




January 17, 2012

## MEMORANDUM

**TO:** District Board of Trustees

**FROM:** Jim Murdaugh, President 

**SUBJECT:** Policy Manual Revision - Computer Security and Access, Software Licensing, and Electronic Correspondence

---

### Item Description

Policy Manual Update - Chapter Three

### Overview and Background

Policy manual updates are necessary for the following reasons: to remain compliant with new state and federal laws; to update staff/organizational references; to remove procedures from policy and to recommend changes to improve College governance and operations.

Attached for your review and approval is the proposed college policy 3-26 Computer Security and Access, Software Licensing, and Electronic Correspondence. This policy has been through the appropriate College Standing Committees for review and comment.

### Past Actions by the Board

The Board last amended policies in Chapter 3 on September 21, 2009.

### Funding/Financial Implications

There are no costs related to this item.

### Staff Resource

Teresa Smith

### Recommended Action

Approve the policy as presented.

**TALLAHASSEE COMMUNITY COLLEGE  
DISTRICT BOARD OF TRUSTEES  
P O L I C Y**

<b>TITLE:</b> Computer Security and Access, Software Licensing, and Electronic Correspondence	<b>NUMBER:</b> 03-26
<b>AUTHORITY:</b> Florida Statute: 775.0847, 827.071 (4), (5), 1001.64, 1001.65 Florida Computer Crimes Act Chapter 815; Electronic Communications Privacy Act 18 USC, §2510-2522; Computer Fraud and Abuse Act 18, § 1030	<b>SEE ALSO:</b>
<b>DATE ADOPTED:</b> 01/17/2012	

**Policy Scope and Applicability:**

- A. As an institution of higher learning, Tallahassee Community College encourages, supports, and protects freedom of expression and an open environment to pursue scholarly inquiry and to share information. Access to networked computer information in general and to the Internet, in particular, supports the academic community by providing a link to electronic information in a variety of formats and covering all academic disciplines. Consistent with the College’s anti-discrimination policy, the use of information resources should not be denied or abridged because of race, sex, religion, national origin, age, disability, marital status, gender identification, genetic information, and sexual orientation. The computing and network facilities of the College are limited and should be used wisely and carefully with consideration for the needs of others. As with any resource, it is possible to misuse computing resources and facilities and to abuse access to the Internet. The following statements address, in general terms, the College’s philosophy about computing use.
  
- B. This policy is applicable to all individuals using College owned or controlled computer and computer communication facilities or equipment, whether such persons are students, staff, faculty, or authorized third-party users of College computing information resources. It is applicable to all College information resources whether individually controlled or shared, stand alone or networked. It applies to all computer and computer communication facilities owned, leased, operated, or contracted by the College. This includes, but is not limited to, personal computers, workstations, servers, personal communication devices, associated peripherals and software, and electronic mail accounts, regardless of whether used for administration, research, teaching, or other purposes.



- C. Individual units within the College may define "conditions of use" for information resources under their control. These statements must be consistent with this overall Policy but may provide additional detail, guidelines, and/or restrictions. Such policies may not relax or subtract from this policy. Where such "conditions of use" exist, enforcement mechanisms in conditions of use of individual College units shall apply. These individual units are responsible for publicizing both the regulations they establish and their policies concerning the authorized and appropriate use of the equipment for which they are responsible.
  
- D. Computer accounts are provided to faculty, staff, and students as a privilege associated with membership in the College community. When an individual accepts this privilege, a number of responsibilities must be assumed, including knowledge of appropriate College policies and procedures.

#### **Electronic Communication and Access to Information:**

The TCC internal networks and connections to the National Information Infrastructure provide a wide range of facilities for communication between individuals and for disseminating information and ideas. Electronic communication and information resources will be increasingly important to College faculty, staff, and students. The College supports open access to electronic communication and information, as follows:

1. Members of the College community may freely communicate and access information on electronic networks.
  
2. Material accessible to the TCC community through networks and materials disseminated from TCC should not be restricted on the basis of its content, nor because of the origin, background, or views of those contributing to its creation.

#### **User Responsibilities and Expectations:**

- A. Access to the information resource infrastructure both within and beyond the College campus, sharing of information, and security of the intellectual products of the community all require that each and every user accept responsibility to protect the rights of the community. Access to the networks and to the information technology resources at Tallahassee Community College is a privilege granted to College students, faculty, staff, and third parties who have been granted special permission to use such facilities. Access to College information resources must take into account the following factors: relevant laws and contractual obligations, the requestor's need to know, the information's sensitivity, and the risk of damage to or loss by the College.

