Information Technology Department

Security and Acceptable Use Procedures

Table of Contents

1.0 Overview

The focus of this Information Technology *Security and Acceptable Use Procedure (SAUP)* document is to protect Salem Community College faculty, staff and students from damaging or illegal actions whether accidental or intentional. This document is intended to promote and encourage responsible use, while minimizing the potential for misuse and avoiding unnecessary restrictions on users. This document is not intended to prevent or prohibit the authorized use of resources required to meet the mission and the academic and administrative purposes of Salem Community College. The procedures in this document supersede any existing verbal or written agreement, policy, procedure, guideline, or codicil so decreed by any past or present official of SCC.

Effective security can only be accomplished by a team effort involving every faculty and staff member who deals with information systems. It is the responsibility of every computer user to know the contents of this document and to conduct activities accordingly.

Version control of this document is addressed in the Information Technology Department Operations Manual: *IT1 General Procedures*.

2.0 Purpose

The purpose of this document is to outline the acceptable use of computing, communications and information resources at SCC. The rules are intended to protect College resources including College information, equipment, students, faculty and staff.

3.0 Definitions

Information technology resource includes any computer, communication system and information resource, including, but not limited to, means of access, networks, and any data that may reside thereon.

Database is a system intended to organize, store, and retrieve large amounts of data easily. It consists of an organized collection of data for one or more uses. One way of classifying databases involves the type of their contents, for example: bibliographic, document-text, statistical. **Digital databases** are managed using database management systems, which store database contents, allowing data creation and maintenance, and search and other access.

Electronic communications, electronic communication services or electronic communication systems include, but are not limited to, electronic mail, electronic mail address or account, College computer systems, Internet services, voice mail, mobile cell phone or smartphone, audio and video conferencing, and facsimile messages.

The College's **computer systems** include, but are not limited to, any and all College owned, leased, or rented computer hardware, software, databases, telecommunication equipment, telephone and related equipment, and any other system used in connection with College programs.

E-mail means an electronic message transmitted between two or more computers or electronic terminals, whether or not the message is converted to hard copy format after receipt and whether or not the message is viewed upon transmission or stored for later retrieval. E-mail includes electronic messages that are transmitted through a local, regional, or global computer network.

Voice mail means an audio message transmitted telephonically between two or more telephones, whether or not the message is converted to hard copy format after receipt and whether or not the message is heard upon transmission or stored for later retrieval. Voice mail includes telephonic messages that are transmitted through a local, regional or global telephone network.

Cell phone, **mobile phone**, **smartphone**, and **text messaging** means the transmission of voice or text based short message service messages via any College issued portable device used on behalf of the College or for incidental personal use.

Authorization or **authorized** means any person who has expressly received permission from Information Technology Department (ITD) to perform a specific function or service.

Permissions means any authorization granted to any individual on behalf of SCC to access, read, audit, review, edit, or modify any document, report, or computer system or application maintained and controlled by SCC.

Information is data owned, maintained, and managed by the College in any database (or other electronic format) or paper based records.

For the purpose of this document, a **user** is any person who utilizes any SCC information technology resources.

4.0 Scope

This document applies to any user of the College's information technology resources, whether connected from a computer located on or off-campus.

This document applies to the use of all of the College's information technology resources, regardless of the division or department that administers that resource. The chief administrators of divisional/departmental information technology resources may enact additional procedures specific to those resources, provided they do not conflict with the provisions of this or other procedures or laws.

All users are subject to both the provisions of this document, as well as any procedures specific to the individual systems they use.

5.0 Disclaimer

SCC is not responsible for loss of information from computing misuse, malfunction of computing hardware, malfunction of computing software, or external contamination of data or programs. It cannot be guaranteed that, in all instances, copies of critical data will be retained for all systems. It is ultimately the responsibility of computer users to obtain secure backup copies of their own files for disaster recovery.

Both the nature of electronic communications and the public character of the College's business make electronic communications less private than users may anticipate, and confidentiality of electronic communications should not be expected. Users, therefore, should exercise extreme caution in using electronic communications to communicate confidential or sensitive matters. The College has the right to inspect, monitor, or disclose electronic communications which utilize any College-owned equipment. Without prior notice and without consent, the College may perform routine maintenance or system administration of computers and other electronic communications equipment which may result in observation of the contents of files and communications.

