

COLUMBUS STATE COMMUNITY COLLEGE
POLICY AND PROCEDURES MANUAL

INFORMATION TECHNOLOGY
Procedure No. 15-01 (C)
Page 1 of 2

Effective March 29, 2004

- (1) The following constitutes a college-wide procedure for the management of college computer data networks, both on- and off-campus; all equipment housed at the college; and the resources they make available.
- (2) Use of Columbus State Community College resources is for purposes related to the instructional and administrative mission of the college. Faculty, staff, and students may use computing resources for purposes related to their instruction, their studies, their duties as employees of the college, official business of the college, or other college-sanctioned activities. The use of college computer and information resources for commercial purposes other than college-related is prohibited. Facilities used for connectivity are to be used in a responsible, ethical, and legal manner.
- (3) All individuals authorized to use CSCC systems, which include but are not limited to computers, printers, peripherals, network and email, online and web services are required to use the college provided account information that includes user-ID and password.
- (4) Activation and de-activation of the user accounts and access to resources are at the college's discretion.
- (5) Inappropriate use of the information technology resources, which Columbus State Community College makes available to faculty, staff, and students, may result in suspension or termination of access. In addition to federal, state, and international laws, college policy prohibits but is not limited to:
 - (a) Harassment, including creating, displaying, or transmitting threatening, racist, sexist, or obscene language and/or materials both inside and outside of campus community.
 - (b) Deliberate or intentional destruction or damage to equipment, system installations and configurations, software, or data belonging to the college or others.
 - (c) Use of computer systems in a manner that results in a violation of the privacy rights of others.
 - (d) Unauthorized monitoring of electronic communications.
 - (e) Violating computer system security.
 - (f) Unauthorized use of computer accounts or access codes.
 - (g) Use of computer facilities (i.e., labs, rooms) for purposes unrelated to the college's mission, goals, and administrative functions. For non-tangible computing resources, such as e-mail, priority to access and resource use is given to academic and college-

COLUMBUS STATE COMMUNITY COLLEGE
POLICY AND PROCEDURES MANUAL

INFORMATION TECHNOLOGY

Effective March 29, 2004

Procedure No. 15-01 (C)

Page 2 of 2

- related work. Everyone is expected to avoid creating excessive network traffic or storage consumption.
- (h) Using computer systems to commit academic misconduct.
 - (i) Posting on electronic bulletin boards materials that violate existing laws or college policies.
 - (j) Engaging in commercial and non-commercial advertising, Internet gambling, or other non college-related functions.
 - (k) Using computer systems for online or offline games not related to the college's programs and/or mission.
 - (l) Using computer systems for the purpose of creating and distributing harmful programs such as viruses, worms, etc., that incapacitate, compromise, or destroy college or non-college resources.
 - (m) Unauthorized modification to individuals' system profiles or configurations.
- (6) System administrators will not review contents of files nor monitor the content of files, unless one of their special tasks (e.g., recover a file) may require them to review the contents. In a situation where the content of the file is disclosed to the system administrator, he/she has the obligation to maintain complete confidentiality. System administrators include but are not limited to system operators, programmers, analysts, telecommunications staff, managers, Web developers, and administrators.
- (7) System administrators work with files for the maintenance of networks, computers, and storage systems to create backup copies or resolve network difficulties. Additionally, Columbus State may routinely monitor and log utilization statistics (e.g., network session connection times, etc.). Monitoring will be conducted for general statistic gathering and not individually focused. Monitoring of individual activity will require the authorization of the President or his/her designee. In all cases, individuals' privileges and rights of privacy will be preserved to the greatest extent. In extreme cases where health or safety issues necessitate an emergency, files may be accessed by system administrators; appropriate documentation must be filed with the Vice President of Information Technology by the system administrator.