Southwestern Oregon Community College

AP 3720 Computer and Network Use

This procedure is designed to state the acceptable use of computer systems, networks, and other Integrated Technology resources at Southwestern Oregon Community College.

The College community is encouraged to make use of Information Technologies in support of educational and administrative purposes. The College supports access to information with numerous views for the interest, information, and enlightenment of students, faculty, and staff.

Consistent with this document, the College supports the use of Integrated Technology resources in a manner that recognizes both the rights and the obligations of academic freedom.

The College's computer and network systems are the sole property of Southwestern Oregon Community College. They may not be used by any person without the proper authorization of the College. The Computer and Network systems are for College instructional and work-related purposes only.

This procedure applies to all College students, faculty, and staff and to others granted use of College information resources. This procedure refers to all College information resources whether individually controlled or shared, stand-alone or networked. It applies to all computer and computer communication equipment owned, leased, operated, or contracted by the College. This includes personal computers, workstations, mainframes, minicomputers, and associated peripherals, software and information resources, regardless of whether used for administration, research, teaching, or other purposes.

Conditions of Use
Individual departments within the College may define additional conditions of use for information resources under their control. These statements must be consistent with this overall procedure but may provide additional detail, guidelines, or restrictions.

The College cannot protect individuals against the receipt of potentially offensive material. Those who use electronic communications occasionally may receive material they might find offensive. Those who make personal information available about themselves through the Internet or other electronic media may expose themselves to potential invasions of privacy.

Integrated Technology resources are provided to support the College's scholarly, educational, and administrative activities. Integrated Technology resources are limited, and should be used wisely and with consideration for the rights and needs of others. Unless written proof of need for scholarly activities can be provided, transmission or display of pornography is expressly prohibited.

Legal Process
This procedure exists within the framework of the College's board policy and state and federal laws. A user of College information resources who is found to have violated any of these policies will be subject to disciplinary action up to and including but not limited to loss of information resources privileges; disciplinary suspension or termination from employment or expulsion; or civil or criminal legal action.

Copyrights and Licenses

Computer users must respect copyrights and licenses to software and other on-line information.

- Copying - Software protected by copyright may not be copied except as expressly permitted by the owner of the copyright or otherwise permitted by copyright law. Protected software may not be copied into, from, or by any College facility or system, except pursuant to a valid license or as otherwise permitted by copyright law.
- Number of Simultaneous Users - The number and distribution of copies must be handled in such a way that the number of simultaneous users in a department does not exceed the number of original copies purchased by that department, unless otherwise stipulated in the purchase contract.
- Copyrights - In addition to software, all other copyrighted information (text, images, icons, programs, etc.) retrieved from computer or network resources must be used in conformance with applicable copyright and other law. Copied material must be properly attributed. Plagiarism of computer information is prohibited in the same way that plagiarism of any other protected work is prohibited.

Integrity of Information Resources

Computer users must respect the integrity of computer-based information resources.

- Modification or Removal of Equipment - Computer users must not attempt to modify or remove computer equipment, software, or peripherals that are owned by others without proper authorization.
- Unauthorized Use - Computer users must not interfere with others access and use of the College computers. This includes but is not limited to: the sending of chain letters or excessive messages, either locally or off-campus; printing excess copies of documents, files, data, or programs, running grossly inefficient programs when efficient alternatives are known by the user to be available; unauthorized modification of system facilities, operating systems, or disk partitions; attempting to crash or tie up a College computer or network; and damaging or vandalizing College computing facilities, equipment, software or computer files.
- Unauthorized Programs - Computer users must not intentionally develop or use programs which disrupt other computer users or which access private or restricted portions of the system, or which damage the software or hardware components of the system. Computer users must ensure that they do not use programs or utilities that interfere with other computer users or that modify normally protected or restricted portions of the system or user accounts. The use of any unauthorized or destructive program will result in disciplinary action as provided in this procedure, and may further lead to civil or criminal legal proceedings.

Unauthorized Access

Computer users must not seek to gain unauthorized access to information resources and must not assist any other persons to gain unauthorized access as outlined below. (This is not an exhaustive list).

- Abuse of Computing Privileges - Users of College information resources must not access computers, computer software, computer data, or information, or networks without proper authorization, or intentionally enable others to do so, regardless of whether the computer, software, data, information, or network in question is owned by the College. For example, abuse of the networks to which the College belongs or the computers at other sites connected to those networks will be treated as an abuse of College computing privileges.

