Administrative Guideline 1101

ADMINISTRATIVE GUIDELINE TYPE: Information Technology
ADMINISTRATIVE GUIDELINE TITLE: Employee/ Student / Public Technology Usage Guideline

DEPARTMENT RESPONSIBLE: Information Technology
GUIDELINE STATEMENT OF PURPOSE: Employee/ Student / Public Technology Usage Guideline

I. Statement of Purpose

This guideline outlines the acceptable use of Southeastern Community College's (SCC) technical resources. Personally Owned Devices (POD) connected to SCC's technologies and network are also subject to this guideline. SCC's technical resources are the sole property of SCC.

II. Users Governed

This guideline applies to credit and non-credit students, employees, alumni and SCC guests.

III. Resources Covered

This guideline governs the use of technical resources including, but not limited to:

A. Computers (i.e. desktops, laptops, tablets, smartphones, future devices)
B. Networks (Wired and wireless)
C. SCC Web site and associated web pages
D. Social Media (i.e. Facebook, Twitter, and future applications)
E. Telephony (i.e. Voice over IP, voice messaging system, SCC mobile phones)
F. Printers
G. Hardware
H. Digital Media (USB, DVD, CD, SD, online, etc.)
I. Software and Applications (i.e. email, storage)
J. (BYOD) Bring Your Own Device (Tablets, Smartphones, Laptops, etc.)

IV. Access as a Privilege

The use of SCC technologies is a privilege, not a right. Any inappropriate use of said technologies can result in the loss of those privileges. Examples of prohibited uses are listed in section VIII of this guideline and are strictly enforced.

V. Responsibility of Users

Technology users must abide by federal, state and local laws as well as College guidelines. The user bears the primary responsibility for the communication/information that he or she chooses to access, send, or display. The user shall respect the rights of others by complying with all college polices, guidelines, and procedures. It shall be each user's personal responsibility to recognize (attribute) and honor the intellectual property of others. SCC recognizes and adheres to U.S. and international copyright laws and software licenses.

The faculty or staff supervising the use of technical and network resources has the authority to enforce student adherence to this guideline. The supervising employee may issue a warning to users. This warning should be considered as a guide to users to assist them in the correct use of SCC's technical and network resources.

Academic freedom is paramount to SCC's mission as an institution of higher learning, SCC promotes openness to new ideas, sensitivity to multicultural issues and unlimited access to a wide range of information and ideological perspectives.

Each individual is responsible for their technical activities. Individuals who intentionally misuse technical resources, including but not limited to those available at SCC, may be subject to:

A. Students - disciplinary actions outlined in the SCC Judicial Codes and Appeals and any applicable federal, state and local laws.
B. Employees – disciplinary actions consistent with federal, state and local laws and College guidelines.
C. Guests – disciplinary actions consistent with federal, state and local laws and access privileges subject to the discretion of Executive Director of Information Technology Services (ITS).

VI. Security and Privacy of Users

Confidentiality of technical communications is not guaranteed. Therefore, all users should exercise caution when accessing or sending personal, confidential or sensitive information. Southeastern Community College will not impose any undue restraints on communications other than those imposed by applicable Federal, State, or local laws, including laws regarding the right to privacy and laws which prohibit defamatory material or copyright infringement.

Security and system performance requires the SCC ITS department to routinely log and monitor technical resources and activity. SCC values the confidentiality of information and does not monitor individual communication without reasonable cause. Be advised, an Iowa Open Records Law request may require SCC to access specific public data on a College owned computer or POD connected to the wired or wireless network.

VII. Technology users are expected to:

A. Use resources in a manner consistent with federal, state and local laws.
B. Use resources in a manner consistent with SCC's mission, vision and values.
C. Implement security practices to prevent unauthorized access to technical resources. Use only technical resources that you are authorized to use and use them for the purposes for which they were intended. Do not let others use your user name or password. It is the responsibility of the user to lock/log off, ensuring other users are not able to access your account and information.
D. Assist in supporting the integrity of technology resources by taking measures to support the security and privacy of network resources.
E. Immediately report any security incident to the Executive Director of ITS.
F. Support an educational environment free from harassment and discrimination as described in the SCC student handbook and affirmative action plan.
G. Priority of technical resources is given to users for the completion of academic activities.
H. Abide by the instructor's syllabi and/or program handbook in reference to POD usage during scheduled classes and labs.
I. Students may access computers in libraries, open labs and kiosks during non-scheduled class times. Computers located in classrooms should not be accessed unless permission is provided by the instructor or college staff.
J. Use technology resources appropriately so as to not interfere with the educational mission of the institution or the daily business of the College.
K. Employees should adhere to SCC's security guidelines and ensure that confidential information is encrypted at all times. Examples include, but are not limited to, data stored on any mobile device,

email communication, cloud storage, etc.

VIII. Examples of Prohibited Use:

A. Using resources to harass or disseminate mass communication. (i.e. email, social media)
B. Allowing others to use your user name or password is prohibited.
C. Using the campus network to gain unauthorized access to any computer systems.
D. Knowingly running, installing or giving another user a program intended to damage or to place files on another user's account/system without their knowledge.
E. Attempting to monitor or tamper with another user's electronic communications. Reading, copying, changing or deleting another user's files or software without the explicit permission of the owner.
F. Capturing passwords or data on the network not meant for you.
G. Modifying or extending SCC network services beyond the area of intended use. This applies to all network wiring, wireless, hardware and in-room jacks.
H. Intentionally accessing, downloading, or printing illegal material.
I. Reproducing, distributing or displaying copyrighted materials without prior permission of the owner.
J. Students using PODs without instructor permission during schedule classroom/lab time.

IX. Due Process

Activities which are criminal under federal, state, or local law will be reported to the appropriate authorities. Criminal and non-criminal abuses of computer access and network privileges may result in a warning, suspension, or termination of computer and network resources and disciplinary action to include possible termination of employment.

Serious or repeated infractions of this guideline may be referred to the appropriate Dean/Vice President for action under the College's Judicial Codes and Appeals. Actions taken against students may include any sanctions listed in the Judicial Codes and Appeals including suspension or termination of computer and network privileges as well as possible expulsion from the College.

X. Disclaimer

SCC shall not be held responsible for any illegal, negligent, or harmful actions as a result of inappropriate use of college internet, email, or network resources. In addition, SCC is not responsible for content downloaded from external web sites and networks.

SCC will not be responsible for any damages or loss of data experienced by those using computing equipment, facilities and network services.

Information Technology Services will provide troubleshooting assistance to users who experience technical issues on Southeastern Community College equipment and services only; instruction in the use of computers or particular software applications is not their responsibility.

XI. References

A. Administrative Guideline 1102 – BYOD (In progress)
B. Administrative Guideline 1111 - Ellucian Security Access

C. Administrative Guideline 1114 - Employee Guidelines for Securing Confidential Data
D. Administrative Guideline 1115 - Employee Guidelines for Securing Mobile Technologies
E. Administrative Guideline 1116 - Employee Guidelines for Reporting Security Incidents
F. SCC's Mission, Vision and Values - this information can be accessed on the SCC Web site under "About SCC" and "Institutional Effectiveness".
G. SCC Student Handbook