SOUTHWEST TENNESSEE COMMUNITY COLLEGE

SUBJECT: **Employee Email**

EFFECTIVE DATE: **October 4, 2001; January 21, 2010; Revised July 1, 2024**

*In October of each year, Information Technology related policies are reviewed as required by external regulations.

Purpose

The purpose of this policy is to establish the appropriate use of employee email at Southwest Tennessee Community College ("Southwest" or "the College").

Policy

This policy is not intended to address the ownership of intellectual property stored or transmitted through the College's e-mail system. Ownership of intellectual property is governed by law. It will be consistent with and not supersede other Southwest policies, including the Information Systems Acceptable Usage Policy, 6:00:00:00/5.

Procedure

Southwest recognizes that principles of academic freedom, freedom of speech, and privacy hold important implications for the use of electronic communications. The College respects the privacy of electronic communications in the same way that it respects the privacy of paper correspondence and telephone conversations. However, employee privacy does not extend to the employee's work-related conduct or to the use of College-provided equipment or supplies. Personal use of email is a privilege, not a right. As such, the privilege may be revoked at any time. Abuse of the privilege may result in appropriate disciplinary action. Each College employee should be aware that the following practices and procedures might affect your privacy in the workplace.

Administration's Right to Access Information

A. Email is available at Southwest to facilitate quick, reliable, and cost-effective College communications among staff, faculty, and students. Although each member of the College community has an individual password to access this system, the system belongs to the College and the contents of email communications are accessible at all times by the College for any business purpose.

B. All email correspondence in the College's communications systems is the property of the College, regardless of where it originated.

C. Employee email communications are not considered private despite any such designation by the sender or the recipient.

D. Employees should be aware that messages sent to recipients outside of the College, if sent over the internet and not encrypted, are not secure. Accordingly, no College student's or client's confidential information should be sent over the Internet except by the College's approved means. Secure Copy or Secure FTP are approved by the College for file transfers or confidential information.

E. As stated in the College's Acceptable Usage Policy, 6:00:00:00/5, the College does not routinely inspect, monitor, or disclose electronic communications without the holder's consent. Nonetheless, the College reserves the right to inspect, monitor, or disclose electronic communications under compelling circumstances. These circumstances include, but are not limited to:

1. Legal discovery, writ, warrant, subpoena, etc.
2. When there is a threat to the computer system's integrity or security as determined by the system administrator.
3. To enforce policies against harassment and threats to individuals.
4. To protect the College or its employees and representatives against liability or other potentially adverse consequences.
5. When there is significant reason to believe Southwest policies have been violated.

These actions must be requested by a member of the senior staff through their department reporting structure and/or the Vice President of People and Culture (Human Resources). These requests are directed to the Chief of Administrative Services, who oversees Information Technology.

The existence of passwords and "message delete" functions do not restrict or eliminate the College's ability or right to access electronic communications. Even deleted messages may be recovered and reviewed.

Employees who use their own equipment to connect to the College's information systems from outside the campus premises or from home should know that any communications that are delivered to or sent through the College's communications systems are not private, may leave copies behind on the College system, and are subject to all of the terms and provisions of this policy statement.

User Accounts

A. Each employee of the College shall be granted an email account.

B. The primary method of communication to all faculty, staff, and students shall be through College email. The College has the right to expect that those communications will be received and read in a timely fashion.

1. All College employees must maintain their email accounts so that they are available to receive important communication from the College. The College expects that all employees check their College email account on a frequent and consistent basis in order to stay current with College communications and to respond in a timely fashion to any time-sensitive inquiries.
2. It is recommended that all College employees utilize the archival utility feature to relocate emails older than six (6) months to a .PST file if such files are needed for continued reference. This will maximize employee email disk space quotas. Assistance setting up this feature is available through the IT Help Desk by submitting a Quick Ticket.
3. Failure to maintain one's College email account may be cause for disciplinary action up to and including termination.

4. It is the responsibility of the user to protect access to their email account with a private password. Employees shall not share email account passwords, provide email access to an unauthorized user, or access another user's email inbox without authorization. Further information is available in the College's Electronic Information Security Policy 6:02:20:00/37, which describes the standards for the creation of strong passwords, the protection of those passwords, and the frequency of change.
5. Email account holders will not be asked for any personally identifiable information such as their username, password, or any other similar information.

C. Email access is provided only to current employees who are actively employed by the College. Employees who terminate employment, take extended leave, or retire will have their account disabled. Access to an employee's email account may be given to their supervisor or the supervisor's designee, if requested. After a reasonable period of time, the account and inbox are subject to deletion. Returning retired, post-tenured, or re-hired employees may be provided with a new account username/email address upon their return.

Message Content

Email messages from the Southwest email system reflect upon the College. Refer to the College's Acceptable Usage Policy 6:00:00:00/5 for further information on the Unacceptable Uses of Information Technology Resources.

A. Offensive, demeaning, or disruptive messages are prohibited. This includes, but is not limited to, messages that are inconsistent with the College's policies concerning equal employment opportunity and sexual or other unlawful harassment.

B. The use of the "All", "Macon", "Union," and similar distribution lists on the College's email system shall be limited to Deans, Executive Directors, Directors, Department Chairs, and members of the President's Senior Staff. Any official information that needs to be sent by an associate of a department will be sent to "All" by the appropriate Dean, Executive Director, Director, Department Chair, or Senior Staff member. Information regarding College-wide announcements, etc. should be submitted to the Communications and Marketing department for publication.

C. Employees should be aware that when sending an email of a personal nature, there is always the danger of the employee's words being interpreted as official College policy or opinion.

Personal Email

A. Email should not be used for any personal monetary interests or gain.

B. Employees should not subscribe to mailing lists or mail services strictly for personal use.

C. Personal email should not impede the conduct of College business.

D. Chain email should be deleted immediately upon receipt and not forwarded to any other employees. Circulating chain email results in an enormous volume of messages on the network, which may impede the ability of the College to conduct legitimate business.

Email Virus Protection

Employee email is protected from viruses by antivirus software and hardware. It is recommended that employees also take appropriate precautions and load antivirus software on their personal computers/devices with which they plan to access any College information systems.

Meta Policy

Policy maintenance, communication, and storage are in accordance with the College's Acceptable Usage Policy 6:00:00:00/5.

All users of Southwest computer and telecommunications resources are expected to read and abide by the College's Acceptable Usage Policy.

Source of Policy: **Chief Financial Officer**

Responsible Administrator: **Chief of Administrative Services**

Related Policy: **6:00:00:00/5**

TBR Policy Reference: **1.08.05.00; 1.08.00.00**

Approved: Tracy D Hall
President

Date: **July 1, 2024**