

## **140-01 ACCEPTABLE USE OF TECHNOLOGY—PROCEDURE**

### **1. PURPOSE**

All College systems are considered College property, and as such, supervisors have the right to access these systems when needed, including staff desktop computers, file folders, etc.

Any individual who uses the technology resources of Coconino Community College consents to all of the provisions of the Acceptable Use of Technology Policy (Policy 140-00) and agrees to comply with all of the terms and conditions set forth herein, and with all other applicable College policies, regulations, procedures, and rules, including applicable local, state, and federal laws and regulations.

### **2. PROCEDURE**

Users of Coconino Community College technology resources are expected to abide by the following guidelines:

1. User shall comply with all applicable local, state, and federal laws.
2. User shall comply with all Coconino Community College policies, regulations, procedures, and rules.
3. User shall respect the intellectual property rights of others. Making unauthorized copies of licensed software or copyrighted material is prohibited.
4. User shall refrain from sharing passwords or accounts with anyone, including trusted friends or family members. Users will be held responsible for any actions performed using their accounts. Coconino Community College staff will never ask users for their passwords.
5. No user shall intentionally use any system/resource in such a manner that will damage the equipment; destroy/corrupt programs, or render the hardware/software inoperable.
6. No user shall attempt to copy unapproved College-owned software from any College equipment to another media (diskette, tape, zip drive, etc.) for the purpose of using the software on personal equipment.
7. No user shall attempt unauthorized distribution of copyrighted material using systems/technology resources. Violations of copyrighted material distribution laws are subject to civil and criminal liabilities.
8. No user shall install or use personal software on college computers without the approval of the Chief Technology Officer or designee.
9. No user shall access/use another user's account for any reason unless requested and authorized to do so by the Chief Technology Officer, and designated supervisor(s), or other authorized employees such as the Human Resources Director.
10. No user shall use technology resources to solicit or proselytize for commercial ventures, religious or political causes, outside organizations, or other non-job or non-instruction related solicitations, or create offensive or disruptive messages. These would include any comments that contain sexual implications or offensively addresses someone's race, age, gender or sexual orientation, religious or political

- beliefs, ethnicity, disability, or any other message which may bring the College into disrepute.
11. No user shall use systems/technology resources to abuse, slander, harass, threaten, or in any way harm another group/user.
  12. No user shall use any systems/technology resources for illegal or malicious purposes.
  13. No user shall intentionally damage or sabotage the systems and adversely impact other users.
  14. The Human Resources Director in conjunction with the Chief Technology Officer and other appropriate managers will be responsible for reviewing all postings, flyers, departmental procedures, etc., regarding the use of technology resources prior to adoption.
  15. No user shall use another person's system files or data without permission.
  16. No user shall use computer programs to decode passwords or access control information.
  17. No user shall attempt to circumvent or subvert system or network security measures.
  18. No user shall engage in any activity that might be purposefully harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, damaging files or making unauthorized modifications to College data.
  19. No user shall excessively use College systems for personal video, music, and/or pictures, and other personal documents. Excessive use as determined by his/her supervisor.
  20. No user shall use College systems for printing large amounts of personal documents or pictures.
  21. No user shall download, store, create and/or display threatening, obscene, pornographic, racist, sexist, or harassing material, including broadcasting unsolicited messages or repeatedly sending unwanted mail, unless legal and for the purposes of specifically meeting course learning objectives.
  22. No user shall use the College's systems or networks for personal gain; for example, by selling access to your user ID or to College systems or networks, or by performing work for profit with college resources in a manner not authorized by the College.
  23. No user shall engage in any other activity that does not comply with the guidelines presented above.
  24. No user shall use personal devices in a way that will disrupt service to students.

#### Disciplinary Action

Violations of this policy or any other College policy or regulation may be subject to revocation or limitation of computer and network privileges as well as other disciplinary actions or may be referred to appropriate external authorities.

Failure to follow these guidelines may result in disciplinary action up to and including termination for employees (refer to the Disciplinary Action Procedure 450-01) or

disciplinary action up to and including expulsion from the College for students (refer to the Student Code of Conduct Procedure 503-01) and civil and criminal liabilities.

### **3. BACKGROUND**

1. References: none
2. Revision history: 04/28/2010 (new), 09/14/2011
3. Legal review: none
4. Sponsor: Information Technology Services

Adopted by College Council: 09/14/2011

**COCONINO COMMUNITY COLLEGE**