).
    c. For students and parents, please also refer to the CCU Registrar's Family Educational Rights and Privacy Act (FERPA) page for additional support and information.
4. There are no privacy rights in the creation, sending or receipt of email.
5. In response to system restrictions and space limitations, pictures, graphics, movies or any other email file attachments in the system without a valid business reason should be kept to a minimum.

6. Whenever electronic mail is sent, the sender's name and user ID are included in each message. The sender is responsible for all electronic mail originating from their user ID. Therefore:
    a. Forgery (or attempted forgery) of email messages is prohibited.
    b. Attempts to read, delete, copy or modify the email of other users are prohibited.
    c. Attempts to send harassing, obscene or threatening email to another user are prohibited.
    d. Attempts to send junk mail, "for-profit" or chain email are prohibited.

## IV. WIRELESS TECHNOLOGY

A. ITS is responsible for managing the technology infrastructure of the Coastal Carolina University Data Network, including wireless network access.
   1. Wireless access points (WAPs) intended for colleges, departments or divisions of the University must be approved and registered in ITS prior to installation. Unapproved WAPs will not be allowed to connect to the campus network.
   2. The installation of non-University wireless access points (WAPs), routers, bridges and similar equipment without prior consent from ITS is prohibited.

## V. NEW AND EMERGING TECHNOLOGIES

New and emerging technologies are to be approved in advance by the appropriate departmental official, the University Technology Council (if applicable) and ITS prior to installation or use on University resources. To ensure data integrity/security, efficiency, effectiveness, compatibility with University systems, the non-redundancy of system resources and the strategic alignment of the University mission, while also meeting the technology needs of the University, technology adoption should follow the appropriate channels and the IT governance structure.

## VI. SOCIAL MEDIA

See UNIV-408 Social Media.

## VII. HARDWARE SANITATION

The South Carolina Division of Technology Operations mandates that all equipment (e.g., computers, copy machines and electronic media) that may contain intellectual property or personal information must be sanitized prior to transfer for other uses or for disposal. Departments should consult with ITS prior to disposing of any computer equipment.

## VIII. KIMBEL LIBRARY COMPUTER USE

A. All sections above apply to computer usage in Kimbel Library.

B. Coastal Carolina University students, faculty, and staff wishing to use these computers for research purposes will be given preference over all other users. The Kimbel Library reserves the right to limit the amount of time an individual user can devote to a single session. A one (1) hour time limit is in effect for users not affiliated with Coastal Carolina University.

C. Access by minors: Full internet access is available in Kimbel Library via its public access computers. Parents or legal guardians of those under age 18 must assume responsibility for deciding what library resources and websites are appropriate for their children and are encouraged to guide their children in the use of the internet and inform them about materials they should not use. Kimbel Library does not monitor or control information accessible through the internet and is not responsible for its content, for changes in content of the sources to which the library home pages link, or the content of sources accessed through secondary links.

D. Accessing websites displaying information or material in violation of state or federal law, or sites that create a “hostile environment” for other users of the library is prohibited.

## IX. VIOLATIONS OF THIS POLICY

A. Users of the University network and systems are responsible for respecting and adhering to local, state, federal and international laws. Users who violate any such laws may be subject to prosecution and/or litigation. The University will fully comply with any complainants to provide any information necessary for prosecution and/or litigation. Activities on the University network may be recorded and may be turned over to the appropriate legal authority.

B. Deliberate attempts to violate the provisions of this policy may result in immediate disciplinary action, regardless of the success or failure of the attempts. The disciplinary action may include permanent loss of all computer accounts, suspension (for students), dismissal (for employees), and/or legal prosecution. Disciplinary action may be administered by University police (consistent with University policies) and/or the FBI.