Electronic communications that utilize College equipment, whether or not created or stored on College equipment, may constitute a College record subject to disclosure under the *New Jersey Public Records Act* NSJA 47:1A-1 or other laws, or as a result of litigation.

The College cannot guarantee that users will not receive electronic communications they may find offensive, nor can the College guarantee the authenticity of electronic communications received, or that electronic communications received were in fact sent by the purported sender. Users are solely responsible for materials they access and disseminate on the College's electronic communication systems.

6.0 Security and Acceptable Use Procedures

This section defines acceptable use of the College's electronic communication services and computer systems. It does not articulate all permissible and prohibited uses, but is intended to

provide a framework that honors the rights of other users, respects the integrity of the systems, and observes relevant laws, regulations, contractual obligations, and Board of Trustees policies.

6.1 Authorized Use

Access to SCC's information technology resources is a privilege granted to the faculty, staff and students in support of their studies, instruction and duties, and for purposes consistent with the mission of the College. Unauthorized access to the College's information technology resources is not permitted.

The College's computing, communications and information resources are provided for the support of its educational and service goals and the use of such resources for any other purpose is prohibited.

Gaining access to the College's information technology resources does not imply the right to use those resources. The College reserves the right to limit, restrict, or remove access to its information technology resources. It is expected that these resources will be used efficiently and responsibly in support of the mission of the College. All other use not consistent with this document will be considered unauthorized use.

6.2 Information Security and Confidentiality

Users of the College's information security resources are responsible for ensuring the confidentiality and appropriate use of all the data to which they have access by:

1. Ensuring the security of any account issued in one's name; ensuring the security of the equipment where such information is stored or displayed; and
2. Abiding by related privacy rights of students, faculty and staff, concerning the use and release of personal information, as required by law or existing procedures.

The College's electronic communication systems and services are College property. Any electronic mail address or account associated with the College or any department of the College, assigned by the College to individuals, departments or functions of the College, is the property of the College. Authorized College personnel, while performing routine or investigative operations, have access to files, including electronic mail, web browsers information and any other personal or class data stored on College computers. In the event of a sanctioned College forensic investigation, files or electronic mail may be locked or copied to prevent destruction and loss of information.

All users are advised to consider the open nature of information transferred electronically, and should not assume any degree of privacy or restricted access to such information. The College provides the highest degree of security possible when transferring data, but disclaims responsibility if these security measures are circumvented and the information is compromised. Disclosure of confidential information to unauthorized persons or entities, or the use of such

information for self-interest or advantage, is strictly prohibited. Access to non-public institutional data by unauthorized persons or entities is strictly prohibited.

The confidentiality of student and staff information is protected under state and federal law. Any information regarding students or staff that an employee might access in the course of a work assignment through a computer, student file, or other documentation, is to be used strictly to perform the job duties and may only be shared with those who are authorized to have such information. An employee may not change, alter, copy, or divulge any such information unless it is required to carry out a College job assignment.

6.3 Network and System Integrity

In accordance with *New Jersey State Code* § 2C:20-32 and other procedures and laws, activities that threaten the integrity of computer networks or systems are strictly prohibited. This applies to College-owned and privately-owned equipment operated on or throughout College resources. These activities include but are not limited to:

1. Interference with or disruption of computer systems and networks and related services, including but not limited to the propagation of any computer "worm," "virus" and "Trojan Horse."
2. Intentionally or negligently performing an act that places an excessive load on a computer or network to the extent that other users may be denied service or the use of electronic networks or information systems may be disrupted. An example of this activity would be the use of Internet Radio or Peer-to-Peer (P2P) file sharing.
3. Failure to comply with authorized requests from designated College officials to discontinue activities that threaten the operation or integrity of computers, systems or networks.
4. Negligently or intentionally revealing passwords or otherwise permitting the use by others of College-assigned accounts for computer and network access. Individual password security is the responsibility of each user. The user is responsible for all uses of their accounts, independent of authorization.
5. Altering or attempting to alter files or systems without authorization.
6. Unauthorized scanning of ports, computers and networks.
7. Unauthorized attempts to circumvent data protection schemes or uncover security vulnerabilities.
8. Connecting unauthorized equipment to the campus network or computers.
9. Attempting to alter any College computing or network components without authorization or beyond one's level of authorization, including but not limited to bridges, routers, hubs, wiring, and connections.
10. Utilizing network or system identification numbers, accounts or names that are not assigned for one's specific use.
11. Using campus resources to gain unauthorized access to any computer system and/or using someone else's computer without their permission.

