

STOCKTON UNIVERSITY



PROCEDURE

Acceptable Usage Standards of Computing and Communication Technology

Procedure Administrator: Chief Information Officer

Authority: N.J.S.A. 18A: 64-8, N.J.S.A. 2C:20-23, et seq., 16 CFR Part 314, Family Educational Rights and Privacy Act (20 U.S.C. 1232g; 34 CFR Part 99)

Effective Date: December 29, 2018

Index Cross-References: Policy I-55 – Campus Conduct Code; VI-28 - Policy Prohibiting Discrimination in the Workplace

Procedure File Number: 4200

Approved By: Harvey Kesselman, President

Introduction

The Standards set forth below apply to all users of Stockton University computing and communication technology, which includes all email, computing, video, data and telecommunication hardware and software systems owned, leased, granted or used in name, conjunction or association with the University. The Standards also apply to the use of Stockton University computing and communication technology operated on a privately-owned computing device that is not managed or maintained by Stockton University. Use of Stockton University computing and communication technology must be limited to the users' status and function at the University.

Furthermore, users are advised not to consider any of their work, e-mail or electronic communication correspondence on University systems to be private. A violation of any of these Standards may result in revocation of usage privileges and/or appropriate disciplinary action under the University's Campus Conduct Code, and civil liability or criminal prosecution under applicable local, Federal and State laws and regulations (e.g., New Jersey Computer Crimes Act, N.J.S.A. 2C:20-23, et seq.).

The Standards of acceptable use of computer and communication technology follow below along with an explanatory discussion.

Standard 1 - Appropriate Use of Facilities

Authorized use of and access to the University's computing and communication technology is intended and permitted solely to support the legitimate educational, administrative and mission-centered programs of the University.

Discussion - Students may access University computing and communication technology to perform certain administrative functions needed for admission, advising, degree completion, financial aid, registration, residential life, tuition payment, as well as for course-related instructional and approved extra-curricular purposes. Residential students in good standing may access data and telecommunication facilities for personal use subject to this Procedure and related Residential Life policies and procedures. Members of the faculty and staff may access University computing and communication technology for institutionally-recognized or sponsored instructional, grant, or research purposes. Faculty and staff also may access academic and administrative computing technology, as needed, in accordance with their job responsibilities and professional development. However, personal use should be incidental and kept to a minimum. Limited access to computing and communication technology may be granted to users such as alumni, retirees, and other groups sanctioned through the University based upon any usage guidelines established by the University.

Authorization for use of and/or access to computing and communication technology is granted by the Chief Information Officer (CIO) or appropriate University supervisory authority. Authorization for the use of and/or access to administrative computing technology is granted by the Chief Information Officer and the Director or supervisor of the organizational unit that is the recognized custodian of the data for which access is requested. To protect Stockton University computing and communication technology against unauthorized or improper use, and to protect authorized users from the effects of unauthorized or improper usage, the CIO or appropriate University supervisory authority has the right with or without notice, to monitor, record, limit or restrict any user account, access and/or usage of account. Likewise, the CIO or appropriate University supervisory authority may also monitor, record, inspect, copy or remove any data, file or system resources in its sole discretion. As permitted by law, nothing herein shall prevent local, State or Federal law enforcement from monitoring computer usage.

Standard 2 - Appropriate Use of Accounts

Computer accounts or other identifiers used to gain access to computing and communication technology or data may be used only by the individual authorized to use the account or identifier, and only for the purposes for which the account was authorized.

Discussion - Computing and communication technology is not to be used for the preparation or transmission of commercial or personal advertisements, non-University solicitations or promotions, personal monetary gain, unsolicited mass mailings, or for political or religious purposes.

The sharing of passwords or other access tokens by users with other individuals is prohibited. Users shall not disclose the password associated with an account or otherwise make an account, computing or communication system, or data available to others who have not been authorized to use the account, system or data. Users are responsible for all use of resources conducted under their user accounts and/or passwords and are expected to take appropriate safeguards to ensure that their account passwords and/or personal identification numbers (PINs) are private and not disclosed to others. Users shall not capture, decipher or record other users' account information,

passwords, PINs, or keystrokes, nor use or attempt to use another individual's account or personal information.

Standard 3 - Appropriate Use of Accessible Materials

Users shall not create, use, view, transmit, or store materials using the University's computing and communication facilities that violates civil or criminal law.

