PimaCountyCommunityCollegeDistrict
Administrative Procedure

AP Title:	**Electronic Email (Email)**
AP Number:	AP 9.01.12
Adoption Date:	
Schedule for Review & Update:	Every three years
Review Date(s):	8/6/25
Revision Date(s):	
Sponsoring Unit/Department:	Information Technology
Policy Title(s) & No(s).:	Information Technology Resource Management, BP 9.01
Legal Reference:	Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g; Arizona Revised Statutes (A.R.S.) § 39-103, Size of public records; A.R.S. 39-121, Inspection of public records
Cross Reference:	AP 2.15.01: Records and Information Management; AP 9.01.01: Acceptable Use of Information Technology Resources; AP 9.01.08: Information Management Standard Electronic Mail (Email) Handbook Version

PURPOSE

This administrative procedure ("AP") sets standards for use of electronic mail ("email") consistent with applicable law and other Pima Community College ("PCC" or "College") policies, while respecting principles of academic freedom, freedom of speech, privacy, and confidentiality.

The purpose of this AP is to ensure that:

1. Email is used by the College community in an ethical and considerate manner in compliance with applicable law and policies;
2. Email users are informed about how concepts of privacy and security apply to email; and
3. Disruptions to College email and other services and activities are minimized.

SCOPE

This policy applies to:

1. All email services provided, owned, or funded in part or in whole by the College;
2. All users and holders of College email systems or accounts, regardless of intended use; and
3. All College email Official Records and/or Public Records in the possession of, or generated by, College employees and other users of email services provided by the College, regardless whether the records were generated on College or non-College computers.

This policy applies equally to transmission and receipt data, including email headers, summaries, and addresses associated with email records, and any attached files or text. This policy does not apply to:

1. Internet services other than email
2. Voice mail
3. Audio and video conferencing
4. Facsimile messages

This policy does not apply to printed copies of email, but other law and policy may apply to such documents. Under Arizona records law and other state laws, information appearing in this format may need to be retained as Official Records or treated as State Publications under A.R.S. section 39-101, et seq. If the user prints out email Official Records (including transmission and receipt data) and retains them in hard copy according to approved College records management policies and retention schedules, the electronic copy may be deleted immediately. (See AP 2.15.01 Records and Information Management for related definitions and guidelines or contact the College Records & Archives for instructions.)

SECTION 1: Procedure and Responsibilities

Baseline Requirements:

1.1 Specific Use Provisions

1.1.1. Provision of Service: Official College email is provided to all faculty, staff, and students by PCC Information Technology (IT) in support of the College's mission. PCC IT may provide email to other colleagues upon request.

1.1.2. College Property: Email services are extended for the sole use of College faculty, staff, students, and other appropriately authorized users to accomplish tasks related to and consistent with the mission of the College. College email systems and services are College facilities, resources, and property as those terms are used in College policies and applicable law. Any email address or account assigned by the College to individuals, sub-units, or functions of the College is the sole property of the College.

1.1.3. Authorized Service Restrictions

1.1.3.1. Email users are required to comply with state and federal laws, College policies, and standards of professional and personal courtesy and conduct. Access to College email services is a privilege that may be wholly or partially restricted by the College without prior notice and without the consent of the email user: (a) when required by and consistent with applicable law or policy; (b) when there is a reasonable suspicion that violations of policy or law have occurred or may occur; or (c) when required to meet time-dependent, critical operational needs. Such access restrictions are subject to the approval of the appropriate College supervisory or management authority.

1.1.3.2. When an individual's affiliation with the College ends, the individual's College email service will be discontinued. The only exception is for Emeritus faculty.

