Policy Number: VI.01
Policy Level: Operating Policy
Originally Issued: October 9, 2013
Revised: April 13, 2016
Revised: November 16, 2016
Revised: March 7, 2017
Policy Owner: Provost/VP for Academic Affairs
Policy Implementation: Chief Information Officer

Information and Communication Technologies Acceptable Use Policy

I. Policy Statement and Purpose

In accordance with state and federal laws and other University policies (including the University's *Information Systems Security Policy),* this policy establishes the standards for acceptable use of computing technology at Athens State University. This policy prohibits various actions described herein which may or may not constitute a crime.

This policy applies to all students, faculty, staff, and guests of Athens State University (including vendors/contractors, visitors, and all others conducting business with the University) who participate in any activity within the scope of authority of the University's administration, faculty, or staff; and/or who use the University's information and communication technologies. This policy applies to all fixed and portable University information and communication technologies. The underlined terms in Sections I and II are defined and elaborated upon in Section III of this policy.

II. Rights and Responsibilities

Any content generated and moved through the University's information and communication technologies (including but not limited to the University network or the Internet), with the exception of content covered by the University's *Intellectual Property: Ownership of Created Works Policy*, is the sole property of the University. As such, all users of information and communication technologies have no ownership in such content or any expectation of privacy with respect to the same. Further, all users of University information and communication technologies must (i) operate within each user's s Limited Access, (ii) engage only in Acceptable Use, and (iii) refrain from Unacceptable use.

The University respects the privacy of Electronic Communications and will make every effort to keep Electronic Communications secure from unauthorized hackers and other outside parties. However, users of Electronic Communications systems (electronic mail, texting, voicemail) should not assume the confidentiality or integrity of any message that is sent or received in connection with the University's information and communication technologies. Users are cautioned that such Electronic Communication is subject to security breaches such as message interception, message alternation, and spoofing.

The University retains the right to access and inspect any active or stored information in the University's information and communication technologies (including but not limited to Electronic Communications stored therein) without the consent of the user(s) as may be authorized by the administration. Such circumstances may include, but are not limited to, access/inspection to protect the integrity of computer technology resources, to manage urgent University matters, to respond to health and safety emergencies, to facilitate personnel disciplinary matters, to conduct discrimination/harassment investigations, or respond to subpoenas, court orders and other valid forms of legal process. Where there is evidence of a criminal offense, the matter will be reported to the University's Administration and/or law enforcement.

The Administration at the University reserves the right to deny the privilege of the use of any or all of the University's information and communication technologies to individuals who violate this policy. Users will also be held accountable for violations of all applicable federal and/or state laws. Violations of this policy may result in the termination or suspension of employment, suspension of computing privileges, personnel/disciplinary review, or other personnel/disciplinary action.

Violators of this policy may owe financial restitution to the University for damages and costs related to Unacceptable Use.

Individuals are responsible for their actions while using the University's information and communication technologies. As such, individual users must respect the privacy and rights of others and demonstrate appropriate concern for the integrity of all University information and communication technologies.

III. Definitions

- Information and Communication Technologies: Computers and computer-related hardware/software including PCs, laptops, tablets, servers, proxy servers, fixed or portable disk drives, mobile telephones, mobile devices, mobile network hotspots, voice-over-IP (VOIP) systems, radio, television, satellites, firewalls, tape/disk backup resources, routers, switches, hubs located on or off of the physical campus used to create, manage, transmit, store manipulate transact, communicate or archive audio, video, text, or electronic mail content using information system, web site, electronic mail systems, software applications, firmware, campus networks, or the Internet that are standalone or attached and accessible through the University network.

- **Electronic Communications**: The transfer of writing, signals, data, sounds, images, signs or intelligence sent via an electronic device. Examples of electronic communication are electronic mail, text messages, social media messaging, blogging (i.e., expressing a writer's own experiences, observations, and opinions), image sharing, online chat, instant messaging, and audio/video conferencing, generated from or received by fixed or portable devices.

- **Limited Access:** The University limits employee access to software programs, data, directories, and processes. Control levels are established jointly by administration, functional area data stewards, and the Chief Information Officer (CIO) and are based on standard industry practices, state and federal laws. Employees are assigned access control levels necessary to complete the duties assigned. Access control levels are implemented and monitored by processes and procedures in the Information Technology Services (ITS) department.