12. Providing services or accounts on College computers or via College networks to other users from a personal computer unless required to meet the normal activities of students working as individuals or in collaborative groups to fulfill current course requirements.
13. Registering a Salem Community College IP address with any other domain name or the SCC name.

6.4 Copyright Law, Infringement, and Fair Use

Violations of the rights of any person or entity protected by a copyright, patent, trademark or similar law, or regulation is strictly prohibited. Violations include, but are not limited to, the unauthorized reproduction of any copyrighted material, including but not limited to software, text, images, audio, and video. Also included is the installation, distribution or use of "pirated" software, as well as the display or distribution of copyrighted materials over computer networks without the author's permission.

Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to copyright owner under the Copyright Act*. These rights include the right to reproduce and distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.

The unauthorized distribution of copyrighted material, including unauthorized peer-to peer file sharing, may subject you to disciplinary action as well as civil and criminal liabilities. Upon receipt of an alleged violation of the *Digital Millennium Copyright Act (DCMA),* the Director of Public Safety will notify the user of the claim. If this is a first offense and the user acknowledges a violation of the *SAUP* by admitting to the claim, he/she will be asked to stipulate in writing that he/she will comply with the *SAUP* in the future. If the Director of Public Safety does not receive such an acknowledgement and stipulation within the prescribed time period, or if the user challenges the validity of the claim, the Director of Public Safety will initiate disciplinary proceedings with the requisite office (Human Resources or Student Affairs). A second offense of the *SAUP* will become a part of the user's disciplinary record. Additional violations will result in sanctions that may include fines and/or a disciplinary probation period, expulsion, or termination. The College may suspend the rights of access to the College's network pending the final disposition of the disciplinary matter.

** The "fair use" provisions of the copyright law, section 107 of the U. S. Copyright Law, may permit the reproduction of copyrighted work for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use) scholarship or research.*

6.5 Equal Access to Electronics and Information Technology

In accordance with Section 508 of the *Federal Rehabilitation Act of 1973*, SCC is required to assure that all electronic and information technology purchased, used, and developed by the College is as fully and equally accessible to persons with disabilities as it is to persons without disabilities. Specifically, this applies to products such as telecommunications, video, multi-media, ATMs, copiers, fax machines, computers, software and operating systems, web pages and other instructional materials.

6.6 Web Sites

SCC's web sites are for the sole purpose of supporting the College's academic and service goals. Any other purpose is not allowed.

Official web pages may be created by the College as well as the divisions and departments contained therein. Official web pages must be reviewed for accuracy and appropriateness by the responsible administrator. Official web pages provide a source of communication with the public and the information they provide becomes the legal responsibility of the College. This requirement does not apply to on-line courses or web pages created to supplement course work.

Personal web pages that utilize the College's electronic communication systems and identify the individual as an employee or student of the College are the sole responsibility of the individual, should support the academic, research, and public service mission of the College, and must comply with the provisions of this document. Formal approval is not required for student, staff and faculty personal pages. However, the College reserves the right to remove pages from the Web (under *New Jersey State Code* § 3C:18) if they are deemed inappropriate or deviate from this document. An official home page is the web page that serves as the initial entry point to an institution's web site.

Standards and procedures for the development and maintenance of web pages are established to provide consistency and accuracy of information published on the World Wide Web. All web pages must comply with the requirements listed in the *Federal Rehabilitation Act*, Section 508.