Discussion - Censorship is not compatible with the values of Stockton University; however, some computers may be dedicated to specific research or teaching missions that limit their use. The University does not limit access to any information based on its content when it meets the standard of legality, and is viewed in a proper time, place, and manner.

Examples of inappropriate use include, but are not limited to: creation, possession, distribution, or transmission of material that is offensive, violent, constitutes child pornography; is obscene or sexually explicit and is unrelated to University-sanctioned work functions or scholarship; annoying or harassing communications (as defined by law); user's participation in, or facilitation of, communications in furtherance of illegal activities; or other material that violates local, State or Federal law.

University computers, computer files, the e-mail system, Internet access and the software furnished to users are to be used for University-related business and/or scholarly activity. The University specifically prohibits the use of computers (including Internet access) and the e-mail system in ways that conflict with any University discrimination policy and procedures including, but not limited to, the policy prohibiting discrimination in the workplace and Title IX. E-mail and Internet access should be used in such a way that all transmissions, whether internal or external, are accurate, appropriate, ethical and lawful. To enforce these standards, computer, Internet and e-mail usage may be monitored by the CIO or appropriate University supervisory authority, including retrieving and reading e-mail messages and other computer files, and monitoring of Internet traffic. Therefore, e-mail messages, and other use of the University's computers, are not confidential, and even though users may be issued a private password or other PIN or private access code to log in to the computer, users should have no expectation of privacy regarding their use of the University's computing and communication technology.

Standard 4 - Reliability and Integrity of Facilities

Users of computing and communication technology shall not knowingly develop, use, or transmit through the University's technology system any programs, data, or technology that interferes with, infiltrates, or damages computing and communication technology, or violates any civil or criminal law.

Discussion – Users of the University's computer and communication technology shall exercise great care to prevent or protect the use of programs or utilities accessed through such technology and shall not engage in actions that interfere with, infiltrate, or damage such technology.

Users shall not engage in any activity that may lead to unauthorized access to systems, accounts, or data on the University's computing and communication technology. Additionally, users shall not attempt to circumvent or subvert system or network security measures. Further, implementing methods that mask network traffic for unauthorized or unlawful purposes is prohibited. Any defects discovered in system security must be reported immediately to the Chief Information Officer.

Standard 5 - Regulations

The University prohibits the use of computing and communication technology, including e-mail, phone, Internet, webpages, or systems with similar functions, to send fraudulent, harassing, obscene, indecent, profane, intimidating, or unlawful messages that are sufficiently severe, pervasive, or persistent, and are objectively offensive as to substantially disrupt or undermine a person's ability to participate in or receive the benefits, services, or opportunities of the University. Additionally, users are prohibited from using electronic communication facilities to access, or attempt to access, remote computing facilities without authorization from the remote site. Users shall in the use of all computing and communication technology, which also includes technology used in name, association or conjunction with the University, adhere to the rules and regulations governing the use of such technology and the University Campus Conduct Code.

Discussion - Use of and access to computing and communication technology, including computing laboratories, computer networks, telephony equipment, and remote facilities accessed through local or wide area networks, shall be used in accordance with the University's policies and procedures and the Campus Conduct Code; and shall maintain a work environment free from discrimination or harassment.

Standard 6 - Proprietary Rights

Users shall respect and observe proprietary rights associated with software, data, and documents.

Discussion - Computer software, documents or files protected by copyright are not to be copied from or into computing facilities, except as permitted by license or law. Additionally, the number of copies and the distribution of copies must adhere to copyright restrictions and/or provisions. Typewritten or machine-readable documents protected by copyright are not to be reproduced or copied, unless permitted by the copyright owner or legally accepted as “fair use”.

Standard 7 - Privacy

Users shall respect the privacy of other users.

Discussion - Users without the authorization of the CIO or CIO’s designee shall not attempt or knowingly seek, provide, view, use, delete, or modify information in, or obtain copies of files or programs belonging to other computer or telephony users without the permission of those users. Searching through non-public directories, libraries, or any other storage media for unauthorized information is prohibited. Further, computer users shall not use the computing and communication technology to plagiarize or claim the intellectual or literary property of others.

