BOARD OF EDUCATION UMPQUA COMMUNITY COLLEGE DOUGLAS COUNTY, OREGON	___ Information Item _X_ Action Item
Subject: Second Reading Policy	Date: Oct. 14, 2020

Second Reading Policy:

Old #	New #	Title	Addendum Page #
348	3720	Computer and Network use	1

The associated administrative procedure is shared as an information item:

Old #	New #	Title	Addendum Page #
348	3720	Computer and Network use	2-6

See Board Packet Addendum for 2nd reading policy and procedure

Recommendation by:	Approved for Consideration:
Lorynne Wilgus	Debra Thatcher

UMPQUA COMMUNITY COLLEGE

BOARD POLICY

TITLE: COMPUTER AND NETWORK USE

BOARD POLICY # 3720

This policy seeks to ensure that users of the College's Information Technology Resources:

1. Respect the rights of all students, faculty, and staff.
2. Ensure that technology services are available when needed.
3. Protect the College from harm that may result in misuse.

Students, employees, and visitors who use **Umpqua Community College** "Information Technology Resources" have a responsibility not to abuse those resources and to respect the rights of others. These resources include computers, electronic devices, networks, electronic communications systems such as the College's email and voice mail.

The College's procedures shall provide guidelines to students, employees, and visitors for the appropriate use of information technology resources. The procedures shall require users to respect software copyrights and licenses, respect the security and integrity of computer-based, information resources, refrain from engaging in or allowing others to engage in unauthorized access, comply with the College's anti-discrimination and anti-harassment policies, and respect the rights of other computer users.

Non-compliance with any of the provisions of this policy or the related administrative procedures may subject the user to sanctions including removal of privileges, disciplinary action, and/or potential legal liability or criminal prosecution.

RESPONSIBILITY:
The Director of Information Technology is responsible for implementing and updating this policy. Specific guidance for policy implementation may be found in the associated Administrative Procedure(s).

NEXT REVIEW DATE:
DATE OF ADOPTION:
DATE(S) OF REVISION:
DATE(S) OF PRIOR REVIEW:

UMPQUA COMMUNITY COLLEGE

ADMINISTRATIVE PROCEDURE

TITLE: Computer and Network Use

ADMINISTRATIVE PROCEDURE # 3720

RELATED TO POLICY # 3720 Computer and Network Use

A. APPLICATION

This Administrative Procedure applies to all students and employees of the College, as well as visitors who use the College's facilities ("users"), and it applies to all information technology resources of the College. "Information technology resources" means the College's computers and other electronic equipment and devices, including mobile devices and facsimile machines, and networks and electronic communications systems including internet, email, and voice mail.

B. OWNERSHIP AND NON-PRIVACY

1. The College's information technology resources are provided to students and employees to assist with the College's business activities, student educational activities, and visitors. These resources remain the property of the College, including all information that is accessed, transmitted or stored in or on these systems. It is important to understand that users have ***no reasonable expectation of privacy*** in information that is accessed, transmitted or stored in or on these systems.

2. The College reserves the right to monitor and record the usage of college computing resources as necessary to evaluate and maintain system efficiency and security. Users should also be aware that all information on electronic office equipment, network storage devices, or personal computers ***is a public record,*** if the content of the information would be a public record in any other format. As such, it is subject to disclosure under the public records law. Only authorized Information Technology staff members may access, monitor, or audit equipment, systems, networks, network traffic, or specific usage.

C. OVERVIEW OF ACCEPTABLE USE

1. The College's information technology resources should be used for legitimate instructional, research, or administrative purposes, and only by employees, students and visitors who have been authorized by the College for such use. Users

shall be individually responsible for the appropriate use of their computer, account, and any IT resource assigned to them, and for exercising good judgement regarding the reasonableness of incidental personal use.

2. The College's general standards of ethical and appropriate conduct apply to the use of the information technology resources. Users must also comply with all federal, state and other applicable laws; all applicable college rules and policies; and all applicable contracts and licenses. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.

D. COMPLYING WITH THE COLLEGE'S NON-DISCRIMINATION AND NON-HARASSMENT POLICIES

The College's Information Technology Resources may not be used for transmitting, accessing, viewing, retrieving, displaying or storing any communications or content of a sexual, discriminatory or harassing nature, or conduct that is otherwise prohibited by the College's policies and procedures against discrimination, harassment and retaliation. This includes communications or content with derogatory or inflammatory material about an individual's race, age, disability, religion, national origin, physical attributes or sexual preference, as well as abusive, profane or offensive language. If a user receives a communication from a third party that is prohibited by this section, the user must promptly advise the sender that the conduct violates the College's standards and should stop immediately.