The World Wide Web is a fluid environment that offers access to a wide range of information. While the College assumes full responsibility for the accuracy and appropriateness of official College web pages, the College is not responsible for individual, personal pages. Users who believe the content of a personal page is offensive, obscene, violates College procedures, or is inconsistent with the generally-accepted norms for web page content may register a formal complaint by following the procedures outlined in section 9.0, Reporting Improper Use and Violations.

Links to other web sites contain information that is created, published, maintained, or otherwise posted by organizations independent of the College. The College does not endorse, approve, certify or otherwise guarantee the accuracy of any information at linked web sites.

The College is not responsible for material viewed as a result of individual links or connections.

6.7 Harassment

Harassment of others via electronic methods is prohibited under *New Jersey State Code* § 2C:20-1.1. It is a violation of this document to use the College's information technology resources as a means to harass, threaten, or otherwise cause harm to any individual(s), whether by direct or indirect reference. It may be a violation of this document to use information technology resources as a means to harass or threaten groups of individuals by creating a hostile environment.

6.8 Commercial Use

The College's information technology resources are provided strictly for College business or College fundraising activities. Any use of these resources for unauthorized commercial activities, personal or private financial gain, or otherwise unrelated to the College business is strictly forbidden under *New Jersey State Code* § 2C:25. This includes the unauthorized soliciting, promoting, selling, marketing or advertising products or services, or reselling information technology resources.

6.9 Obscene Material

Distribution of pornography or patently obscene material other than for authorized research or instructional purposes is prohibited under *New Jersey State Code* § 2C:1-12.

6.10 Social Media Procedures

These procedures are intended to guide and enable faculty, staff, students, and alumni who create and administer social networking pages on behalf of the College. They do not pertain to, nor do they constrain, scholarly, academic, or pedagogical use of social media.

The goal of social networking sites is to foster a virtual community for various audiences. Although these sites are outside the direct control of the college, the College maintains an interest in how it is portrayed by them. The College's official Web site remains the central communications vehicle for many of its audiences and should not be neglected in favor of social networking. Rather, social networking should be used to enhance communications with the college's target audiences.

Purpose

For the College as a whole

- To support and enable recruiting, retention, and alumni relations
- To develop virtual communities
- To foster interactivity
- To share information

For academic departments

- To maintain connection to alumni and help foster connections among alumni
- To assist with assessment
- To find opportunities (internships, job leads) for current students

For admissions

- To create community among admitted students
- To assist in yielding students who enroll

For alumni affinity groups such as reunion classes

- To share information, foster attendance, reconnect

Main College Facebook site:

- To push news, keep the College at the top of mind, stay connected
- Friend-raiser (leads to fund-raising)

Basic Privacy

The options for communicating and interacting online are continuously advancing and changing at a fast pace. The College does not closely monitor the use of electronic communications by students, faculty, and staff, as a rule, however it is within each individual community member's best interest to be aware of issues related to privacy online. These guidelines have been established to assist individual users in making good decisions to protect themselves.

1. Be familiar with privacy options on social networking sites, e-mail, blogs, etc.
2. Set appropriate privacy guards for your personal comfort level.
3. Be aware that no privacy option protects you 100 percent from personal information being shared beyond desired boundaries. Information shared online, even with the highest privacy settings (including e-mails intended for a specific individual or individuals), cannot be protected.

4. Be aware that information posted online may be perceived differently depending on the viewer despite intended effect or outcome.

Usage by student and alumni organizations and campus offices

The College recognizes that student organizations, alumni organizations, and campus offices may use various online media to communicate, promote, and inform others about their programs, services, and activities. Groups choosing to use online services need to be aware that they are using the College's name and that this can impact the image and reputation of specific individuals, the group, and the college.

Photo Guidelines

Photos posted on social networking should be done so with the utmost care. Nothing posted online is private, and photos should be regarded as such. The following guidelines should be used when posting photos:

- Photos of children should not be posted without expressed consent from the parents. Even then such photos should be avoided.
- Care should be taken not to post photos of individuals who would object. This may involve obtaining the appropriate permissions.
- Photos posted on social networking sites must be appropriate. As a guideline, they should be photos that could be posted on the College's official Web site. Examples of photos that should be avoided include but are not limited to: photos involving alcohol, nudity, medical and hospital patients, and graphic scenes.
- Appropriate photo credits should be given. Social networking sites still represent the College and any agreed-to credits must be maintained.