- B. All members of the college community are responsible for protecting the confidentiality, integrity and availability of information resources created, received, stored, transmitted or otherwise used by the college.
- C. Anyone who accesses, uses, destroys, alters, or damages College information resources, properties or facilities without authorization, may be guilty of violating state or federal law, infringing upon the privacy of others, injuring or misappropriating the work produced and records maintained by others, and/or threatening the integrity of information kept within these systems. Such conduct is unethical and unacceptable and will subject violators of this Policy to disciplinary action by the College, including possible termination from employment, expulsion as a student, and/or loss of computing systems privileges.
- D. The College requires that members of its community act in accordance with these responsibilities, this Policy, the College's Student or Faculty Handbook, as appropriate, TCC Policies and Procedures, relevant laws and contractual obligations, and the highest standard of ethics. The policies as stated in this Policy are intended to ensure that users of College information resources shall:
  - 1. respect software copyrights and licenses,
  - 2. respect the integrity of computer-based information resources,
  - 3. refrain from seeking to gain unauthorized access,
  - 4. respect the privacy of other computer users.
- E. The College reserves the right to limit, restrict, or extend computing privileges and access to its information resources. Data owners—whether departments, units, faculty, students, or staff—may allow individuals other than College faculty, staff, and students access to information for which they are responsible, so long as such access does not violate any license or contractual agreement, College policy, or any federal, state, county, or local law or ordinance. However, users are personally responsible for all activities on their userid or computer system and may be subjected to disciplinary action and/or loss of privileges for misuse of computers or computing systems under their control even if not personally engaged in by the person controlling the computer or system.

#### **Authorized User Purposes:**

- A. College computing facilities and accounts are to be used for the College-related activities for which they are assigned. Campus and network computing resources must be used in a manner consistent with Chapter 815, Florida Statutes Computer Crimes Act and Title 18, United States Code, Electronic Communications Privacy Act of 1985. Unauthorized or fraudulent use of the College's computing resources may result in felony prosecution and punishment as provided for in Florida Statutes, Chapter 775, Florida Criminal Code. When users cease to be members of the academic community (such as by graduating or ceasing employment), or when persons are assigned to a new position and/or responsibilities within the College, the access authorization of such person will be reviewed and may be altered. Users whose relationships with the College change may



not use computers and computing resources, facilities, accounts, access codes, privileges, or information for which they are not authorized in their new relation to the College.

- B. Users may use only their own computer accounts. The negligence or naïveté of another user in revealing an account name or password is not considered authorized use. Convenience of file or printer sharing is not sufficient reason for sharing a computer account. Users are personally responsible for all use of their computer account(s).
- C. Appropriate use of computing and networking resources includes instruction, independent study, authorized research, independent research appropriate to college business, communications, and official work of the offices, units, recognized student and campus organizations, and agencies of the College. Computing facilities, services, and networks may not be used in connection with compensated outside work for the benefit of organizations unrelated to the College except in connection with approved scholarly pursuits (such as faculty publishing activities). The computing and network resources of the College may not be used for personal financial gain or commercial purposes. For information regarding use of computing and network resources in connection with College-sponsored commercial projects refer to the TCC District Board of Trustees Policy 6Hx27:03-29.
- D. The computing and network resources of the College may not be used to harass another person. Users should not transmit to others or display images, sounds, or messages that might be perceived by a reasonable person as, or have been identified as, harassing. (See the College policies on harassment, Employee Code of Conduct and Student Conduct Codes.)
- E. Electronic forums such as mail distribution lists and Usenet news groups all have expectations regarding subject area and appropriate etiquette for postings. Members of the TCC community should be considerate of the expectations and sensitivities of others on the network when posting material for electronic distribution.
- F. Computer users must observe and comply with Federal, State, and local laws governing computer and information technology, and all College rules and regulations. The College also supports the policy of EDUCOM, the non-profit consortium of colleges and universities committed to the use of information technology in higher education, on "Software and Intellectual Rights".

### Software Licensing

- A. Information Technology will maintain licensing for approved application software that resides on the LAN or mainframe. Individual departments or users will be responsible for licensing of software that is to be run locally on a personal computer.
- B. At orientation, every new employee shall be furnished with a brochure that explains the fundamentals of computer software licensing. The employee shall sign a form indicating that he/she will not receive and use unauthorized copies of software or make

unauthorized copies of software for others. Annually, every user who is connected to the network will complete a survey that lists the software he/she is using on the LAN and on his/her personal computer hard drive, if any.