E. CONFIDENTIAL INFORMATION

Employees must be aware that a greater degree of caution is required when transmitting confidential information on the computer system. Confidential information may only be accessed and used as specifically required to perform your job duties. Confidential information should never be transmitted or forwarded to outside individuals or companies who are not authorized to receive that information, nor should such information be transmitted or forwarded to other employees at the College who do not need to know the information. Always use care in addressing e-mail messages and ensure that any mailing lists are current to avoid inadvertently sending confidential information to the wrong person.

F. SECURITY AND INTEGRITY OF SYSTEMS

Employees and students shall:

1. Secure and lock, or log off, all unattended devices.
2. Not leave mobile devices that contain controlled sensitive data unattended.

3. Promptly report the loss of mobile devices, or any other media containing controlled sensitive data, immediately (or as soon as possible).
4. Promptly report the theft, loss, or unauthorized disclosure of the College proprietary information and/or IT resources.
5. Promptly Report any defects discovered in systems security to the IT help desk at 541-440-7808 or email helpdesk@umpqua.edu.
6. Use extreme caution when opening attachments in email or text messages (or other electronic files) received from unknown senders.
7. Make a reasonable effort to protect their passwords and to secure IT resources against unauthorized use or access. Specifically, writing down passwords (even if stored out of public view) or storing in plain text in a computer file are violations of this policy.

Employees shall also use an authorized encryption process when sending emails containing controlled sensitive data from an Umpqua.edu email address to an outside email address.

G. COMPLIANCE WITH COPYRIGHT LAWS

All users shall observe all applicable federal and state intellectual property laws and regulations, including copyright, trade secret, trademark, and any similar laws governing the use of intellectual property. This includes the following:

1. Users shall access, use, or share the College's proprietary information only to the extent authorized for their specific usage.
2. Users shall not install "pirated" or other software products that are not licensed for use by the College.
3. Users shall abide by the terms of any licenses, contracts, or agreements into which they or the College have entered regarding the use of intellectual property.
4. Users shall not copy or export College software or technical information without written authorization from the College's Information Technology personnel.

Employees and students may use copyrighted or otherwise legally restricted materials as permissible under "fair use" and other essential exemptions from copyright law (e.g.: classroom exemption). However, it is the responsibility of the user to understand these exemptions and ensure their particular usage falls within legal parameters. If you have questions regarding "fair use" exemptions, you should contact Director of Information Technology for clarification ***before*** engaging in the conduct.

H. OTHER PROHIBITED CONDUCT

Users shall not:

1. Perform any unauthorized upgrades, modification, or repairs to any College computer, workstation or other equipment, or install any unauthorized software, including upgrades on any College computer or equipment.
2. Physically remove IT resources from the College premises for personal use.
3. Use IT resources for uses that are inconsistent, incompatible, or in conflict with State or Federal law or other the College policies.
4. Intentionally or carelessly disrupt the computing environment or obstruct the work of other users.
5. Engage in malicious behavior, including but not limited to:

    a. Installation of hardware devices or the development, download, or use of software or other methods with the intent to gain unauthorized access to IT resources, disrupt other computer or network users, or damage or degrade the performance, software, or hardware components of IT resources.

    b. Introduction of malicious software into the network, or in any other way cause security breaches or disruptions of network communication.

    c. Circumvention of user authentication or the security of any host, network, or account.

    d. Interference with or denial of service to any user.

6. Share their passwords, or otherwise provide access to their the College credentials, with another individual.

7. Use their the College credentials for personal purposes. When creating personal accounts with non-licensed websites (such as Facebook, Netflix, or Twitter) or other third party entities, users shall not:

    a. Use their the College User-ID/Password pair as their account login to personal accounts; or

    b. Store controlled sensitive data in personal accounts.

8. Use another user's College credentials, attempt to capture or guess another user's the College credentials, or otherwise attempt to access another user's the College account.

9. Network or use programs that create “Peer to Peer” computing.

10. Engage in Commercial Use. The College information resources should not be used for commercial purposes. Users also are reminded that the “.cc” and “.edu” domains on the Internet have rules restricting or prohibiting commercial use, and users may not conduct activities not authorized within those domains.

11. Use any email accounts other than @umpqua.edu for College business or College communication. This includes communication to students.

I. VIOLATIONS AND ENFORCEMENT

1. The College strictly prohibits use of the College’s computers, electronic equipment, or any electronic communications systems to engage in any communications that are in violation of any College policy or procedure, or state or federal law. We consider misuse of our computer, electronic, telephonic and e-mail systems to be a serious matter.

2. Violations of this policy will be grounds for disciplinary action, up to and including termination of employment or expulsion. The College also reserves the right to advise appropriate legal officials of any potentially unlawful violations, as the College deems appropriate. If you have any questions regarding this policy, please contact the Director of Information Technology.

RESPONSIBILITY:
The Director of Information Technology is responsible for implementing and updating this procedure.

NEXT REVIEW DATE:
DATE OF ADOPTION:
DATE(S) OF REVISION:
DATE(S) OF PRIOR REVIEW: