

Murray State College

Employee's Acceptable Use of

Computer, Network, and Communications

2015

INTRODUCTION

Murray State College (MSC) is committed to maintaining our progressive, modern- information technology systems in a manner that facilitates successful achievement of the mission of our college. A critical aspect of this is a responsible use procedure for students, faculty, staff, and others who use MSC's computers, network, distance learning facilities, and/or other communications technology.

All technology users have the responsibility of using technology in an effective, efficient, and ethical manner. The standards stated in this procedure are derived from common sense and common decency that apply to the use of all public resources within the college.

A. GENERAL RULES

Purpose. The purpose of developing and maintaining information technology at MSC is to promote access, use, and exchange of knowledge and information. This technology is intended to: a) promote learning, research, and other scholarly activities and b) conduct official MSC business and activities. Resources and technology for this purpose include telephones, FAX machines, photocopiers, computers and peripherals, distance learning resources, a local area network, and network connections to the Internet via the Oklahoma State Regents for Higher Education's OneNet.

User Responsibilities, Violations, and Abuse. Rules and conditions apply to all users of MSC technology. Violation of any of these is unethical and some violations are unlawful. The use of technology and related facilities at MSC is a **privilege, not a right**, and MSC seeks to protect legitimate technology users by imposing sanctions on those who abuse the privilege. This is to ensure that legitimate users will have the maximum resources possible.

To retain the privilege of technology use, individuals must accept responsibility to protect the

rights of all users by adhering to all rules and conditions for use. The following are examples of abuse:

- interference with the intended use of technology;
- violation of copyrights, patents, authorization agreements, licensing agreements, and/or other actual or implied contractual agreements;
- unauthorized removal/use of MSC property;
- unauthorized access or attempted access to confidential resources and information;
- unauthorized modification of any technology, programs, files, or other resources;
- attempt to restrict/remove access rights from the IT department;
- unauthorized destruction, dismantling, or disfigurement of any technology, programs, files, or other resources;
- violation of privacy of other individuals or entities who are users or providers of information resources;
- harassment of another individual on the network or connected systems and/or developing or using programs which harass other computer users;
- use of technology, including telephones, to send fraudulent, harassing, obscene, indecent, profane, intimidating, or other unlawful messages according to state or federal law;
- any personal/for-profit use, including but not limited to transmission of commercial or personal advertisements, invitations, solicitations, promotions, auctions, and gambling;
- use of home directory account for storage of personal items;
- transmission of messages in support of illegal activities; and
- transmission of destructive programs.

Copyrights. Additional elaboration on copyrights is warranted. All software protected by copyright is not to be copied except as specifically stipulated by the owner of the copyright. Protected software is not to be copied onto, from, or by any MSC system except in accordance with applicable licensing agreements. Thus, the number and distribution of copies of programs may not be done in such a way that the number of simultaneous users exceeds the

number of original copies purchased unless otherwise stipulated in the purchase contract.

Images and written materials available via electronic resources are most often subject to copyright laws. Individual users are responsible for acquiring, maintaining, and submitting a copy to their appropriate supervisor, the permissions for any uses of such materials. Additional information on copyright information is available in a separate MSC copyright procedure.

Display of Offensive Materials. Display of potentially offensive ethnic, sexual, or otherwise offensive materials is prohibited. Special arrangements may be made for research or projects that require viewing such potentially sensitive materials. Students, faculty, staff, and other users of MSC technology and facilities may complain of sexual or racial harassment by virtue of being exposed to obscene images, video, or text. In such cases, the user responsible for publicly displaying such material may have their user privileges revoked if evidence is presented that substantiates the complaints.

Limiting Use. MSC reserves the right to limit a computer user's sessions if there are insufficient resources or if the user violates or abuses user rights. The protection of rights of all computer and other technology users depends on the protection of the integrity of the MSC system as a whole. Users are responsible for reporting any abuses by other users, defects in system accounting, or defects in system security to the IT department immediately upon discovery.

Monitoring. The IT Department is authorized to electronically monitor information technology resources at MSC. Reports of suspected violations of this procedure will be reported to the appropriate direct supervisor/administrator. It is the responsibility of all users to visually monitor information technology resources and report any misuse of resources to the appropriate supervisor/administrator and/or Information Technology. Violations supported by evidence will be handled in the same manner as any other violation of campus procedure according to the applicable procedures for counseling students, staff, faculty, and administrative personnel.

It is to be noted that a supervisor/administrator will be notified of any violations and may at any time request to view or know of any violation(s) committed by any individuals under their direct supervision.

It is also to be noted that once the supervisor/administrator is aware of any violation(s), it is the responsibility of that supervisor/administrator to determine the appropriate course of action. If action is not taken by the supervisor/administrator within ten working days, then the next appropriate supervisor/administrator will be notified

Web Page Development. The World Wide Web offers MSC the opportunity to provide a broad spectrum of information in the multimedia format to large numbers of people. Institutional information published on the Web by MSC users must meet certain basic standards and represent MSC in a coherent, positive, and appropriate manner. These standards are presented in a separate MSC Web Page Development Guide.

Passwords. System security is maintained in large part by password protection of computer accounts. You are required to change your network logon password every ninety days. When your password expires, at the next attempted logon, you will be prompted to set a new password before being permitted to logon. Passwords are required to be at least 8 or more characters in length. By law, a computer user who has been authorized to use an account may be subject to both civil and criminal liability if that account is made available to unauthorized persons. The authorized user of the account is responsible for activity that occurs under that account.

Passwords may be changed through self-help. Employees must first set up security questions to enable the self-help function. Please visit the MSC Email webpage to set up security questions, and to perform self-help password resets. This capability is available to employees only; students must contact the IT Department for account assistance.

Protect your passwords as you would a key to your car or house.

B. COMPUTER AND E-MAIL ACCOUNTS

Email. Murray State College provides email service through Google (GMail). All employees therefore have the range of Google services, including calendaring, cloud storage, Google office-type programs, and video/chat conferencing.

Employee Accounts. These accounts are for MSC employees. They are the property of MSC and are to be used for academic or administrative purposes in accordance with applicable policies, copyrights, intellectual property rights, and federal and state laws. Authorization for these accounts is the responsibility of the appropriate area supervisor who will request accounts for persons under their supervision.

Affiliate Accounts. These accounts are for individuals or groups who are not directly associated with MSC but whose access to the network has a clear and distinct connection to the accomplishment of the mission of the college. Affiliate accounts are the property of MSC. Users must sign an Acceptable Use Policy and record pertinent information with an authorized college official before being allowed to utilize the affiliate account. Affiliate users are subject to all applicable policies, copyrights, intellectual property rights, and federal and state laws. Authorization of affiliate accounts is the responsibility of the appropriate dean, vice president, or the college President who will provide the names of authorized individuals or groups to the IT Department.

Home Directories. One home directory will be issued to each employee account. These directories are designed for MSC business and academic affairs. MSC reserves the right to monitor all contents of these directories. Additionally, users have unlimited storage available through their MSC Google accounts.

Right to Revoke Account Rights. MSC reserves the right to revoke the account of any technology user who does not abide by applicable policies, copyrights, intellectual property rights, and federal and state laws. The following steps shall be enforced when a violation occurs:

- ✓ First violation – Individual’s account is disabled. Individual shall meet with appropriate supervisor/administrator. A statement acknowledging the violation will be required to be signed by the violator. The

individual’s account will be re-enabled once the IT department receives a copy of the signed acknowledgement and a request for reinstatement of the account from the appropriate supervisor/administrator. If the violation involves an illegal program or copyright violation, the program and related folders or files will be removed by or in the presence of IT department personnel.

- ✓ Second violation - Individual’s account is disabled. Individual shall meet with the appropriate dean or vice president. Upon resolution, the user will receive a restricted account for a period of one calendar year.
- ✓ Third violation – The individual’s account is disabled. An ad-hoc committee comprised of two peers, one representative from each of the campus assemblies, and one administrator (excluding the President) will review the series of events, and recommend the appropriate disciplinary action to the President.

If an individual is uncertain if a planned action is a violation, that individual is encouraged to contact the IT Department before taking that action.

Inactive Accounts. Individuals no longer employed by MSC, whether by retiring, resigning, or termination, and have retained information on the MSC network shall release all stored data to their immediate supervisor or VP over their area of employment.

C. TELEPHONES

Desk telephones and institution-issued cell phones are the property of Murray State College, and follow the same acceptable use guidelines as computer and network devices. Phones are to be used for official institution business. If individuals are incurring charges due to personal calls, the institution can and will levy those charges upon the individual.

D. “BRING YOUR OWN DEVICE” (BYOD)

Murray State College does not support BYOD, nor requires employees to use their personal phone or technology devices. Employees who choose to set up their personal devices to accept email, or use their personal phones to conduct

institution business, do so of their own choice and will not be reimbursed.

The IT Department will not provide services or software for personal devices to connect to the MSC network. Laptops and other devices are available for check-out. If it is necessary for personal devices to be connected to the network, a request by both the individual and the department head will be submitted; and the device will be imaged/configured to meet MSC security policy requirements.

Murray State College and its IT Department accept no liability for any damage, lost data, etc. incurred while re-configuring personal devices to meet MSC security policy requirements.

E. IT SUPPORT REQUESTS

Requests for IT assistance can be submitted through the MSC website on the Information Technology webpage; or may be emailed to: help@mscok.edu. If internet or email is unavailable, please call the IT Department to submit your request.

- 1) Include your name, contact email and/or phone number, and a detailed description of the request. Include as much information as possible, including the scope and impact to operations.
- 2) Requests are handled on a priority basis. Whenever possible, target completion dates will be met considering that the date is reasonable.
 - a. The IT Department will assign a priority to your request based on scope and impact to operations.
 - b. **Normal.** These issues do not impact ability to continue operations, and/or affect a small portion of the institution community. Response time is typically within one business week.
 - c. **Medium.** These issues affect an entire department, major area, and/or safety and security of the institution. Response time is typically within 72 hours.
 - d. **High.** These issues affect one or more departments, major areas, and/or safety and security of the institution. Response time is typically within 24 hours.

- e. **Emergency.** These issues affect the entire institution. An immediate response is required.

- 4) Please note: If a request would typically be categorized as “Normal,” failure to submit that request until the last minute does NOT constitute an upgraded priority. The priority system allows the IT Department to manage available assets and resources. “Last minute” requests may not be honored because assets or resources may not be available.
- 5) If an individual feels that his or her request has not been handled appropriately or in a reasonable amount of time, the individual should contact the CIO/Executive Director for IT. If still unsatisfied, contact the Vice-President for Financial Affairs.

Personal Equipment. IT service on personal technology devices can sometimes result in damage to the employee’s personal device, resulting in the IT department and/or the institution being held liable. Therefore The IT Department will not provide service for/on employee or student personal technology devices.