EL PASO COMMUNITY COLLEGE PROCEDURE

For information, contact Institutional Effectiveness: (915) 831-6740

CR-1 **Electronic Mail Services, Personal and Broadcast Email, and Email Restrictions**

APPROVED: March 23, 2007 **REVISED**:
Year of last review: 2021
AUTHORIZING BOARD POLICY: CR

Classification: Institutional
Responsible Vice President or Associate Vice President: Vice President of Information Technology/Chief Information Officer
Designated Contact: Executive Director of IT Software Applications & Analytics

---

OBJECTIVE: Information Technology (IT) provides electronic mail (email) services to all staff of El Paso County Community College District, referred to in this document as EPCC. All users have the responsibility to use email services in an efficient, ethical, and legal manner in accordance with College procedures.

PROPONENT: The Office of the Chief Information Officer is the proponent of this procedure, annual review and updates. The Chief Information Officer (CIO) will provide clarification for any issue regarding this procedure.

DEFINITIONS:

1. Electronic mail system: A computer software application that allows electronic messages to be communicated from one computer to another.

2. Electronic mail (email): Any message, form, attachment, or other communication sent, received, or stored within an electronic mail system.

I. PERSONAL EMAIL

A. Electronic mail sent, received, or stored on computers owned, leased, or administered by EPCC is the property of EPCC. Email is a communication tool used to facilitate business communications. The use of any EPCC resources for electronic mail must be related to College business, including academic pursuits. A recipient-user may copy or forward such emails within the EPCC community as required. EPCC cannot guarantee the delivery of any email or any attachment but will assist the sender in identifying problems and recovering messages and attachments.

B. Only EPCC staff and other persons who have been granted permission and an email account are authorized users of the EPCC email system. No user shall use another employee's user-ID or password to access or transmit an email communication. All email accounts will be created using the External Login ID assigned to them when they are added to the Banner System. These Login ID's usually take the form First Initial, Last Name (or portion thereof), and a number which is used to ensure that each Login ID is unique. All email accounts will be LoginID@epcc.edu.

C. A default password is created and sent when account creation occurs. Users are expected to change the account password for security reasons. EPCC requires that all passwords must meet the following complexity requirements: be at least 8 characters long and contain a combination of at least three of the following four types of characters: (1) uppercase, (2) lowercase, (3) numbers, (4) special characters, such as @, #, $, etc.

D. Incidental Use. As a convenience to employees, incidental use of electronic mail is allowed. The following restrictions apply.

   1. Incidental personal use of EPCC Information Resources is acceptable, provided electronic mail is restricted to EPCC employees; it does not extend to family members or friends.

   2. Incidental use must not result in direct costs to EPCC.

   3. Incidental use must not interfere with the normal performance of an employee's work duties.

4. No messages should be sent or saved that may cause damage to EPCC.

5. No personal messages should be sent, read, or saved that have high likelihood to expose College computer systems to computer viruses or other harmful programs. All employees should review the guidelines established by Information Technology. Storage of personal email must not exceed the default allowance. To minimize space requirements, employees are encouraged to delete personal messages as soon as possible. Employees will be notified by email if any changes to this posting occur.

6. Employees should remove themselves from any personal mail lists that send messages containing content not in compliance with this procedure. Examples are periodic messages that have nothing to do with delivery of instruction or the administration of the College, such as inappropriate jokes or unofficial virus alerts not issued by the Information Technology Service Center are examples. Also, if the recipient is personally uncomfortable with the content of messages sent via a personal mail list of which he is an addressee, the employee should request the sender remove him from the mailing list or group.

7. Abuse of incidental use privileges may result in disciplinary action in accordance with EPCC procedures.

8. All messages - including personal messages - are owned by EPCC, may be subject to open records requests, and may be accessed in accordance with this procedure and state and federal law.

E. EPCC neither sanctions nor censors individual expression of opinion on our email services. The standards of behavior, however, are expected in the use of email as in the use of telephones and written and oral communication.

1. Email attachments are often used to spread computer viruses and worms. While EPCC scans incoming email for Internet attacks such as these, there are other ways for these threats to make their way onto the College's computer systems. For this reason, the College restricts the opening of certain types of attachments, and users should take extreme care when opening email attachments. Messages with attachments having filename extensions of .exe and .com are executable programs and can do great damage to a computer's hard drive. Users should use caution when opening attachments.