#### **Special User Notifications:**

- A. The District Board of Trustees for Tallahassee Community College is the legal owner of all College "owned" or controlled computers and networks. The contents of all storage media owned or stored on College computing facilities are property of Tallahassee Community College.
- B. The College cannot protect individuals against the existence or receipt of material that may be offensive to them. As such, those who make use of electronic communications are warned that they may come across or be the recipients of materials they find offensive. Those who use e-mail and/or make information about themselves available on the Internet should be forewarned that the College cannot protect them from invasions of privacy and other possible dangers that could result from the individual's distribution of personal information.
- C. Misuse and/or violation of College policy, as determined by the college and governing statute will be grounds for disciplinary action and possible termination of employment. Any individual using College computing resources and facilities must realize that all mainframe computer systems maintain audit trails logs or file logs within the mainframe computer. Such information as the user identification, date and time of the session, the software used, the files used, the computer time, and storage used, the user account, and other run-related information is normally available for diagnostic, accounting, and load analysis purposes. Under certain circumstances, this information is reviewed by system administrators, either at the request of an academic department, or in situations where it is necessary to determine what has occurred to cause a particular system problem at a particular time. For example, analysis of audit files may indicate why a particular data file is being erased, when it was erased, and what user identification has erased it.
- D. The College reserves the right to view or scan any file or software stored on the computer or passing through the network, and will do so periodically to verify that software and hardware are working correctly, to look for particular kinds of data or software (such as computer viruses), or to audit the use of College resources. Misuse and/or violation of the College policy, as determined by the college and governing statute will be grounds for disciplinary action and possible termination of employment.
- E. The College supports each individual's right to private communication, and will take reasonable steps to ensure security of the network. Although messages on College computing resources are potentially accessible to others through public records laws, Public Records Law requests for documents maintained on College computing resources must be dealt with by the user who controls the requested documents. The College cannot guarantee absolute privacy of electronic communication.



**Conduct Expectations and Prohibited Actions:**

- A. All uses of College IT resources are subject to applicable rules, policies, and procedures of the College and/or governing boards as well as the Florida Statutes governing computer fraud, misuse of state equipment resources, public information, and related criminal offenses.
  
- B. Occasional, incidental personal use of IT resources is permitted by this policy, except when such use:
  - 1. Interferes with the performance of the user's job, employment, or other College responsibility.
  - 2. Results in additional incremental cost or burden to the College's IT resources.
  - 3. Exceeds occasional, incidental use, which is defined as "non-constant, infrequent use" (e.g. use on an agreed upon work break and/or lunch period).
  - 4. Is otherwise in violation of this policy.

This does not preclude additional limits on personal use of College equipment as may be determined by individual units within the College in accordance with normal supervisory procedures.

- C. The following examples of acts or omissions, though not covering every situation, specify some of the responsibilities that accompany computer use at Tallahassee Community College, and outline acts or omissions that are considered unethical and unacceptable, and may result in immediate revocation of privileges to use the College's computing resources and/or just cause for taking disciplinary action up to and including discharge, dismissal, expulsion, and/or legal action:
  - 1. Individuals must not attempt to undermine the security or the integrity of computing systems or networks and must not attempt to gain unauthorized access. Users may not use any computer program or device to intercept or decode passwords or similar access control information. If security gaps are observed, they should be reported to the appropriate system administrators.
  - 2. Individuals should not intentionally damage or disable computer systems, networks, or software without authorization for any purpose. (See the Student Conduct Code, Article II, B-13)
  - 3. Copying or using software, except as explicitly permitted under licensing agreements, is a violation of law. Computer users should be able to prove ownership of software in their possession.

4. Using College computing resources to generate or access obscene material as defined by Florida or federal law and acceptable community standards or creating a hostile work and/or educational environment.
5. Using College electronic communication facilities to send fraudulent, harassing, obscene, threatening, or other unlawful messages is prohibited.
6. Using College computers or computing systems in any manner which violates Federal, state, or local laws, or College policies.

### **Consequences of Misuse of Computing Privileges**

- A. Users, when requested, are expected to fully cooperate with system administrators in any investigations of system abuse. Failure to cooperate may be grounds for cancellation of access privileges or disciplinary action.
- B. Abuse of computing privileges is subject to disciplinary action. If system administrators have evidence of misuse of computing resources, and if that evidence points to the computing activities or the computer files of an individual, they have the obligation to pursue any or all of the following steps to protect the user community:
  1. Notify the user's instructor, department or division chair, or supervisor of the investigation.
  2. Suspend or restrict the user's computing privileges during the investigation.
  3. Inspect the user's files, diskettes, tapes, and/or other computer-accessible storage media. System administrators must have a reasonable belief that the trail of evidence clearly leads to the user's computing activities or computing files before inspecting the user's files.
  4. Refer the matter for possible disciplinary action to the Director of Human Resources.
- C. Violations of computer and network policy as outlined in this document will be considered on a case-by-case basis according to established policies; determinations may include denial of access privileges and/or disciplinary action. In all instances, measures will be taken to protect the system; however, due-process rights of everyone involved will be observed in all cases. Users are reminded that some uses of the network are governed by the Student Honor Code, local, state, or federal laws. As incidents of misuse and/or violation of College policy occurs, discipline will be administered with reference to the nature and seriousness of the violation.