Copyright

Beware that intellectual property may be protected by copyright. Newer copyright statements allow creative but non-commercial uses. One website that provides content (including music and images) that may be used in this way is www.creativecommons.org.

7.0 Procedures Compliance

The Chief Technology Officer is authorized by the President to ensure that the appropriate processes to administer the procedures are in place.

The Chief Technology Officer, or designee, will ensure that suspected violations receive the proper and immediate attention of the appropriate College officials and the appropriate law enforcement authorities, if applicable.

The Chief Technology Officer or designee will inform users about the procedures; receive and respond to complaints; collect and secure evidence as required; advise and assist on the interpretation, investigation and enforcement of these procedures; consult with legal counsel on matters involving interpretation of law or requests from outside entities; and maintain a record of each incident and its resolution.

8.0 Violation of Procedures

Violation of these procedures may result in disciplinary action. Additionally, inappropriate use of information technology resources may result in criminal, civil, and other administrative liability.

9.0 Reporting Improper Use and Violations

Improper use and suspected violations of this document should be reported to ITD via e-mail at abuse@salemcc.edu. This email list includes representatives from Human Resources, ITD, and Campus Security. Violations can also be reported via telephone to the ITD Help Desk.

10.0 Document Review and Practices Oversight

The Chief Technology Officer, or designee, is responsible for application and enforcement of this document and will review this document on an annual basis, or when the need arises, make recommendations for any changes and provide oversight and periodic review of the practices used to implement this document. A current version of this document will be posted on the SCC web site. A printed copy will be available at the Library and the ITD Help Desk.

11.0 Equipment & Media Disposal Procedures

The disposal of media, computer equipment and computer software can create information security risks for SCC. These risks are related to the potential unauthorized release of sensitive or confidential information, violations of software license agreements, and unauthorized disclosure of intellectual property that might be stored in hard disks and other storage media.

11.1 Purpose

The purpose of this section is to establish the security procedures for the disposal of all data-containing media, including the disposal, storage, transfer or sale of computer equipment.

11.2 Deletion of Old Information

Employees are required to delete information from their computers if it is clearly no longer needed or potentially useful. Use of an "erase" feature (e.g., putting a document in a trash can

icon) is not sufficient for sensitive information because the information may still be recoverable. Sensitive information must be deleted via an overwrite program that is available from ITD. Contact the Help Desk for assistance.

11.3 Media Disposal

Prior to disposal, storage media including floppy disks, CDs, zip disks, hard drives, and tapes containing sensitive information must be destroyed or properly disposed of. This may be accomplished by returning the media to ITD for destruction or by contacting Administrative Services to coordinate the removal of these items by the College's confidential media and document disposal company. All hardcopy containing sensitive information must be disposed of via a shredder or sent to ITD for destruction. Storage media may not be donated to charity or otherwise recycled unless they have first been subjected to a "zero-ization" (wipe/obliteration) process approved by ITD.

11.4 Equipment Disposal or Servicing

Before computer or communications equipment is sent to a vendor for servicing, all sensitive information must be removed. Likewise before any computer or communications equipment is marked for trade-in, disposal, donation or long-term storage, all sensitive information must be destroyed. Contact the Help Desk or ITD for assistance.

11.5 Photocopiers and Photocopies

Administrative Services handles all copier devices for the College. All waste copies of sensitive information that are generated in the course of copying, printing, or other sensitive information handling must be destroyed according to the instructions found in this document. If a copy machine jams or malfunctions when employees are making copies of sensitive information, the involved employee should make a reasonable attempt to retrieve the information before leaving the machine. Photocopiers have hard drives that retain College information even after copies are made. Before return or disposal of copier machines, ITD should be consulted to determine if the leasing or reclaiming firm has cleared the hard drive of College data.

