

ACCEPTABLE USE OF COMPUTING RESOURCES

ADMINISTRATIVE RULE NUMBER: B007

LAST APPROVED: July 02, 2013, January 15, 2015, January 2017

RELATED TO POLICY SERIES NUMBER: 211

REFERENCE: ORS 339.351 TO 339.364 AND ORS 164.377

OVERVIEW: B007.1

Computing resources at the College are made available to assist with work related tasks. Remember that professionalism extends to all communications, use, and interactions with and on computing resources. If any of the following are found or seen occurring, please notify your supervisor or the IT Department.

The wireless infrastructure is made available to the College Community as a courtesy. It is not designed nor should it be construed as being part of the College's infrastructure. As such it is each person's responsibility to govern their activities while checking College email on their personal devices such as cell phones, laptops and iPads or similar devices. All following rules apply whether on College owned resources or personal devices.

The unauthorized use of resources is prohibited and, in many cases, may be violations of the law. Unauthorized use includes, but is not limited, to the following types of activities.

A. Harassment or threats to specific individuals, or a class of individuals:

- a. Transmitting unsolicited information that contains obscene, indecent, lewd, or lascivious material or other material which explicitly or implicitly refers to sexual conduct.
- b. Using e-mail, newsgroups, or other social media to threaten or stalk someone.
- c. Transmitting unsolicited information that contains profane language or panders to bigotry, sexism, or other forms of prohibited discrimination.

B. Interference or impairment to the activities of others:

- a. Creating, modifying, executing, or retransmitting any computer program or instructions intended to: (a) obscure the true identity of the sender of electronic mail or electronic messages, such as the forgery of electronic mail or the alteration of system or user data used to identify the sender of electronic e-mail; (b) bypass, subvert, or otherwise render ineffective the security or access control measures on any network or computer system without the permission of the owner; or (c) examine or collect data from the network (e.g., a "network sniffer" program).

ACCEPTABLE USE OF COMPUTING RESOURCES

ADMINISTRATIVE RULE NUMBER: B007

LAST APPROVED: July 02, 2013, January 15, 2015, January 2017

RELATED TO POLICY SERIES NUMBER: 211

REFERENCE: ORS 339.351 TO 339.364 AND ORS 164.377

- b. Allowing unauthorized persons or organizations to use user computer accounts or TBCC network resources. Users are responsible for the appropriate use of all College computer access and accounts assigned them and must take all reasonable precautions, including password maintenance and file protection measures, to prevent unauthorized use. Users must not share passwords with anyone else or provide access to network resources to unauthorized persons. Student wireless access is available for all students and guests at the college.
- c. Communicating or using any password, personal identification number, credit card number, or other personal or financial information without the permission of its owner.

C. Unauthorized access and use of the resources of others:

- a. Use of College computer resources to gain unauthorized access to resources of this or other institutions, organizations, or individuals.
- b. Use of false or misleading information for the purpose of obtaining access to unauthorized resources.
- c. Accessing, altering, copying, moving, or removing information, proprietary software or other files (including programs, libraries, data, and electronic mail) from any network system or files of other users without prior authorization (e.g., use of a "network sniffer" program).
- d. Making unauthorized copies of copyrighted materials. Users should assume all software, graphic images, music, and the like are copyrighted. Copying, downloading, or peer-to-peer file sharing of copyrighted materials without the authorization of the copyright owner is against the law, and may result in civil and criminal penalties, including fines and imprisonment.

D. Damage or impairment of College resources:

- a. Use of any resource irresponsibly or in a manner that adversely affects the work of others. This includes intentionally, recklessly, or negligently (a) damaging any system (e.g., by the introduction of any so-called "virus," "worm," or "Trojan-horse" program), (b) damaging or violating the privacy of information belonging to others, (c) misusing or allowing misuse of system resources, or (d) physical damage of units
- b. Use of College resources for non-College related activities that unduly increase network load (e.g., non-business or -education related email, chain

ACCEPTABLE USE OF COMPUTING RESOURCES

ADMINISTRATIVE RULE NUMBER: B007

LAST APPROVED: July 02, 2013, January 15, 2015, January 2017

RELATED TO POLICY SERIES NUMBER: 211

REFERENCE: ORS 339.351 TO 339.364 AND ORS 164.377

mail, network games, and spamming).

E. Unauthorized commercial activities:

- a. Using College resources for one's own commercial gain, or for other commercial purposes not officially approved by the College, including web ads.
- b. Using College resources to operate or support a non-College related business.
- c. Use of College resources in a manner inconsistent with the College's contractual obligations to suppliers of those resources or with any published College policy.

F. Violation of city, state, or federal laws:

- a. Pirating software, music, and images.
- b. Effecting or receiving unauthorized electronic transfer of funds.
- c. Disseminating child pornography or other obscene material.
- d. Violating any laws or participating in the commission or furtherance of any crime or other unlawful or improper purpose.

WHEN INAPPROPRIATE USE OF COMPUTER RESOURCES OCCURS: B007.2

The use of College resources is a privilege. The resources have always been, and will remain, the property of the College.

It is each user's responsibility to promptly report any violation of this policy to the IT Director. Reports of unauthorized use or misuse of computer resources will be investigated pursuant to standard College procedures. All illegal activities will be reported to local, state, or federal authorities, as appropriate, for investigation and prosecution. While the College desires to maintain user privacy and avoid the unnecessary interruption of user activities, the College, at the direction of the College President, reserves the right to investigate any suspected unauthorized or improper use of College resources (as described above). As directed by the College President, investigations may be initiated which could include the inspection of data stored or transmitted on the network. In the event that use is determined to be contrary to College policy or applicable law, appropriate measures will be taken. These measures may include, but are not limited to, permanent or temporary suspension of user

ACCEPTABLE USE OF COMPUTING RESOURCES

ADMINISTRATIVE RULE NUMBER: B007

LAST APPROVED: July 02, 2013, January 15, 2015, January 2017

RELATED TO POLICY SERIES NUMBER: 211

REFERENCE: ORS 339.351 TO 339.364 AND ORS 164.377

privileges, deletion of files, disconnection from the Tillamook Bay Community College network, referral to student or employee disciplinary processes, and cooperating with the appropriate law enforcement officials and government agencies.

INFORMATION ON APPLICABLE LAWS AND STATUTES: B007.3

All users of the College computer and information resources are expected to be familiar with and to abide by College policies, as well as local, state, and federal laws relating to electronic media, copyrights, privacy, and security.

In accordance with civil liability laws, persons found to have committed copyright infringement may be held liable for substantial damages and attorneys' fees. The law entitles a plaintiff to seek statutory damages of \$150,000 for each act of willful infringement. In the cases filed by the RIAA against students at Princeton, RPI, and Michigan Tech, the recording industry sued for damages of \$150,000 for each recording infringed.

Copyright infringement also carries criminal penalties under the federal No Electronic Theft Act. Depending on the number and value of the products exchanged, penalties for a first offense may be as high as three years in prison and a fine of \$250,000. TBCC is not the police; however, TBCC will cooperate with the law enforcement agencies when required.

As a condition of being granted internet and network access, employees of the College complete and sign a user agreement affirming an understanding and intention to abide by these acceptable use guidelines. A summary of these guidelines are also posted at various locations across campus where they are freely accessible by students and other non-employee users.

QUESTIONS RELATING TO THIS POLICY: B007.4

The examples of unauthorized use set forth above are not meant to be exhaustive. Whenever in doubt regarding an issue of questionable use, it is in the user's best interest to resolve the issue before pursuing any questionable use of College computing resources. Questions of appropriate use should be addressed to the IT Department.