2. Users are advised to take care when giving out their email addresses to online web sites, newsgroups, etc. Spammers or companies that send unsolicited email, typically buy, steal, or harvest email address lists from these sources.

3. Prohibited Activities.

   a. The following activities are prohibited:

      (1) The sending of email that is intended to intimidate or harass;
      (2) The use of email for managing and conducting a personal enterprise;
      (3) The use of email for purposes of political lobbying or campaigning with the exception of internal College governance;
      (4) The violation of copyright laws by inappropriately distributing protected works;
      (5) The accessing of another employee's email without that employee's consent unless doing so in accordance with established policy, procedure or law;
      (6) The posing as anyone other than oneself when sending email, except when authorized to send messages for another when serving in an administrative support role.

   b. The following activities are prohibited because they impede the functioning of network communications and the efficient operations of electronic mail systems:

      (1) The sending or forwarding of chain letters;
      (2) The sending of unsolicited messages to large groups, except as required to conduct College business;
      (3) The sending or forwarding of email that is likely to contain computer viruses.

Prohibited activities identified in this section are not all inclusive. EPCC electronic mail must never be used in a manner that violates EPCC policy or procedure, state law or federal law. EPCC has the right to terminate access to electronic mail services if a user is determined to have violated EPCC policy, procedures or standards.

F. EPCC will make reasonable efforts to maintain the integrity and effective operations of its email systems, but users are advised that those systems should not be regarded as a secure medium for the communication of sensitive or confidential information. EPCC can assure neither the privacy of an individual user's use of the College's email resources nor the confidentiality of particular messages that may be created, transmitted, received, or stored.

G. Network and Email Monitoring: The goal of monitoring, logging and retention of network packets that traverse the EPCC network backbone is to maintain the integrity and security of the College's network infrastructure and information assets and to collect information to be used in network design, engineering, troubleshooting and usage-based accounting. EPCC considers all electronic information transported over our network to be private and confidential. Network and system administrators are expected to treat the contents of electronic packets as private and confidential. Any inspection of electronic files, including email messages and attachments, and any action performed following such inspection, will be governed by all applicable federal and state statutes and by College policies. Human Resources authorized to analyze network backbone flow will not disclose any information realized in the process without approval of the cognizant administrator and the Chief Information Officer.

1. EPCC may monitor or access email and attachments, with or without prior notice, for the following reasons:

   a. To check network traffic

   b. To investigate and repair system malfunctions

   c. To action a request by a user to repair or restore his or her own email

   d. To prevent the business of the College from being obstructed or delayed by the unavailability of a user, subject to paragraph I.G.3

   e. To investigate a breach or suspected breach of the EPCC procedures or of state or federal law.

2. The Vice President for Information Technology can authorize a qualified staff member to monitor or access email and attachments under sub-paragraph G.1.a, G.1.b, or G.1.c. The assigned staff member shall review email and attachments on a need-to-know basis and only to the extent of their need-to-know and will be bound by an obligation of confidentiality.

3. Where it is necessary for the College to access a user's email and attachments to prevent the business of the College from being obstructed or delayed, the following procedure is to be followed:

   a. The user, with the agreement of the supervisor, will attempt to arrange reasonable alternatives to make the email and attachments available without the need to access the user's email.

   b. If reasonable alternative arrangements cannot be agreed upon to make the email and attachments available, the supervisor will advise the relevant administrator or member of the President's Cabinet.

   c. The administrator or Cabinet member must first be satisfied that reasonable efforts have been made to agree upon alternative arrangements and that the business of the College will be obstructed or delayed by the lack of access to the user's email. If satisfied, (s)he will make a request for the accessing of the email pursuant to paragraph I.G.4, below. If the request is approved, access to the email will be given to the user's supervisor.

   d. The user, with the agreement of the supervisor, will attempt to arrange reasonable alternatives. The supervisor will be solely responsible for accessing the email and attachments on a need-to-know basis only. The supervisor may open, copy, forward or

reply to email, and may open or modify attachments, but only those necessary to further the business of the College. Any forwarding or reply must be in the name of the supervisor and not in the name of the user. The supervisor must keep a record of all emails and attachments accessed, including hard copies, to be provided to the user as soon as possible.

e. Where the user is a student of EPCC, the Vice President for Student and Enrollment Services is the "supervisor" of the user.

4. A request for the monitoring or accessing of email and attachments under sub-paragraph I.G.3 or I.G.5 must be addressed to the Vice President for Information Technology in writing setting out the reason(s) for making the request. The Vice President for Information Technology, after approving the request, will then forward it to the Vice President of Administration and Financial Operations for co-authorization. Results from the monitoring or access request must be provided to the person who made the request and used by that person only in connection with the reason(s) for the request. The person monitored will be notified. The Vice President for Information Technology will produce a quarterly report to the President of all investigations undertaken pursuant to this paragraph.

5. During any foreseen absence from the College, all staff members are encouraged to put in place an email forwarding or notification facility such as vacation message.

H. Records Retention. Electronic mail is subject to the same records retention rules that apply to other documents and must be retained in accordance with departmental records retention schedules.

1. The retention requirement associated with any document is determined by its content, not the method of delivery. Each EPCC component should have a records retention schedule that specifies the retention period to be applied to various documents.

2. The responsibility of retaining an internally created and distributed document (or message) most often falls on the author - not the recipients. Recipients may delete such received messages when their use has been fulfilled.

3. Employees who receive messages from outside EPCC are responsible for proper records retention of those messages.

4. Most casual email messages are "transitory records" and can be discarded as their purpose is served.

5. For records retention purposes, electronic mail that is digitally signed must be filed electronically rather than on paper if the signature is of importance to the legal status or business usefulness of the document.

6. Email that has been requested in a subpoena or public information request must be retained until the request has been addressed, even if the retention period has expired.

I. Electronic Mail Backup and Recovery. Information Technology creates electronic mail backup tapes daily (Monday through Friday) solely for the purpose of restoring the entire electronic mail system in the event of disaster.

Tapes are retained for a period of one week. Backup tapes do not allow for restoration of individual mailboxes and cannot be used as a convenience to retrieve "deleted" messages.

Backup tapes do not serve the records retention function. Each EPCC department must make provisions to retain documents and messages in accordance with their departmental records retention policy.

II. BROADCAST EMAIL:

A. Email broadcast messages are email messages sent to all or a portion of the District and are used to announce College events and functions, or College-related news. Individuals do not send broadcast email messages; the messages must be sponsored at the organizational level. Requests to send email messages to the District will be the responsibility of the administrator for that area. Users shall not circumvent this procedure by creating their own "all employees" distribution list.

B. All other announcements are to be made through web pages or listservs.

C. The Chief Information Officer/Vice-President for Information Technology may, from time to time, issue additional guidelines pertaining to use of the College's Email facilities. These guidelines will be issued through the IT Help Center, voicemail broadcasts, IT web page news alerts, or via notice using supervisory channels.

D. The Information Help Center will maintain four mail accounts to support the broadcast emails of these types:

1. Emergency Notification: The request to transmit this message to all employee mailboxes must come from the office of a Vice President. The information everyone must know is critical information regarding emergency situations that require immediate action. To confirm the request, the IT Help Center will verify the information with the originating office via telephone and then transmit the message with all the alerts available in Microsoft Exchange.

2. Facilities and Services Bulletin: Important information that may affect the working conditions in any EPCC-owned or occupied facilities will be sent to everyone in the District. Messages must be sent to facilities_services@epcc.edu. The use of this broadcast account is restricted to the Director of Physical Plant, the EPCC Police Department, and the supervisory channels above those positions.

3. District News: Official information pertaining to the mission of the District that everyone should know will be sent to EPCCdistrictnews@epcc.edu. Messages will be reviewed to determine if they fit this category and, if questioned by the Help Center management, will be discussed with the requestor.

4. Postings: This category of information fits those messages that are not related to the delivery of instruction or administration of a support or service mission. The viewing of the information contained in these messages is voluntary and the failure to view them will not affect any employee's ability to successfully perform their job tasks. The requesting department should send its broadcast email request along with an attachment with the contents to EPCCpostings@epcc.edu. These messages will be transmitted to all employees at 11:00 a.m. each morning and, if there are more requests, at 3:00 p.m. every afternoon. A single "Postings" message may be used to convey all accumulated requests. **Requestors should take care to ensure that the filename of their attachment effectively represents the title of their message**.

