BUSINESS SERVICES
ACCEPTABLE USE OF COLLEGE COMPUTING RESOURCES
CHAPTER 2 Board of Trustees Approval: 03/27/2013
POLICY 17.01

I. POLICY

Salt Lake Community College's (SLCC) computing resources are provided for the use of the College's Authorized Users in support of its instructional programs, learning activities, and administrative activities. Computing resources are to be used in support of the mission of the College. College computing resources are public resources, and as such they may not be used for personal profit and/or gain, or for the promotion of non-college sponsored commercial ventures. Unacceptable use of computer resources as defined by the College is prohibited. Computing resources are owned and/or operated by SLCC, and all rights to these services may be terminated without notice. SLCC does not endorse all transmissions through the SLCC network.

I. REFERENCES

A. All Relevant SLCC Policies

B. Civil Rights Act of 1964 42 U.S.C 21

C. Education Amendments of 1972 20 U.S.C. 20 U1681-1688

D. United States Copyright Act 17 U.S.C 101-810

E. Family Educational Rights and Privacy Act 20 U.S.C. 1232g; 34 CFR Part 99

F. Electronic Privacy Act 18 U.S.C. 2510–2522

G. Authority to Promulgate Policies and Procedures, U.C.A. 76-8-708

H. Damage to Records, U.C.A. 76-8-412, 413

I. Vandalism on Campus, U.C.A. 76-8-703,705,706

J. Federal Trade Commission, Identity Theft Rules; 16 C.F.R. Part 681

K. Utah Code Title 76 Utah Criminal Code Chapter 10 Section 1201, 1203, 1204, 1205, 1206

L. Utah Code Title 76 Utah Criminal Code Chapter 5 Section 106.5

M. Utah Administrative Code Rule R477-15

N. Government Records Access and Management Act Utah Code Title 63G Chapter 2

O. Government Records Access and Management Act Utah Code Title 63G- Chapter

P. State of Utah Executive Order 1993. Standards and Procedures on Sexual Harassment Prevention

Q. Higher Education Opportunity Act 2008 P.L 110-315

II. DEFINITIONS

A. Computer Resources: Computer resources include the computing hardware, network hardware, software, cabling and telecommunications, and all computing peripherals owned or leased by the College and used in the conduct of College business, regardless of location of these resources. Also included are computer resources which are entrusted to the College by other organizations

B. Computer System Administrators: Any person with the authority and/or responsibility for granting permission to ~~users~~ Authorized Users for the use of computer resources at the College.

C. Copyrighted Materials: Any material protected by United States or internationally accepted copyright laws.

D. Harassing Conduct: Conduct evaluated as demeaning or hostile as defined by federal and state laws regarding harassment.

E. Hostile Educational Environment: A hostile educational environment is established when harassing conduct is sufficiently severe, pervasive, or persistent so as to interfere with or limit the ability of an individual to participate effectively and positively in their role at the College.

F. Authorized User: Employees, students, volunteers, alumni, contractors or any other person who maintains an official relationship with the College and has been granted rights to use computer resources by a computer system administrator.

G. Confidential information: Includes personally identifiable information such as, but not limited to student, ~~faculty~~ or ~~staff~~ employee home address or phone number, ~~SSN~~ Social Security Number, S number, driver license number, financial information such as financial aid or payroll information, benefit information, medical information, personal status information such as marital status, race, religion, disability, and any other personally identifiable information that should not be disclosed to the public.

H. Government Records Access Management Act (GRAMA): GRAMA defines what a record is and establishes the criteria for accessing government records. All outside entity access to College records should be through a request to the SLCC GRAMA officer.

I. Pirated: to reproduce without authorization especially in infringement of copyright law.

J. Computing Device: An end user device that is used to access information resources

K. Media: any device that can store data. Examples CD,DVD,USB flash drives, external hard drives

L. Mobile Computing Device: a computing device that has its own power source and is carried from place to place.

III. PROCEDURES

A. General Use and Ownership

1. While SLCC's Office of information technology (OIT) administration desires to provide a reasonable level of privacy, Authorized Users should be aware that the data they create on the College's systems remains the property of SLCC or under the guardianship of SLCC. Because of the need to protect SLCC's computing resources, the College cannot guarantee the confidentiality of information stored on any network device belonging to SLCC or removable devices left by Authorized Users.

2. In conjunction with this policy, Authorized Users are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible to manage personal use of information systems. Employees should be guided by departmental guidelines in conjunction with this Policy but not to contradict this Policy on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

3. For security and computing resource maintenance purposes, authorized individuals within SLCC may monitor computing resources at any time.

4. SLCC reserves the right to audit computing resources on a periodic basis to ensure compliance with this policy.

B. Security, Proprietary Information and Privacy

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by the Ethical Conduct Policy, details of which can be found in Human Resources policies.

