

## 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 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 Guidelines along with any local, state, and federal law that may apply. All users are subject to both the provisions of these Guidelines, as well as any guidelines 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 permitted to install any software on any campus computer without written approval 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 Dean of Collegiate Services 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 guidelines, 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, or online gaming) are not permitted without written approval from the Dean of Collegiate Services or his/her designee.
- Employees can use personal computing assets (to include, but not limited to: laptops, external hard drives, thumb drives, tablets, smartphones) with the express written consent of the Dean of Collegiate Services (via Help Desk request). If the employee does use a personal computing asset, by virtue of the use for College business, the following conditions must be met:
  - The equipment is registered with the ITD help desk.
  - SCC anti-virus software is installed where applicable and never disabled.
  - A personal firewall is installed where applicable and never disabled.
  - Full disk encryption is installed where applicable and never disabled (this includes all external drives).
  - The employee consents to the devices being added to any SCC mobile device management system used by the ITD to track and/or remotely wipe the device.
  - The employee consents to the device being reviewed for compliance at any time while use on the College network.
  - The employee consents that the College data on the device is the property of SCC and must be made available for copy or backup upon request.
  - Personal equipment that is used to access the SCC network falls under the same rules and regulations as College-owned equipment.
  - The College may revoke the use of personal equipment on our network at any time, with or without cause.

- Employees are encouraged to review all Salem Community College's computer policies at our website <http://salemcc.edu/it>.
- To ensure the integrity and reliability of computer and communications resources, employees are encouraged to report improper use and violations of these Guidelines.

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 Dean of Collegiate Services or his/her designee.
- Watching Internet videos or listening to Internet radio on your computer without authorization from the Dean of Collegiate Services.
- Failure to comply with IT Guidelines.
- Attempting to defeat data protection schemes or to uncover security vulnerabilities.
- Connecting any equipment (per BYOD guidelines) to the campus network or computers without written approval from the Dean of Collegiate Services or his/her designee.
- 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 at <http://salemcc.edu/it>. If you do not

agree to 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.

Employee Signature: \_\_\_\_\_

Employee Name (PRINT): \_\_\_\_\_

Title/Division: \_\_\_\_\_

Supervisor Signature: \_\_\_\_\_

Dean Signature: \_\_\_\_\_