

Acceptable Use of IT Resources

Pima Community College

1. Objective

To ensure Pima Community College (PCC) and all PCC Users are protected from illegal and/or harmful actions that result from inappropriate use of PCC Systems, and to ensure that all PCC Users are responsible for proper use of PCC Systems.

2. Definitions

PCC Users: All College employees, faculty, and students, in addition to all contractors, consultants, temporary workers, volunteers and student aides that access PCC Systems.

PCC Systems: This applies to all equipment and data owned by PCC, which includes but is not limited to, desktop and laptop computers, and any data contained on them; external storage devices; printers; network and server resources such as Banner, internet access, e-mail, file shares; software; phone systems; system accounts; electronic and telephone communication.

PCC Data: All information used by the College in its academic or business operations.

Confidential Data: Data that includes, but is not limited to student or employee records, social security number, ID number, grades, financial data, account numbers, bills, employee performance reviews, personnel files, personal information; business data (P-card numbers, account information, etc); passwords, and any other information deemed confidential by PCC.

3. Responsibilities of PCC Users

- a) Use that is consistent with the PCC mission, values, policies, regulations, and standard practice guides;
- b) Use in an effective, efficient, ethical and lawful manner;
- c) Abide by this acceptable use standard, in addition to all security measures;
- d) Use which consistently protects the confidentiality, integrity, and availability of PCC data. This includes the responsibility of all employees to:
 - i. Ensure that data are accurate, including the prevention of any defacement or mishandling;
 - ii. Ensure that access to data are restricted based on the needs of a job function, and ensure that proper authorization has been granted for all data that are accessed;
 - iii. Ensure that data are available for appropriate College personnel;
 - iv. Ensure that confidential data are rigorously protected and used solely for College use.
- e) Use that complies with federal and state law (including, but not limited to, all laws outlined in the Legal Standards section below), including copyright and intellectual property rights as well as license agreements and contracts.

4. Privacy & Monitoring

All College-owned property and the work, correspondence, data and other material therein, whether stored electronically, on paper, or in any other form, are subject to review for legitimate

business reasons. Portions of the IT infrastructure include automatic and manual monitoring and recording systems that are used for reasons that include, but are not limited to, security, performance, backup, and troubleshooting. The College reserves the right at any time to monitor and access any data, including the contents of any College computer or College communications, for any legitimate business reason.

5. Personal Use

While PCC Systems are provided for College use only, the College recognizes that occasional, brief personal uses of telephones and computers may be necessary from time to time to attend to personal matters that cannot be handled outside work/school hours (e.g., making a business or medical appointment, calling a child's school, checking on a child at home). Limited personal use of PCC Systems must not interfere with or disrupt the work of the unit or other College business or educational activities nor unduly tie up PCC Systems such that they are not available for business and educational use. Long distance telephone calls are prohibited.

6. Legal Standards

All PCC Users are expected to abide by all Federal and State laws. The following list is used for illustrative purposes, and is not intended to be a comprehensive guide to Federal and/or State law:

- FERPA (Family Educational Rights and Privacy Act): regulates the confidentiality of student records.
- GLBA (Graham Leach Bliley Act): regulates the confidentiality of financial information.
- HIPAA (Health Insurance Portability and Accountability Act): regulations the security and privacy of health information.
- PCI DSS (Payment Card Industry Data Security Standard): regulates the confidentiality of credit card information.
- DMCA 1998 (Digital Millennium Copyright Act): regulates the protection of intellectual property.
- USC Title 18 §1030 (United States Code: Fraud and related activity in connection with computers)
- ARS 13-2008 (Arizona State Law: Taking identity of another person or entity) prohibits identity theft.
- ARS 13-2316 (Arizona State Law: Computer tampering; venue; forfeiture): prohibits unauthorized use of computers.
- ARS 13-2407 (Arizona State Law: Tampering with a public record): regulates the integrity of PCC Data.
- ARS 13-3001-3019 (Arizona State Law: Eavesdropping and Communications): prohibits forgery and eavesdropping.
- ARS 13-3707 (Arizona State Law: Telecommunication fraud): prohibits telecommunication fraud.
- ARS 38-448: (Arizona State Law: Access to Pornography is Prohibited): prohibits access to pornography by PCC employees on PCC Systems.
- ARS 38-501-511 (Arizona State Law: Conflict of Interest): prohibits use of PCC resources regarding conflicting interests.
- ARS 44-1372 (Arizona State Law: Commercial Electronic E-mail): prohibits spam.



- ARS 44-1373 (Arizona State Law: Confidentiality of Personal Identifying Information) regulates the protection of personal identifying information.
- ARS 44-7501 (Arizona State Law: Notification of Security Breach): regulates the public notification of unauthorized disclosure of confidential information.

7. Investigations & Discipline

Use of all College resources is subject to Section V, Code of Conduct/Discipline of the Personnel Policy Statement for College Employees. Any investigations of misconduct will be conducted according to SPG-5702/AG. For students, use of College resources is subject to the Student Code of Conduct. Unauthorized use or abuse of College resources may result in disciplinary action up to and including termination and/or expulsion. Additional civil and/or criminal punishments may also be applicable.

Appendix A: Examples of prohibited behavior

- Circumvention of any security systems and/or procedures, including any unauthorized activities aimed at compromising system or network security, including: hacking, probing, or scanning; attempts to break into other users' accounts or to obtain passwords; use of computer viruses, worms, or any kind of spyware or malicious software; sharing your username or password with another person, or using another's account name or password.
- Storing confidential PCC Data on non-PCC Systems or removing confidential data off of Pima property without authorization from the proper Data Trustee.
- Any attempt to add or reconfigure any PCC Systems, connecting a personal computer or other non-PCC computing device to the PCC internal network (use of wireless network is allowed), without written authorization from the Vice Chancellor of IT.
- Running IT servers, whether virtual or physical, without the express, written authorization from the Vice Chancellor of IT.
- Attempts to forge e-mail or other electronic information, or any other actions that degrade the accuracy of PCC Data
- Using PCC Systems to view pornography, send spam, pranks, chain letters, pyramid schemes, etc.
- Illegally downloading copyrighted material, or violating any license agreement or intellectual property rights in any way.
- Any conduct prohibited by Section V of the Code of Conduct/Discipline, including section B. Code of Conduct and Standards of Behavior for Employees.

I have read and agree to abide by the above standards and acknowledge that any action by me which is contrary to the above standards may be cause for discipline, discharge or legal action against me.

Print Name

Signature

Date