Users granted access to administrative data in which individuals are identifiable must respect the confidentiality of the data as well as any Federal or State law. Disclosure of data pertaining to students, for example, shall be in accordance with the Family Educational Rights and Privacy Act (20 U.S.C. 1232g; 34 CFR Part 99) (“FERPA”). Additionally, financial data shall be protected in accordance with Standards for Safeguarding Customer Information, 16 CFR Part 314. Privileged, sensitive, confidential, and/or personally-identifiable information may not be exfiltrated from University systems, shared or transmitted to third parties using email or other means without a fully executed confidentiality and non-disclosure agreement in place approved by the Chief Information Officer.

Any personally identifiable or otherwise confidential data that is stored on personal computers, cloud servers, removable storage devices, or transmitted via email or otherwise electronically transferred must be stored and transferred in a secure manner. (See “[Guidelines for Safeguarding Personally Identifiable and Confidential Information from Unauthorized or Accidental Disclosure](#)” or contact the Office of Information Security.)

Security systems are in place to prevent unwanted or unauthorized access. Any defects or weaknesses discovered in the security systems should be immediately reported to the Chief Information Officer, or appropriate authority in cases not involving facilities or technology under the auspices of Information Technology Services. Under no circumstances shall computer or telephony users, other than authorized system administrators, access or attempt to access system configurations, security programs, or files.

Users of e-mail should be aware that electronic mail is recognized as the equivalent of a formal memorandum. The University's e-mail systems are used to conduct official University business and support the academic and administrative operations of the University. Users of the University's e-mail system must use caution when sending and receiving information that is not intended for disclosure to third parties. E-mail system files and messages can be stored locally or offsite by Information Technology Services and may be backed up by Information Technology Services in alternate methods as a precaution against accidental loss or hardware failure. As such, systems and backups may contain privileged, sensitive, confidential, and/or personally identifiable information. The duplication and/or exfiltration of institutional data containing any of the aforementioned properties is strictly prohibited and may result in the violation of State or Federal law.

The contents of the University's electronic communication systems may be subject to disclosure under a subpoena or other written request pursuant to authorized procedures, including requests made pursuant to the Open Public Records Act (N.J.S.A. 47:1A-1 et seq.). Users should not use email or other University technology for any purpose that may be needed after graduation and/or employment and users should have no expectation of access to such technology after such time.

System administrators, operators and certain authorized staff may be allowed full access to files and programs during development, maintenance, backup/restore operations, or in acting to fulfill assigned University duties or in safeguarding the integrity and reliability of computing and communication technology. Staff members who are authorized such access shall respect the confidentiality of data stored. In the event that unauthorized computer or telephony system use is suspected, the staff member who detects, or is informed of the suspected violation, must notify the Chief Information Officer or appropriate University supervisory authority, as well as the Stockton Police Department. See Standard 8 for additional information.

Standard 8 - System Safeguards

Computing and communication facilities will be safeguarded to maintain the overall integrity and ensure reliability to all users.

Discussion – To protect Stockton University computing and communication technology against unauthorized or improper use, and to protect authorized users from the effects of unauthorized or improper usage, the CIO or appropriate University supervisory authority has the right, with or without notice, to monitor, record, limit or restrict any user account, access and/or usage of account. The University may also monitor, record, inspect, copy or remove any data, file or system resources in its sole discretion. The use of encryption, the labeling of a communication as private, the deletion of a communication or any other such process or action, shall not diminish the University's rights in any manner.

The CIO or appropriate University supervisory authority may regularly review access logs of systems, servers, and networked devices to ensure appropriate, safe, and reliable operation and utilization of University computing and communication technology.

If the Chief Information Officer (CIO) or appropriate University supervisory authority believe that an alleged violation of these Standards or other regulations presents a risk to the integrity and/or the orderly conduct of the operation of the University's computing and communication technology, the user may be subject to restricted access or loss of access to such technology; disciplinary action under applicable University policies and procedures up to and including termination and/or expulsion from Stockton University; and where appropriate, civil and/or criminal liability.

Stockton University reserves the right to update or revise these Standards or implement additional policies and procedures in the future. Users are responsible for staying informed about and compliance with Stockton University policies and procedures regarding the use of computing and communication technology.

Review History:

	Date
Chief Information Officer	12/04/2018
General Counsel	12/19/2018
Cabinet	12/19/2018
President	12/29/2018