- Reporting Problems - Any defects discovered in system accounting or system security must be reported promptly to the appropriate system administrator so that steps can be taken to investigate and solve the problem.
- Password Protection - A computer user who has been authorized to use a password-protected account may be subject to both civil and criminal liability if the user discloses the password or otherwise makes the account available to others without permission of the system administrator.
- Usage - Computer users must respect the rights of other computer users. Attempts to circumvent these mechanisms in order to gain unauthorized access to the system or to another person's information are a violation of College procedure and may violate applicable law.
- Unlawful Messages - Users may not use electronic communication facilities to send defamatory, fraudulent, harassing, obscene, threatening, or other messages that violate applicable federal, state or other law or College policy, or which constitute the unauthorized release of confidential information.
- Commercial Usage - Electronic communication facilities may not be used to transmit commercial or personal advertisements, solicitations or promotions (see Commercial Use, below). Some public discussion groups have been designated for selling items by socctalk and may be used appropriately, according to the stated purpose of the group(s).
- Information Belonging to Others - Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, or passwords belonging to other users, without the permission of those other users.
- Rights of Individuals - Users must not release any individual's (student, faculty, or staff) personal information to anyone without proper authorization.
- User identification - Users shall not send communications or messages anonymously or without accurately identifying the originating account or station.
- Political, Personal, and Commercial Use - The College is a non-profit, tax-exempt organization and, as such, is subject to specific federal, state and local laws regarding sources of income, political activities, use of property and similar matters.
- Political Use - College information resources must not be used for partisan political activities where prohibited by federal, state, or other applicable laws.
- Personal Use - College information resources should not be used for personal activities not related to College functions, except in a purely incidental manner. If the College otherwise grants access to email system for personal use, employees may use the college's email system to engage in protected concerted activity during non-work time.
- Commercial Use - 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.

Prohibited Use
The following behaviors are prohibited while using College Integrated Technology resources, including computers and networks owned or operated by the College, or to which the College is connected:
1. Modifying system or network facilities, or attempting to crash systems or networks;
2. Using personal software on College computers without written authorization from the Office of Integrated Technology and Services;
3. Using network resources which inhibit or interfere with the use of the network by others.

4. Using, duplicating or transmitting copyrighted material without first obtaining the owner's permission, in any way that may reasonably be expected to constitute an infringement, or that exceeds the scope of a license, or violates other contracts;
5. Tampering with software protections or restrictions placed on computer applications or files;
6. Using College Integrated Technology resources for personal for-profit purposes;
7. Subverting restrictions associated with computer accounts;
8. Using Integrated Technology resources to obtain unauthorized access to records, data, and other forms of information owned, used, possessed by, or pertaining to the College or individuals;
9. Accessing another person's computer account without permission. Users may not supply false or misleading data, or improperly obtain another's password in order to gain access to computers or network systems, data or information. Obtaining access to an account name or password through the negligence or naiveté of another is considered to be a specifically prohibited use;
10. Intentionally introducing computer viruses, worms, trojan horses, or other rogue programs into Integrated Technology resources that belong to, are licensed to, or are leased by the College or others;
11. Physically damaging Integrated Technology resources;
12. Using, or encouraging others to use, Integrated Technology resources in any manner that would violate this or other College policies or any applicable state or federal law; and
13. Falsely reporting or accusing another of conduct that violates these rules without a good faith basis for such an accusation;
14. Intentional transmission or display of unwanted messages, information, or graphic images which create a hostile school or work environment for the recipient are inappropriate uses of College computer resources;
15. Allowing non-approved users access to information on the College network that do not have a legitimate need and right to know specific information; and
16. Sharing or allowing others to use your logon and password.
17. Connecting networking equipment including, but not limited to servers, routers, hubs and switches, and wireless access points to the campus network without written authorization from the Office of Integrated Technology and Services.

Nondiscrimination

All users have the right to be free from any conduct connected with the use of Southwestern's network and computer resources which discriminates against any person on the basis of national origin, religion, age, gender, gender identity, gender expression, race, color, medical condition, genetic information, ancestry, sexual orientation, marital status, physical or mental disability, military and veteran status, and pregnancy. No user shall use the College network and computer resources to transmit any message, create any communication of any kind, or store information which violates any College procedure regarding discrimination or harassment, or which is defamatory or obscene, or which constitutes the unauthorized release of confidential information.

- **No Expectation of Privacy -** The College reserves the right to monitor all use of the college network and computers to assure compliance with these policies. Users should be aware that they have no expectation of privacy in the use of the College network and computer resources. The College will exercise this right only for legitimate College purposes, including but not limited to ensuring compliance with this procedure and the integrity and security of the system.

- **Possibility of Disclosure** - Users must be aware of the possibility of unintended disclosure of communications.
- **Retrieval** - It is possible for information entered on or transmitted via computer and communications systems to be retrieved, even if a user has deleted such information.
- **Litigation** - Computer transmissions and electronically stored information may be discoverable in litigation.
- **Dissemination and User Acknowledgment**
- All users shall be provided copies of these procedures and be directed to familiarize themselves with them.
- All users shall acknowledge and agree to this procedure stating that they have read and understand this procedure and will comply with it. This acknowledgment shall be in the form as follows:

Computer and Network Use Agreement
During Employee Onboarding and New Student Orientation:
I have read the College Computer and Network Use Procedures and recognize and understand the guidelines. By using the college computer and network resources, I agree to abide by the standards set in the procedures for the duration of my employment or enrollment. I am aware that violations of this Computer and Network Usage Procedure may subject me to disciplinary action, including but not limited to revocation of my network account up to and including prosecution for violation of state or federal law.

At computer or network login:
I have read the College Computer and Network Use Procedures and recognize and understand the guidelines. By using the college computer and network resources, I agree to abide by the standards set in the procedures for the duration of my employment or enrollment.

References:
    15 U.S. Code Sections 6801 et seq. ;
    17 U.S. Code Sections 101 et seq.;
    16 Code of Federal Regulations Parts 314.1 et seq. ;
    Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37, 45;
    NWCCU Standard 2.H.2
    ORS 341.290(4)

Approved: December 2, 2020