- **Acceptable Use:** It is acceptable to use University information and communication technologies in the pursuit of academic goals and carrying out University business processes related to instruction, research, and administration of the University.

- The University does permit incidental personal use of electronic communications provided that such use does not interfere with the University's operations, generate incremental identifiable costs to the University, and does not violate the law or any other applicable policy/guideline at the University.

Employees are strongly encouraged to have a separate electronic mail account through which they conduct their personal communications and personal business transactions.

Unacceptable Use: All users of University information and communication technologies should use such technology in a professional, ethical, and lawful manner. University information and community cation technologies include, but are not limited to, the following:

- Using another person's computer account or allowing someone else to use your account (e-mail, secure systems, etc.).
- Giving passwords, access codes or other security level access information to any other person.
- Using computers logged into accounts other than their own.
- Sending electronic mail using a University account of another person.
- Using University or personally owned technology to "break into" or "hack into" any computer, network, storage device, or any other accessible device owned by the University or external third party for the purpose of reading, copying, deleting, modifying, or distributing data and/or information of others, or any other purpose or with the intention to mislead or trick others into believing/accepting/doing something.
- Engaging in activities to damage or disrupt any information and communication technology owned by the University or external third party by such acts as virus creation, and propagation, wasting system resources, overloading, or denying access to computing and network resources with excessive data.
- Adding any device to the network with the intention of bypassing existing security or capturing network traffic of any kind.
- Removing any device on the network without the assistance and authorization of a trained technician.
- Making accessible any device and any content intended for official University use without review and approval by Information Technology Services.
- Transmitting messages known to contain a computer virus, worm or spyware, or any form of malware.
- Engaging in activities for the purpose of promoting personal gain and/or profit, or use for organizations other than those directly associated with Athens State University.
- Engaging in any activity which is in violation of the Code of Alabama (1975) §§ 36-25-1 through 36-25-30, as amended, (the "State Ethics Law"), or which, in the opinion of the University administration, is contrary to such law.
- Engaging in any activity that uses University or personally owned information and communication technology to copy, distribute or alter content that violates copyright law, patent protection, or hardware/software license or service agreements.
- Using information and communication technology to engage in illegal activity to support or oppose any candidates or candidates for public office, or for any other political purpose.
- Creating, displaying, transmitting or making accessible threatening, defamatory, libelous, discriminatory, obscene, or harassing language and/or material.
- Sending chain letters, junk electronic mail, or any other type of widespread distribution of unsolicited electronic mail.

- Taking unauthorized possession or creating unauthorized copies, of institutionally owned software and/or hardware technology such as computers, components, disks, or peripherals.
- Masking the identity of an account or machine in any manner misrepresenting your identity in electronic mail or other electronic communication.
- Creating, modifying, executing, or retransmitting any embedded code or command intended to obscure the identity of the sender of electronic mail or electronic messages.
- Transmitting any non-public, sensitive information about University students, employees, or any other individual affiliated with the University such as a password, personally identifiable information (SSN, birthdate, credit card number, grades) or other confidential information to third parties that is outside the legitimate assigned job functions, without the permission of its owner.
- Attempting to gain unauthorized access to any information facility, whether successful or not including running programs that attempt to guess passwords, tricking other users into disclosing their passwords, eavesdropping on communication facilities, and attempting to circumvent data protection schemes or uncover security loopholes.
- Transmitting or receiving any material in violation of any federal or state law is prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material, or material protected by trade secret.
- Sending political advertisement or political lobbying on campus or through the internet.
- Transmitting personally identifiable information through electronic mail, file transfer, or other method both on campus and through the Internet without using appropriate encryption or data movement protocols that protect the integrity of the data.
- Using University trademarks, logos, and any other intellectual property in connection with any non-University sanctioned activities.
- Participating in any activity violates the University's non-discrimination and anti-harassment policies, or misrepresents personal opinion/beliefs as being those of the University.

IV. Responsibility for this Operating Policy

Policy Owner

As part of the initial approval of this policy by the President and subsequent to the original dissemination of the policy, the Provost is the policy owner for the ongoing evaluation, review, and approval of this policy. Subsequent reviews and revisions to this policy must be in accordance with approved operating policy procedures and processes.

This policy will be reviewed every two years or more frequently as needed.

Responsibility for Policy Implementation

The President has assigned the responsibility of implementing this policy to the Chief Information Officer.