1.1.3.3. The following timelines are provided for discontinuation of email services:

1.1.3.3.1. Staff: Immediately upon non-affiliation

1.1.3.3.2. Faculty: Immediately upon non-affiliation

1.1.3.3.3. Students: three semesters after the last semester in which the student has completed a PCC course

1.1.3.3.4. Emeritus: N/A

1.1.4. Authorized Access and Disclosure

1.1.4.1. The College may permit the inspection, monitoring, or disclosure of email when:

1.1.4.1.1. required by or consistent with applicable law or policy such as Arizona Public Records law (A.R.S. section 39-121, regarding inspection of public records); the Family Educational Rights and Privacy Act (regarding access to student records); or any appropriately issued subpoena or court order. The Electronic Communications Privacy Act of 1986 also permits messages stored on College systems to be accessed by authorized personnel in certain circumstances;

1.1.4.1.2. there is a reasonable suspicion that violations of a law or College policy have occurred or may occur; or

1.1.4.1.3. there are time-dependent, critical operational need of College business if the College determines that the information sought is not more readily available by other means.

1.1.4.2. In such instances, the College will, as a courtesy, try to inform email users prior to any inspection, monitoring, or disclosure of email records, except when such notification would be detrimental to an investigation of possible violation of law or College policy. Users are required to comply with College requests for access to and copies of email records when access or disclosure is required or allowed by applicable law or policy, regardless whether such records reside on a computer housed or owned by the College. Failure to comply with such requests can

lead to disciplinary or other legal action pursuant to applicable law or policy, including but not limited to appropriate College personnel policies or Codes of Conduct.

1.1.4.3. All inspection, monitoring, or e-discovery will be conducted by College IT staff. Data will be provided to College General Counsel for legal matters and to the business unit supervisor for business matters.

1.1.4.4. Matters pertaining to legal authority or necessity will be determined by College General Counsel.

1.1.5. Indemnification of the College: Users agree by virtue of access to the College computing and email systems, to indemnify, defend, and hold harmless the College for any suits, claims, losses, expenses, or damages, including but not limited to litigation costs and attorney's fees, arising from or related to the user's access to or use of College email and computing systems, services, and facilities.

1.2 Misuse

1.2.1. Using email for illegal activities is strictly prohibited. Illegal use may include but is not limited to: obscenity; child pornography; threats; harassment; theft; attempting unauthorized access to data or attempting to breach any security measures on any electronic communications system; attempting to intercept any electronic communication transmissions without proper authority; and violation of copyright, trademark, or defamation law.

1.2.2. Failure to follow state law regarding the disposition of email records may lead to criminal charges. Theft or unauthorized destruction, mutilation, defacement, alteration, falsification, removal, or secretion of email records may lead to class 4 or class 6 felony charges under A.R.S. section 38-421.

1.2.3. In addition to illegal activities, the following email practices are expressly prohibited: entry, examination, use, transfer, and tampering with the accounts and files of others, unless appropriately authorized pursuant to this policy; altering email system software or hardware configurations; or interfering with the work of others or with College or other computing facilities.

1.2.4. If a user is requested by another user via email or in writing to refrain from sending email messages, the recipient is prohibited from sending that user any further email messages until such time as they have been notified by the system administrator that such correspondence is permissible. Failure to honor such a request shall be deemed a violation of this policy. This provision does not apply to email messages required solely for the performance of job-related duties.

1.2.5. College email services may not be used for commercial activities not approved by appropriate supervisory College personnel consistent with applicable policy; personal financial gain (except as permitted under applicable academic policies); personal use inconsistent with Section 1.3 of this policy; uses that violate other College policies or guidelines; or uses inconsistent with applicable state or federal law. Applicable College policies include, but are not limited to, policies and guidelines regarding personnel, intellectual property, or discrimination and harassment.

1.2.6. Email users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the College or any unit of the College unless expressly authorized to do so. Where appropriate, the following explicit disclaimer shall be included: "The opinions or statements expressed herein are my own and should not be taken as a position, opinion, or endorsement of Pima Community College."

1.2.7. College email services shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, strain on any computing facilities or interference with others' use of email or email systems. Such uses include, but are not limited to, the use of email services to:

1.2.7.1. Send or forward chain letters.

1.2.7.2. "Spam"; that is, to exploit listservs or similar systems for the widespread distribution of unsolicited mail.

