Appendix E. Acceptable Use of Information Technology Resources

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, polices, 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): regulates 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 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.