Policy No: 621.3 **Policy Contact: Vice President for Business Operations**

Policy Title: ACCEPTABLE USE OF COLLEGE COMPUTER RESOURCES AND NETWORKS

East Central Community College seeks to provide computer resources, computer networks, and information technology for the students, faculty, staff, and administration at a level that enhances student success, teaching and learning, and productivity. It is the responsibility of the users of computers and networks to act in a manner consistent with the rights of all other users. To that end, the College promotes the following policies and procedures.

- Electronic information is volatile, easily reproduced, and easily vandalized. Respect for the work and personal expression of others is critical. Further, one should never publish anything on computer networks that they are unwilling to have made public. Users must never access, use, or edit files for which they do not have authorization.

- Technology Management monitors the College's network. Security and management considerations require that the networks be open for review and maintenance. Users of the network can assume that any material transferred through and/or stored on College network or storage infrastructure is public information and should act accordingly. There should be no expectation of privacy by the user of College servers, workstations, or network equipment. The College may delete or deliver contraband (illegal materials) discovered on College computer equipment to legal authorities without permission from or notification of the assigned user.

- Technology Management filters access to the Internet. Requests to either block or allow a particular Internet site should be made in the following fashion: requests that are instructional in nature should be made to the division chair and then forwarded to the Vice President for Instruction for approval. Requests that are non-instructional in nature should be made to the respective Vice President for approval. Approved requests will be forwarded to Technology Management. Any questions or concerns related to blocking or allowing access to websites using the College's network should be presented to the College President.

- The College's computers and networks are provided for official business and for the purpose of fulfilling the mission of the College. Users shall access only those files and data for which they have authorization. Official records accessed online via the College's ERP/SIS or over any other College information medium by administrators, faculty, and staff at East Central Community College are exclusively for College business, are intended strictly for appropriate College personnel, and must not be used for any other purpose or disclosed to parties, on or off campus, except as delineated in Policy 816. Users shall protect his/her personal computer(s) from unauthorized use and safeguard his/her user-IDs and passwords.

- Private and/or commercial uses of the College's computers or networks and work conducted for personal gain or profit will not be allowed.

- Employees should not use the college network to take courses over the Internet during normal working hours. Should employees have a legitimate need to use the college network to take courses for credit from a source other than East Central Community College or the Mississippi Virtual Community College, permission should be obtained from their Vice President prior to enrollment.

- At no time shall a computer user engage in illegal or immoral activities on the College's networks. Examples of these activities include the transmission of defrauding, obscene, threatening, violent, or unlawful materials. In addition, the distribution of copyrighted materials over the College network without the permission of the copyright owner is prohibited - this includes the file sharing of copyrighted digital files or the long-term storage of same or transfer to portable media. The College may delete such files within its infrastructure without permission from the assigned user.

- Publication of annoying, harassing, or intimidating messages on the networks will not be allowed.

- Using the College or state networks to advocate personal political positions will not be allowed.

- Computer or network users are not allowed to circumvent system security measures, modify the computer system or software, install invasive software such as "worms" or "viruses," or install pirated software on the College's computers or networks.

- Users are not allowed to remove hardware, data, software, manuals, supplies, etc. from the College's computing sites without proper authorization.

Copyright Infringement

Unauthorized distribution of copyrighted material, including through peer-to-peer file sharing, may subject users of computers and networks to civil and criminal liabilities.

Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.

Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than $750 and not more than $30,000 per work infringed. For "willful" infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorney's fees. For details, see Title 17, United States Code, Sections 504, 505.

Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense. For more information, please see the website of the U.S. Copyright Office at www.copyright.gov.

Anyone who knowingly violates the principles outlined in this policy will be subject to appropriate disciplinary action.

(Revised 3/14/00; Revised 11/12/02; Revised 10/14/03; Revised 06/11/13; Reviewed 6/14/16; Revised 4/9/2019)