

Cookeville Higher Education Campus urges everyone in its community to abide by the computer acceptable use policy and comply with copyright law. Copying or sharing music or other copyrighted material, including software, without a permissible copyright defense, such as Fair Use, or a valid license, is not only a violation of the college's and the Tennessee Board of Regent's policies, it is illegal. It may have dire personal consequences and jeopardize the individual's continued enrollment or continued employment, as well as future job prospects.

### [Acceptable Use Policy](#)

**STANDARD:** This document represents the Cookeville Higher Education Campus's (CHEC) policy for the acceptable use of computers and networks that are made available to faculty, staff, and students. The act of accessing your computer account represents your acceptance of the following policy (see TBR Policy 1:08:00:00).

#### **PROCEDURES:**

- The computers, the Tennessee state network (NetTN), and the Internet are available for use, at the discretion of CHEC, by all faculty, staff, and students affiliated with the Campus. CHEC reserves the right to deny access to any individual as it deems appropriate. The purpose of providing access to the computers, NetTN, and the Internet is to support the primary functions of CHEC, i.e. instruction, research, public service, and the accompanying administrative support functions, by facilitating the exchange of information consistent with the purposes of the cooperating institutions that make up NetTN and the Internet.
- Users should be aware that NetTN and the Internet are not secure networks. Information that is transmitted over these networks is not encrypted or made private between the sender and the addressee.
- Guidelines for use of these resources (the computers, NetTN, and the Internet) are as follows:
- a. Individual usage of information technology resources should be consistent with the goals and purposes of these resources.
  - b. These resources should not be used for any activity that does not support the mission and purposes of CHEC. If a particular usage is not in the best interest of the Campus or if it does not support the mission and purposes, then it should not be done.
  - c. Users shall obtain proper authorization before using CHEC information technology resources.
  - d. User access to information technology resources is granted to an individual by the college solely for the grantee's own use. User access privileges must not be transferred or shared, except as expressly authorized by an appropriate official of the college.
  - e. Users should be professional and respectful when using electronic media to communicate with others; the use of college resources to libel, slander, or harass any other person is not allowed and could lead to college discipline as well as legal action by those who are the recipient of these actions.
  - f. Material published on the CHEC site is protected by the Digital Millennium Copyright Act. Any questions pertaining to copyright infringement should be directed to the CHEC Executive Director.
  - g. Unauthorized peer-to-peer file sharing (of music, movies, etc) and/or copyright infringement is strictly prohibited and subject to civil and criminal penalties.
  - h. Campus IT resources must not be used to attempt unauthorized access to private information maintained by users or the college itself.
  - i. Computer and network resources should not be used for commercial purposes.
  - j. Users must not engage in any behavior or activity that unreasonably interferes with the access privileges of other users or with the college's ability to provide access to these resources for its entire community of users.
  - k. Users shall not use CHEC information technology resources for solicitation for religious or political causes.
  - l. These resources should not be used for any unlawful purposes.
  - m. Attempts to penetrate a remote site without proper authorization ("hacking") are strictly forbidden and also violate the Tennessee Code Annotated, which states suitable punishment for violators.
  - n. User shall not intentionally introduce any program or data intended to disrupt normal operations (e.g. a computer "virus" or "worm") into any CHEC information technology resource.
  - o. Forgery or attempted forgery of e-mail messages is prohibited.
  - p. Sending or attempts to send unsolicited junk mail or chain letters is prohibited.
  - q. The distribution and display of obscene materials is prohibited by the laws of the State of Tennessee (see Tenn. Code Ann. 39-17-902)
  - r. If CHEC provides access to other networks, all rules and conventions of the other networks must be followed.
  - s. Disruption of any activity on a remote node is forbidden.
  - t. Compliance with the Password Policy is required of all computer and network users.
  - u. The sending of unencrypted Personally Identifiable Information by end-user messaging technologies (for example, e-mail, instant messaging, chat) is prohibited.
  - v. The transfer of Personally Identifiable Information to removable electronic media (including but not limited to external hard drive, diskette, flash drive, CD-ROM, DVD-ROM, PDA) will require the written authorization of management.

**Copyright:** Materials published on the Nashville State site is protected by the Digital Millennium Copyright Act. The DMCA also requires that CHEC inform all computer and network users that downloading of copyrighted material is prohibited. In addition, Tennessee Code Annotated §49-7-1(c) specifies that the college ensure that no copyrighted digital music or videos be downloaded using CHEC resources. Any attempts to do so will result in appropriate actions (see Section 7).

**Inspection of Electronic Records:** Electronic records sent, received, or stored on computers owned, leased, or administered by CHEC is the property of the Campus and the Tennessee Board of Regents. As the property of CHEC and TBR, the content of such records, including electronic mail, is subject to inspection by CHEC personnel. Users should have no reasonable expectation of privacy in the use of these resources.

**Violations:** Violations of the policy will result in action by the appropriate college office. Students who violate this policy will be referred to the Dean of Students for appropriate action. Employees who violate this policy may be subject to disciplinary measures imposed by their supervisor in conjunction with the college's Human Resources office. Violations of local, state or federal laws regarding unlawful access or use may be referred to the appropriate law enforcement officials for investigation and/or prosecution.