COCC Acceptable Use of Information Technology Resources

Central Oregon Community College (COCC) supports an environment of learning and sharing of information through the acquisition and maintenance of computers, computer systems, networks, and associated computing resources and infrastructure. COCC computing resources and facilities of COCC and are intended to support the College's missions, administrative operations and activities, student and campus life activities, and the free exchange of ideas and information between the College and the greater community in which it operates.

Personal use of COCC computing resources may be permitted if it does not interfere with the College's or the employee's ability to carry out College business, and does not violate the terms of this policy. The use of College computing resources is subject to the generally accepted tenets of legal and ethical behavior within the College community. COCC computing resources system shall not be used for material or activities that reasonably could be considered harassing, obscene, or threatening by the recipient or another viewer.

This policy applies to all users of college computing resources, whether affiliated with the College or not, and to all use of those resources, whether on campus or from remote locations.

Basic Terms and Conditions of Use:

- Users do not own accounts on College computers, but are granted the privilege of exclusive use. Users may not share their accounts with others, and must keep account passwords confidential.
- Users may only access those computing resources to which they are authorized to use and use them only in the manner and to the extent authorize. Users must refrain from unauthorized viewing or use of another person's computer files, programs, accounts, and data.
- It is a violation of this policy to attempt (even if unsuccessful) to gain unauthorized access by circumventing system security, uncovering security loopholes, guessing passwords/access codes, or through any fraudulent means
- COCC cannot guarantee that messages or files are private or secure. COCC may monitor and record usage to enforce its policies; any information gained in this way may be used in disciplinary and civil and/or criminal legal proceedings; or to respond to a public record request for files which are deemed public records under public records laws.
- Users must adhere strictly to software licensing agreements and copyright laws; all generally 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. The unauthorized publishing or use of copyrighted material on College IT systems is prohibited and users are personally liable for the consequences of such unauthorized use. For more information on Copyright Enforcement at COCC please go to: http://its.cocc.edu.
- It is a violation of this policy to load any third-party software on computer systems in the computer labs or other public computers, unless authorized by the college.

- When accessing remote systems from COCC systems, users are responsible for obeying the policies set forth herein as well as the policies of other organizations.
- Users must not intentionally or negligently use computing resources in such a manner to degrade system performance or capability, or cause network congestion; or damage systems, software or intellectual property of others.
- It is a violation of this policy to use College IT resource for commercial, political, or illegal purposes; personal financial gain; or harassment of any kind. This includes, but is not limited to, the use of College electronic mail systems for "broadcasting" of unsolicited mail or for any purpose prohibited by state or federal laws.
- It is a violation of this policy to: give or publish a password, identifying code, personal identification number or other confidential information about a computer, computer system, network or e-mail account, database, or any other College IT resource, unless authorized by the ITS department for legitimate purposes.
- It is a violation of this policy to intentionally and without authorization: access, modify, damage, destroy, copy, disclose, print, or take possession of all or part of any computer, computer system, network, software, data file, program, database, or any other College IT resource.
- Misuses of COCC computing, networking, or information resources may result in the immediate loss of computing and/or network access, and may lead to further disciplinary action as well.
- Any violation of this policy or of any local, state, or federal law may be referred to appropriate COCC offices and/or, as appropriate, law enforcement authorities.

Provisions for Private Computers and Devices Connected to the College Network

The following apply to anyone connecting a private computer or electronic device (e.g. tablet, iPad, smart phone, etc.) to the College network via a wireless LAN connection, a dial-up network connection, a virtual private network (VPN) connection, a regular network connection in an office, or any other network connection.

1. The owner of the computer or device is responsible for the behavior of all users on the device, and all network traffic to and from the device, whether or not the owner is aware of the traffic generated.
2. A private device connected to the network may not be used to provide network access for anyone who is not authorized to use the College systems. The private device may not be used as a router or bridge between the College network and external networks.
3. Should ITS staff have any reason to believe that a private device connected to the College network is using College resources inappropriately, if justified, the system will be disconnected from the network, and action will be taken with the appropriate authorities.
4. Users are responsible for the security and integrity of their systems. Where a personal device is "compromised" the user shall either shut down the system or remove it from the campus network as soon as possible to stop the attack from spreading.
5. The following types of devices should never be connected to the College network by anyone outside of ITS staff: DNS, DHCP, BOOTP, WINS, or any other server that manages network addresses as well as RADIUS, LDAP, AD, or any other server that provides authentication services.