SECTION: 1. GENERAL

SUBJECT: APPROPRIATE USE POLICY FOR TECHNOLOGY

Subject: Appropriate use for technology

Background: The purpose of this policy is to discuss proper use of LCSC's technology within a collaborative and collegial campus environment.

Point of Contact: Director of Information Technology

Other LCSC offices directly involved with implementation of this policy, or significantly affected by the policy: IT executive steering committee, the President, the Provost, the Vice President for Finance & Administration

Date of approval by LCSC authority: 3/14/19

Date of State Board Approval: NA

Date of Most Recent Review: March, 2019

Summary of Major Changes incorporated in this revision to the policy: Reviewed with no changes.

1. Introduction

Information technology resources are valuable assets provided to enhance the core functions of Lewis-Clark State College. The use of the college's information technology resources is a privilege extended by the institution to authorized users for the purpose of teaching, learning, research, service, and administration. This **APPROPRIATE USE POLICY FOR TECHNOLOGY** governs the use of the college's information technology resources in an atmosphere that encourages free exchange of ideas and an unwavering commitment to academic freedom. The college community is based on principles of honesty, academic integrity, respect for others, and respect for privacy, and respect for property. The college seeks to:

- Protect the confidentiality and integrity of electronic information and privacy of its users, to the extent required or allowed under federal and Idaho state law;
- Ensure that the use of electronic communications complies with the provisions of college policy and state and federal law; and
- Allow for the free exchange of ideas and support of academic freedom.

Since the college cannot protect users from the Internet presence of materials they may find offensive, such materials must not be represented or construed as being approved by the college.

This policy applies to all students, staff, and others while they access, use, or handle Lewis-Clark State College's technology resources. In this policy, the term "users" includes – but is not limited to – subcontractors, visitors, visiting scholars, potential students, research associates, grant and contract support personnel, media representatives, guest speakers, and all other non-college entities granted access. The assumption of the college is that all users of campus technology are familiar with this policy.

SECTION: 1. GENERAL

SUBJECT: APPROPRIATE USE POLICY FOR TECHNOLOGY

2. General Policy

A. All users are expected to act in a responsible, ethical, and lawful manner when accessing the college's information technology resources.
B. The college's information technology resources are provided for use in conducting authorized college business. Using these resources for personal gain, illegal, or obscene activities is prohibited.

(1) The prohibition against using the college's information technology resources for personal gain does not apply to:

(a) Scholarly activities, including the writing of textbooks or preparation of other teaching materials by faculty members.
(b) Consulting and other activities that relate to the faculty member's professional development or as permitted under college policy.

(2) The state of Idaho allows some personal use of these resources, except when such use:

(a) Is excessive or interferes with the performance of the user's college responsibilities;
(b) Results in additional incremental cost or burden to the college's information technology resources;

(c) Violates any state or federal law;
(d) Is prohibited by a college department’s imposition of further restrictions on personal use.

C. Users observing any illegal activities should report their observance to LCSC’s administration. Although not an inclusive list, examples include theft, fraud, gambling, copyright infringement, illegal file sharing, audio or video piracy, hacking, and viewing or distributing of pornographic images and videos.
D. Abuse of networks or computers beyond the college through the use of LCSC's information technology resources will be treated as an abuse of the college's information technology resource privileges.
E. State law prohibits the use of college resources for campaign or political advertising on behalf of any party, committee, agency, or candidate for political office. This prohibition does not forbid use of college resources to discuss or examine political topics or issues of public interest so long as the use of college resources does not advocate for or against a particular party, committee, agency, or candidate.

3. Prohibited Activities

SECTION: 1. GENERAL

SUBJECT: APPROPRIATE USE POLICY FOR TECHNOLOGY

A. All users are expected to act in a responsible, ethical, and lawful manner when using the college's information technology resources. The following examples – although not exhaustive -- are prohibited activities.

(1) The use of the college's information technology resources to attempt unauthorized use or interference with the legitimate use by authorized users of non-LCSC computers or networks, including misrepresentation of his or her identity to other networks (e.g., IP address "spoofing");

(2) Modification or reconfiguration of the software, data, or hardware of the college's information technology resource (e.g., system/network administration, internal audit, key logging) without appropriate authorization or permission;

(3) Creating, installing, executing, or distributing any malicious code (including but not limited to viruses, worms, key logger, and spyware) or any other surreptitiously destructive program on any of the college's information technology resource, regardless of the result;

(4) "Hacking" (attempting to gain access to unauthorized areas) into college computers, applications, or networks. (***Note****: This activity may be subject to prosecution by state or federal authorities. LCSC will notify law enforcement immediately upon detection of any network or system intrusion.*);

(5) Copyright infringement not covered in legislation aimed at educational institutions, including the illegal possession or sharing of:

(a) video files,
(b) digital audio, and/or
(c) writings;

(6) Using a electronic equipment attached to college resources to capture data packets;

(7) Launching *denial of service* attacks against other users, computer systems, or networks;

(8) Use of the college's information technology resources to transmit abusive, threatening, or harassing material, chain letters, SPAM, or communications prohibited by Idaho or federal laws;

(9) Knowingly interfering with the security mechanisms or integrity of the college's information technology resources. Users shall not attempt to circumvent information technology protection schemes or exploit security loopholes;

(10) Connecting electronic devices (switches, routers, hubs, computer systems, key loggers, and wireless access points as examples) to the college network that are not approved by the Information Technology department;

(11) Intentionally physically damaging or disabling college computers, networks, or software without authorization.

(12) Removing any computer component or equipment from LCSC's campus without prior approval of the Information Technology department or the relevant division representative.

4. Department and Division Responsibilities

A. Each departmental unit is responsible for security on its computer systems and may apply more stringent security standards than those detailed here. However, any elaboration of constraints must follow the principles and rules in this policy statement as a minimum standard, or risk losing connectivity to the college's networks and/or use of its resources.
B. There are situations where departments and divisions have employees who administer LCSC systems. Even though these system administrators are not within the organization umbrella of the Information Technology department, they are still responsible for ensuring that appropriate security is enabled and enforced in order to protect the college's resources and personal data.
C. System administrators not employed in the Information Technology department must remain familiar with the changing security technology that relates to their computer systems and continually analyze technical vulnerabilities in relation to security implications. Stored authentication data (e.g., password files, encryption keys, certificates, personal identification numbers, and access codes) must be appropriately protected with access controls, encryption, shadowing, etc.

5. Remediation

A. Abuse of college policies, resources, or abuse of other sites through the use of information technology resources may result in termination of access, disciplinary review, expulsion, termination of employment, legal action, and/or other appropriate disciplinary action. Notification will be made to the appropriate college office (*e.g., appropriate office for student conduct matters, human resources, general counsel, campus security*) or external law enforcement agencies.
B. The Information Technology department is authorized to isolate and/or disconnect computer systems from the network while assessing any suspected or reported security incident in order to minimize risk to the rest of the college's network.

6. Software Licensure

A. If software includes a license agreement that details restrictions on its use, the college expects employees and/or students to follow the provisions in the license agreements regarding copying, improvements, number of concurrent users, and similar provisions.

B. License agreements differ among software publishers. It is important that users read and understand the license agreement for each software package.

C. Questions about computer software use not addressed by this policy or questions about specific license agreements should be directed to Information Technology department.

D. Each department is responsible and accountable for maintaining records on the license information for the software that it has purchased. The maintenance of records and information related to centrally provided software is the responsibility of the organization that provides it and subject to internal audit review for compliance.

7. Privacy

A. The college has no generic interest in tracking electronic mail, reading digital files, or monitoring patterns of digital behavior. However, since all resources are owned by the state of Idaho and made available for employment purposes, there should be no expectation of privacy of information stored on or sent through college-owned information technology resources and communications infrastructure.

B. The college reserves the right to preserve or inspect any information transmitted through or stored in its computers, including e-mail communications stored in the cloud and individual login sessions. No notice will be forthcoming when:

(1) There is reasonable cause to believe the user has violated or is violating this policy, any campus or institute guideline or procedure established to implement this policy, or any other college policies;

(2) A college account appears to be engaged in unusual or unusually excessive activity;

(3) It is necessary to do so to protect the integrity, security, or functionality of the college's information technology resources or to protect the college from liability; or

(4) The college receives a legal subpoena for specific information.