1.2.7.3. "Letter-bomb"; that is, to resend the same email repeatedly to one or more recipients.

1.3 Personal Use

1.3.1. College email services may be used for incidental personal purposes provided that such use does not:

1.3.1.1. Directly or indirectly interfere with the College operation of computing facilities or email services.

1.3.1.2. Interfere with the email user's employment or other obligations to the College.

1.3.1.3. Violate this policy, or any other applicable policy or law, including but not limited to, use for personal gain, conflict of interest, harassment, defamation, copyright violation, or illegal activities.

1.3.2. Email messages arising from such personal use shall, however, be subject to access consistent with this policy or applicable law. Accordingly, such use does not carry with it a reasonable expectation of privacy.

1.3.3. Users should refrain from registering their College email address with personal use websites (e.g. personal shopping websites, personal social media sites, etc.). College email addresses are largely temporary in nature, active only while maintaining an active college affiliation, and should be treated as such. The College will not provide access after College affiliation is ended and will not retain email data after applicable retention periods.

1.3.4. Where users cannot avoid using their College email address to register for legitimate third-party accounts, College users are prohibited from using the same credentials for both their College authentication and the third-party authentication (e.g. password reuse).

1.4 Confidentiality

1.4.1. The confidentiality of email cannot be assured, and any confidentiality may be compromised by access consistent with applicable law or policy, including this policy, by unintended

redistribution, or due to current technologies inadequate to protect against unauthorized access. Users, therefore, should exercise extreme caution in using email to communicate confidential or sensitive matters, and should not assume that their email is private or confidential.

1.4.2. Users may not access, use, or disclose personal or confidential information without appropriate authorization, and must take necessary precautions to protect confidentiality of personal or confidential information, regardless of whether the information is maintained on paper or is found in email or other electronic records.

1.4.3. The Office of the Registrar may elect to publish student email addresses as directory information, consistent with the requirements of the Family Educational Rights and Privacy Act (FERPA). Individual students may, consistent with College policy and FERPA, request the College not to treat the address as directory information. Requests for identification or release of student email addresses should be directed to the Office of the Registrar.

1.5 Security and Preservation

1.5.1. Email users and operators must follow sound professional practices in providing for the security of email records, data, applications programs, and systems programs under their jurisdiction.

1.5.2. Users and operators must guard against storage media deterioration and email record inaccessibility due to hardware or software obsolescence. To eliminate these situations, users must make provision for future accessibility by:

1.5.2.1. migrating all official email records to the next generation of hardware or software; or

1.5.2.2. migrating only current official email records to new hardware or software or converting official email records not migrated to other media (e.g., optical disk) for short term storage or to "eye readable form" (i.e., paper or microfilm) for long term storage and preservation. (See the Arizona State Library, Archives and Public Records General Retention Schedule for state-mandated

guidelines on the storage and disposal of email records or contact the College Records & Archives for instructions.)

1.5.3. Users are responsible for safeguarding their identification (PCC User ID) code and password, and for using them only as authorized. Each user is responsible for all email transactions made under the authorization of their PCC User ID, and for all network email activity originating from their PCC User ID. Use of email user identifications for commercial purposes is prohibited. Access to user identifications may not be loaned or sold.

1.5.4. Each operational unit should establish:

1.5.4.1. Standards for official email records identification, file organization, and inclusion in their file plan.

1.5.4.2. Measures for protecting sensitive official email stored electronically specific to their unit.

1.5.4.3. Procedures for file backup, if needed beyond what the College IT provides.

1.6 Violations

1.6.1. Suspected or known violations of policy or law should be confidentially reported to the appropriate supervisory level for the operational unit in which the violation occurs. Violations will be processed by the appropriate College authorities and/or law enforcement agencies. Violations may result in revocation of email service privileges; academic dishonesty or Code of Conduct proceedings; faculty, staff, or student disciplinary action up to and including dismissal; referral to law enforcement agencies; or other legal action.