12.0 Acceptable Use Agreement — Employee

Salem Community College provides broad access to its computing, communications and information resources. These resources support the delivery of the College's academic mission and accordingly, they must be used responsibly. These resources include the physical data communications network and all computers, printers, scanners and other hardware attached to that network, as well as all system software, telephone systems, and means of access to the Internet.

With regard to the computing, communications and information resources of Salem Community College, it is understood and agreed that:

- Salem Community College's computing, communication and information resources are provided for the support of its educational and service goals and the use of such resources for other purposes is prohibited. However, incidental personal use not during standard business hours is permissible so long as: (a) it does not consume more than a trivial amount of system resources, (b) it does not interfere with productivity of other campus employees, and (c) it does not preempt any College activity. The College and its employees are to abide by these procedures along with any local, state, and federal law that may apply. All users are subject to both the provisions of these procedures, as well as any procedures specific to the individual systems they use.
- The confidentiality of student and staff information (including social security numbers) is protected under federal and state law and/or regulations. Any information regarding students or staff that an employee might access in the course of a work assignment through a computer, student file, or other documentation, is to be used strictly to perform job duties and may only be shared with those who are authorized to have such information. Employees may not change, alter, copy, or divulge any such information unless it is required to carry out a job assignment. Employees will use secure means to transmit confidential data inside or outside of the College. Electronic mail is not a secure means to deliver information.
- To protect the integrity of computing resources, passwords, access codes, or account names must not be shared with others. Additionally, passwords may be subject to complexity requirements and employees will be required to change their passwords periodically.
- Employees are not allowed to install any software on any campus computer without express consent from ITD.
- Most educational materials (both commercial and employee created, including software) are protected under copyright. Any violation of the rights of a person or entity protected by copyright law is prohibited. The unauthorized duplication, installation, or distribution of computer software utilizing the College's computing, communications and information resources is specifically prohibited. Unauthorized

software installed on College owned computers will not be supported and may be removed if deemed necessary. Employees may not connect any system or install software which could allow any user to gain access to the College's system and information without written approval from the Chief Technology Officer or his/her designee.

- Employees may not use Salem Community College resources for conducting a private business or for personal financial gain.
- Distribution of pornography or patently obscene material other than for authorized research or instructional purposes is prohibited. The definition of "pornography" and "obscene" shall be as determined by law.
- Employees found in violation of the College's computer use procedures, are subject to proper disciplinary action, including the reporting of such activity to the appropriate authorities as required by law, and if serious enough, may result in termination.
- Employees must consider the open nature of information transferred electronically, and should not assume an absolute degree of privacy or restricted access to such information. The College provides the highest degree of security possible when transferring data, but disclaims responsibility if these security measures are circumvented and the information is compromised.
- Salem Community College is not responsible for loss of data, time delay, system performance, software performance, or any other damages arising from the use of College computing resources. Employees are encouraged to secure backup copies of their own files – this is recommended in addition to the routine nightly backup of server-based data.
- Authorized College personnel may, while performing routine or investigative operations have access to data, including electronic mail, web browser information, and any other personal data stored on College computers. However, the College may allow an employee's supervisor access to a College computer in an employee's absence to conduct normal College business. Neither the College nor any employee shall disclose the contents of observed personal data to any other person or entity except as required by law or Board Policy.
- Activities that place excessive strain on network resources, (i.e. net radio, other similar streaming media, online gaming or Peer to Peer (P2P) file sharing) are not allowed without written approval from the Chief Technology Officer or his/her designee. Students are encouraged to review all Salem Community College's computer procedures at our web site http://salemcc.edu/it. Access to our web site is available to all students at the Library and via the Internet.
- To ensure the integrity and reliability of computer and communications resources, employees are encouraged to report improper use and violations of these procedures.

Selected Examples of Unacceptable Use:

- Revealing passwords to others, allowing someone else to use your account.