2. Keep passwords secure and do not share accounts. Authorized Users are responsible for the security of their passwords and accounts. System level passwords should be changed every six months; user level passwords will be changed based on OIT Password Procedure. If a system or network administrator leaves all system level passwords will be changed.

3. All computing devices should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the computing device will be unattended, unless exempt by OIT.

4. Because information contained on computing devices are especially vulnerable, special care should be exercised.

    a) Password Protection: Any computing device that access SLCC's information or systems must require a unique username and password, password, or other security authentication upon startup and after inactivity.

    b) Operating System's Firewalls should be enabled before accessing the Internet.

    c) Storage of Sensitive Information: Sensitive information should be stored on a SLCC approved secure server and only accessed from a mobile computing device. Mobile computing devices that store sensitive information will be required to be encrypted, including any attached storage devices to end users computing device.

    d) Physical Security: Appropriate physical security measures should be taken to prevent theft of mobile computing devices and media. This would include not leaving a computing device or media in plain sight in a vehicle or unattended in a public place.

    e) Lost or Stolen Devices: Theft of a computing device or media should be reported to SLCC Department of Public Safety and SLCC Information Security Office. If possible the lost or stolen mobile computing device will be

remote wiped.

f) Antivirus and Anti-malware: All computing devices must use a functioning and up to date antivirus and anti-malware program, unless otherwise stated by OIT.

5. Postings by employees from a SLCC email address to Social Media should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of SLCC, unless posting is in the course of business duties.

6. All computing devices accessed by Authorized Users that are connected to the SLCC Internet/Intranet/Extranet, whether or not owned by the Authorized Users, shall be continually executing approved virus-scanning software with a current virus database unless overridden by OIT.

7. Authorized Users must exercise extreme caution when opening e-mail attachments received from unknown senders, which may contain malicious code.

8. Any computing resource that could have contained confidential information, when retired from service must be handled following the procedures of the Office of Risk Management for records destruction.

9. Employee files (including e-mail) are records defined and processed according to the Government Records Access and Management Act (GRAMA). Consequently, files may be subject to inspection through the College GRAMA officer. In such cases, the College GRAMA officer has authority to inspect files to determine which portions may be exempt from disclosure. Non-public files will be safeguarded as though they were confidential to the maximum extent possible.

C. Unacceptable Use

The following activities are, in general, prohibited. OIT Staff may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances are Authorized Users to engage in any activity that is illegal under local, state, federal or international law while utilizing SLCC computing resources.

If any misuse of any SLCC computing resources is observed report the misuse to the Information Security Office infosec@slcc.edu

The lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of pirated or other software products that are not appropriately licensed for use by SLCC.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, movies and the installation of any copyrighted software for which SLCC or the end user does not have an active license is strictly prohibited.

3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The Information Security Office should be consulted prior to export of any material that is in question.

4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, malware, etc.).

5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

6. Using a SLCC computing resource to actively engage in procuring or transmitting material that is in violation of Rule R477-15 Workplace Harassment.

7. Using SLCC's computing resource to cause a hostile education environment, inside and outside the classroom environment are prohibited.

8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the Authorized Users are not an intended recipient or logging into a server or account that the Authorized User are not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

10. Port scanning or security scanning is expressly prohibited unless prior notification to OIT is made.

11. Executing any form of network monitoring which will intercept data not intended for the Authorized Users' computing device, unless this activity is a part of the faculty, staff, students, alumni or third-parties' normal job/duty.

12. Circumventing user authentication or security of any computing resource.

13. Interfering with or denying service to anyone other than the Authorized User's computing resource (for example, denial of service attack).

14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's computing resource, via any means, locally or via the Internet/Intranet/Extranet.

15. The viewing of pornography in a public setting is in violation of Utah Code Annotated, Title 76 Chapter 10 Offenses Against Pubic Health, Safety, Welfare, and Morals Sections 1201, 1203, 1204, 1205, 1206.

D. Email and Communications Activities

The following activities are strictly prohibited:

1. Sending unsolicited email messages, including the sending of spam or other advertising material to individuals who did not specifically request such material.

2. Any form of harassment, including cyber-bullying, via email, telephone, paging, or any other form of communication whether through language, frequency, size of messages or content. Utah Code Title 76 Chapter 5 Section 106

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Use of unsolicited email originating from within SLCC's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by SLCC or connected via SLCC's network.

7. Emailing personal identifiers in clear text is prohibited.

E. Enforcement

Any Authorized User found to have violated this policy may be subject to disciplinary action set forth in the Student Code of Conduct or by the Human Resources Department. In such cases, the full range of disciplinary sanctions is available, including not only the loss of computer use privileges, but dismissal from the College, and legal action. Conduct that violates this policy and procedures may constitute a criminal offense