PimaCountyCommunityCollegeDistrict
Administrative Procedure

AP Title:	**Data Protection**
AP Number:	AP 9.01.10
Adoption Date:	5/8/24
Schedule for Review & Update:	Every three years
Review Date(s):	
Revision Date(s):	
Sponsoring Unit/Department:	Information Technology
Policy Title(s) & No(s).:	Information Technology Resource Management, BP 9.01
Legal Reference:	European Union's General Data Protection Regulation (GDPR), Article 13; Arizona State Statutes: §18-552; §18-606 and §18-609
Cross Reference:	Information Management Standard, AP 9.01.08; Security of the Information Technology Infrastructure, AP 9.01.03; Acceptable Use of Information Technology Resources, AP 9.01.01

PURPOSE

Pima Community College recognizes that as part of our operations we must collect and process data. The purpose of this Administrative Procedure (AP) is to describe how personal data must be collected, handled, and stored to meet the Pima Community College's data protection standards, comply with governing privacy and data protection laws, and respect individual rights. The purpose of this AP is as follows:

- Comply with data protection laws and follow best practices.

- Protect the rights of staff, customers, and any related data subjects.

- Ensure transparency around how Pima Community College collects, stores, and processes individuals' data.

SECTION 1: Definitions

Data – information in a format that can be processed, including electronic data and physical data.

Personal Data – any information relating to an individual data subject who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person. This data could be anything from a name, an email address, geolocation data, or even a username or IP address.

Data Subject – an identifiable person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

Consent – consent is any freely given, specific, informed, and unambiguous indication of a data subject's wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.

Data Storage – these rules describe how and where data should be safely stored.

SECTION 2: Procedure and Responsibilities

Baseline Requirements:

2.1. Employees will keep all data secure by taking sensible precautions and following guidelines outlined within this AP and any associated procedures.

2.2. Data will not be shared informally; defined data access levels will be determined based on role and existing access controls.

2.3 Pima Community College will provide training to all employees to help them understand their responsibilities when handling data.

2.4 Personal data will not be disclosed to any unauthorized person, either within the organization or externally.

Data Collection:

2.5. Pima Community College collects personally identifiable information (PII), which has been expressly and voluntarily provided to the College through IT Resources (e.g., applying to the College, applying for financial aid, registering for courses, joining a mailing list, applying for employment, etc.). The program is managed by the Chief Information Security Officer and the Office of the General Counsel and supported by a group of representatives from across the College.

2.6. The College only collects minimal information to fulfill business needs (e.g., employment application, student enrollment).

Data Protection:

2.7. The College uses reasonable organizational, technical, and administrative measures to protect personal data collected.

2.8. The College cannot guarantee the security of any information transmitted through IT Resources because no transmission or electronic storage method is 100% secure.

2.9. The College is not responsible for the content, privacy, or security practices of any non-College IT Resources.

Data Retention:

2.10. The College retains personal data for as long as it is necessary, required, or permitted by law.

Data Use:

2.11. The College may use that information to fulfill requests for our information, services, or communicate information of interest.

2.12. The College does not sell, trade, or share PII with third parties unless one or more of the following conditions apply:

2.12.1 Explicit consent was given to share the information.

2.12.2 Court orders, as required by applicable law, or other legal processes in response to subpoenas.

2.12.3 When a business need arises, the College may share information with service providers acting on the College's behalf to conduct outreach, development, and advertising campaigns, who have agreed to protect the confidentiality and integrity of the data.

2.13. When requested, the College may remove any historical, non-current contact information provided from its IT Resources. Former students should make this request to the Registrar, while former employees should direct their request to Human Resources. If the request is deemed appropriate, the IT Department will process the request.

2.14. By accessing College IT Resources, you consent to process data about and for the purposes stated in this policy and described in the IT Acceptable Use AP.

2.15. Personal data automatically aggregated may be used to improve the content of our websites, analyze trends, investigate security concerns, and identify system performance or problem areas.

Data Storage:

2.16. When data is stored electronically, it will be protected from unauthorized access, accidental deletion, and malicious hacking attempts.

2.17. Pima Community College data will be stored on designated drives and servers and will only be uploaded to approved cloud computing service(s).

2.18. Users will refrain from permanently storing data directly to devices.

2.19 Users must ensure that all data classified as Internal Use, Confidential, or Regulated in hardcopy form is removed from their workspace and secured in a drawer when the desk is unoccupied at the end of the workday. (See AP 9.01.08 for full definitions and examples of Internal Use, Confidential, and Regulated data).