- Utilizing network or system id numbers/names that are not assigned for one's specific use on the designated system.
- Attempting to authorize, delete, or alter files or systems not created by oneself without proper authorization from the Chief Technology Officer or his/her designee.
- Watching Internet videos or listening to Internet radio on your computer without authorization from the Chief Technology Officer.
- Violations of the Digital Millennium Copyright Act through Peer-to-Peer file sharing.
- Failure to comply with IT Procedures.
- Attempting to defeat data protection schemes or to uncover security vulnerabilities.
- Connecting equipment to the campus network without written approval from the Chief Technology Officer or his/her designee. (Devices such as PDAs, printers, and USB drives that connect to a computer and not directly to the network are acceptable.)
- Registering a Salem Community College IP address with any other domain name.
- Unauthorized network scanning or attempts to intercept network traffic.
- Harassing or threatening other users of the campus network.

By accessing Salem Community College computing, communication, and information resources, you agree to be bound by these terms. These terms are subject to change. Updated versions of this and other related documents will be made available http://salemcc.edu/it. If you do not agree with these terms, or with future changes to these terms, you must discontinue all use of applicable College resources. A violation of these terms may result in civil, criminal, or other administrative action.

13.0 Acceptable Use Agreement — Student

Salem Community College provides broad access to its computing, communications and information resources. These resources support the delivery of the College's academic mission and, accordingly, they must be used responsibly. These resources include, but are not limited to, the physical data communications network and all computers, printers, scanners and other hardware attached to that network, as well as all system software, access to the Internet and other communication tools.

As a user of the computing, communications and information resources of Salem Community College, I understand and agree that:

- Salem Community College's computing, communication and information resources are provided for the support of its educational and service goals and the use of such resources for any other purpose is prohibited.
- Students are to abide by this and all campus-wide computer use procedures, along with any local, state, and federal law that may apply. College divisions or departments can enact additional procedures specific to their need. All users are subject to both the provisions of these procedures, as well as any procedures specific to the individual systems they use.
- Students must not share their passwords, access codes or account names with others and will comply with any applicable password complexity requirement.
- Most software is operated under copyright from various software developers. This software is only to be used on campus for school related business. Any violation of the rights of a person or entity protected by copyright law, including, but not limited to, the unauthorized duplication of copyrighted software, is prohibited.
- Students are not allowed to install any software on any campus computer.
- Distribution of pornography or patently obscene material other than for authorized research or instructional purposes is prohibited.
- Student workstations are subject to monitoring. Computer screens, particularly those accessing the Internet, may be periodically viewed to monitor compliance with procedures.
- Students found in violation of the College's computer use procedures, including, but not limited to, the use of its resources for any unauthorized or illegal activity, such as the destruction or alteration of data, attempts to bypass security systems or obtain or alter passwords, disruption of service or any form of harassment of users, malicious introduction of a computer virus or any disrupting activity, are subject to proper disciplinary action, including, as required by law, the reporting of such activity to the appropriate authorities.
- Authorized College personnel may, while performing routine or investigative operations have access to data, including electronic mail, web browser information and any other personal or class data stored on College computers.

- Activities that place excessive strain on network resources, i.e. net radio, other similar streaming media, online gaming or Peer to Peer (P2P) file sharing are not allowed. Students may not use Salem Community College resources for conducting a private business or for personal financial gain. Paying College fees and making purchases from the SCC systems are examples of acceptable use. Students are encouraged to review all Salem Community College's computer procedures at our web site http://salemcc.edu/it. Access to our web site is available to all students at the Library and via the Internet.
- To ensure the integrity and reliability of computer and communications resources, students are encouraged to report improper use and violations of these procedures.

Selected Examples of Unacceptable Use:

- Revealing passwords to others, allowing someone else to use your account, or using someone else's account to access resources.
- Unauthorized attempts to delete or alter others files or systems.
- Violations of the Digital Millennium Copyright Act through Peer-to-Peer file sharing.
- Failure to comply with IT Procedures.
- Attempting to defeat data protection schemes or to uncover security vulnerabilities.
- Connecting unauthorized equipment to the campus network.
- Harassing or threatening other users of the campus network.

By accessing Salem Community College computing, communication, and information resources, you agree to be bound by these terms. These terms are subject to change. Updated versions of this and other related documents will be made available at http://salemcc.edu/it. If you do not agree with these terms, or with future changes to these terms, you must discontinue all use of applicable College resources. A violation of these terms may result in civil, criminal, or other administrative action.