5. Presidential discretion may be used to grant email broadcast privileges.

E. The following table lists some criteria for sending messages.

Table 1: Criteria for sending messages

	District News	Postings
Announcing College events and activities, College office closings, etc.	X	
Announcing community events and activities		X
Announcing Employee of the Month, retirement luncheons, deaths and arrangements, or hospitalization		X
Advertising for-sale items or fund-raising events to financially benefit College programs/activities, official employee organizations, or sponsored student organizations.		X
Advertising for-sale items or fund-raising events to financially benefit either employees or students who are experiencing a hardship		X
Requesting from others items to be purchased or to be given as gifts for personal or non-EPCC use.		X
Sending accolades for College-related activities on behalf of College personnel, teams, or organization.		X
Sending accolades on behalf of individuals, teams, organizations, or activities in the community		X

III. Email Restrictions

A. Unallowable actions

Table 2 lists the types of actions, which are not allowed (either through sending or storing), on campus email systems (including the use of District computers to process email). The unsolicited receipt of content listed in Table 2 shall not constitute an infringement of these procedures.

Table 2: Unallowable actions

	Reference (if applicable)
Engaging in discourse which is not "civil"	Refer to included paragraph on civil discourse (below)
Urging the support or defeat of any political candidate or ballot measure	Texas Education Code
Advertising/promotion (such as "for-sale" items, business opportunities, or fund- raising events) or otherwise conducting business to financially benefit employee(s), external individuals, or external for-profit organizations (unless the activity is for a charitable cause and approved by the President.)	
Engaging in activities that are otherwise prohibited by local, state, and federal laws/regulations.	

B. Civil Discourse

As an academic institution, EPCC recognizes that its purpose for existence is to educate students, seeking to provide them with relevant and factual information as well as the critical analysis tools to interpret and use that information. The College also recognizes that electronic communications, especially through email, is easily shared with or forwarded to other parties beyond our initial intentions. For this reason, the manner in which employees communicate is often visible to colleagues and students, as well as to members of the public. Accordingly, stakeholders of the College and the community will judge the quality of the institution based on its professionalism. The following guidelines are implemented in procedures to enhance the College's role in facilitating a quality student-learning environment:

All electronic communications shall be conducted in:

1. An academic manner with a rigorous attempt to seek and convey truthful statements.

2. A professional manner, focusing in a respectful way on issues and matters related to the College.

3. A collegial manner, to promote a hostile-free work environment including freedom from defamation, libel, intimidation, or harassment.

IV. Glossary

For purposes of this procedure, the following definitions apply:

- Defamation: Any intentional false communication, either written or spoken, that harms a person's reputation; decreases the respect, regard or confidence in which a person is held; or induces disparaging, hostile, or disagreeable opinions or feelings against a person.

- Libel: Distributed material meeting three conditions: The material is defamatory either on its face or indirectly; the defamatory statement is about someone who is identifiable to one or more persons; and the material must be distributed to someone other than the offended party.

- Intimidation: The act of making others do what one wants through fear.

- Harassment: Creating an environment that interferes with another employee's ability to perform his or her official responsibilities.

- Network behavior**:** The manner in which a student or employee uses the EPCC network. Users should consume network capacity with respect for the needs of others. Information Technology reviews network traffic for the purposes listed below. When reviewing network behavior for indications of abuse of the resource, network administrators are required to treat the contents of electronic packets as private and confidential. Any inspection and subsequent action will be governed by all applicable federal and state statutes and by EPCC policies and procedures.

1. Enforcing policies against unlawful discrimination, defamation, harassment and threats to the safety of others.

2. Protecting against, or limiting, damage to College information technology resources.

3. Complying with a request for public information under the Texas Public Information Act, Tex. Code 552.001 *et seq*., or complying with a court order, subpoena or a legally enforceable discovery request.

4. Investing and preventing the posting of proprietary software of electronic copies of texts, data, media or images in disregard of copyright, licenses, or other contractual or legal obligations or in violation of law.

5. Safeguarding the integrity of computers, networks, software and data.

6. Preserving information and data.

7. Upgrading or maintaining information technology resources.

8. Protecting the College or its employees and representatives against liability or other potentially adverse consequences.