



<b>Administrative Policy:</b>		Technology Acceptable Use Policy		<b>Policy Number:</b>	AP 3720
<b>Applicable regulations - Federal/State/Board/College</b>		ORS 341.290 NWCCU Standard 2.G.5			
<b>Accountable Administrator:</b>		Chief of Finance & Operations	<b>Position responsible for updates:</b>	IT Manager	
<b>Original Date:</b>	12/16/2019	<b>Executive Team approval date:</b>		07/07/2020	
<b>Date Posted on Web:</b>	09/21/2020	<b>Revised:</b>		<b>Reviewed:</b>	

The College Computer and Network systems are the sole property of Oregon Coast 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 policy applies to all College students, faculty, and staff and to others granted use of College information resources. This policy refers to all College information resources whether individually controlled or shared, stand-alone or networked. It applies to all computer and computer communication facilities 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**

Functional units within the College may define additional conditions of use for information resources under their control. These statements must be consistent with this overall Policy but may provide additional detail, guidelines, or restrictions.

**Training and Cybersecurity** - Use of College information resources may be contingent upon initial training, and periodic retraining in usage protocols. This requirement is in place to minimize exposure to risk through accidentally downloaded malware, irresponsible browsing, and even unauthorized personal devices. Access may be limited or denied in the event of repeated failure to follow College cybersecurity guidelines and/or complete required trainings.

**Public Access** - Oregon Coast Community College makes available public access workstations for use by College students, faculty, staff, and members of the public. The Acceptable Use Policy applies to the use of these workstations (including printers) wireless and all information technology resources of the College as defined in this policy. Public access computing resources are intended to be used for educational purposes and the legitimate business of the College in accordance with applicable policies and laws, and in a manner consistent with public trust. Appropriate use of public access workstations includes instruction, study, research, and personal enrichment. Limits on printing will be posted and enforced. Users shall be considerate of their use of shared resources and refrain from monopolizing

workstations. During peak periods of use, educational use has priority. Inappropriate uses include interfering with the work of others, wasting resources, using the resources for private economic purposes, gambling, and any activities that include the violation of state or federal laws and College policies and procedures. Obscenity and child pornography are prohibited by law.

## **Legal Process**

This Policy 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 functional unit does not exceed the number of original copies purchased by that functional unit, 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 Policy 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.

**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 Policy 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.

**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.

**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.

## **Nondiscrimination**

All users have the right to be free from any conduct connected with the use of Oregon Coast Community College network and computer resources which discriminates against any person on the basis of race, color, religion, national origin, sex, marital status, disability, veteran status, age, sexual orientation, or any other status protected by federal, state, or local law in any area, activity or operation of the College. The College also prohibits retaliation against an individual for engaging in activity protected under this policy and interfering with rights or privileges granted under anti-discrimination laws. 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 Policy regarding discrimination or harassment, or which is defamatory or obscene, or which constitutes the unauthorized release of confidential information.

## **Disclosure**

**No Expectation of Privacy** - The College reserves the right to monitor all use of the College network and computer 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 policy 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 faculty and staff shall be provided a copy of this policy and will acknowledge the receipt of this policy. Students will be provided a copy of this policy at the start of each term. This policy will be provided to public access users at computing stations.