

CITRUS COMMUNITY COLLEGE DISTRICT GENERAL INSTITUTION

AP 3723 ELECTRONIC MAIL AND BULK ELECTRONIC DISTRIBUTION

1.0 Purpose

Citrus Community College District electronic mail (email) services support the educational and administrative activities of the district and serve as a means of official communication by and between users and the district. The purpose of this procedure is to ensure that this critical service remains available and reliable, and is used for appropriate purposes.

Email is a strategic tool for carrying out the mission of Citrus College. In addition, other electronic methods for distributing information to large groups are becoming available. These methods include but are not limited to phone voice mail, phone text message, and internet portal channels. These methods can be used to easily, quickly, and effectively communicate with large groups of people.

The district provides email services to faculty, staff and students, and to other affiliated classes of individuals, including alumni and official visitors. Use of district email services must be consistent with the district's educational goals and comply with local, state and federal laws and district policies.

2.0 Scope

This procedure applies to all members of the district who are entitled to email services and other electronic bulk distribution services. Users of district electronic mail services are to be limited to district employees, Board of Trustee members, students, and members of associated groups or individuals for purposes that conform to the requirements of this procedure.

Generally, official messages come from the administration or its representatives and are to be sent to the entire community or large subgroups. Mass distribution of messages can have a significant impact on the availability and performance of computing and telephone resources. As such, all bulk electronic message distribution should be authorized as an "official communication" and its distribution and content requires approval prior to distribution.

3.0 Procedure

3.1 Email Addresses and Accounts

Faculty and Staff

Email services are available for faculty and staff to conduct and communicate District business. Incidental personal use of email is allowed with the understanding that the primary use is job-related, and that occasional use does not adversely impact work responsibilities or the performance of the network.

Email services are provided only while a user is employed by the district. Once the user's electronic services are terminated, that user's email services are also terminated and the employee may no longer access the contents of their mailboxes.

Faculty and staff email users are advised that electronic data (and communications using the District network for transmission or storage) may be reviewed and/or accessed by authorized district officials for purposes related to District business. The district has the authority to access and inspect the contents of any equipment, files or email on its electronic systems.

Students

Email services are available for students to support learning and for communication by and between the district and themselves. The services are provided only while a student is enrolled in the district and once a student's electronic services are terminated, students may no longer access the contents of their mailboxes.

Student email users are advised that electronic data (and communications using the District network for transmission or storage) may be reviewed and/or accessed in accordance with the district's Acceptable Computer Use Procedure and Regulation. The district has the authority to access and inspect the contents of any equipment, files or email on its electronic systems.

Alumni and Others

Individuals with special relationships with the district, such as alumni or official visitors are granted limited email privileges, including an email address, commensurate with the nature of their special relationship. The district is free to discontinue these privileges at any time.

3.2 Acceptable Email Use

Email users have a responsibility to learn about and comply with the district's Computer and Network Use policy (BP 3720) and related administrative procedures. Violation of district policies and administrative procedures may result in disciplinary action dependent upon the nature of the violation. Examples of prohibited uses of email include:

- Intentional and unauthorized access to other people's email;
- Sending "spam," chain letters, or any other type of unauthorized widespread distribution of unsolicited mail;
- Use of email for commercial activities or personal gain (except as specifically authorized by district policy and in accord with district administrative procedures);
- Use of email for partisan political or lobbying activities;
- Sending of messages that constitute violations of the district's Standards of Student Conduct or the Employee Responsibilities & Rights handbook.
- Creation and use of a false or alias email address in order to impersonate another or send fraudulent communications;
- Use of email to transmit materials in a manner that violates copyright laws.

District electronic mail services may not be used for unlawful activities; commercial purposes; personal financial gain; personal use inconsistent with this document; or uses that violate other district policies, administrative procedures or guidelines.

District electronic mail services may be used for incidental personal purposes provided that, in addition to the foregoing constraints and conditions, such use does not:

- Directly or indirectly interfere with the district operation of computing facilities or electronic mail services;
- Burden the district with incremental cost; or
- Interfere with the e-mail user's employment or other obligations to the district.

Electronic mail users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the district or any unit of the District unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing the District. An appropriate disclaimer is: "These statements are my own, not those of Citrus College."

District e-mail users shall not employ a false identity. Email might, however, be sent anonymously provided this does not violate any law or these guidelines or any District policy, and does not unreasonably interfere with the administrative business of the District. An example of such anonymous e-mail would be e-mail sent by a system administrator using the Postmaster account.

District e-mail services shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities, or unwarranted or unsolicited interference with others' use of e-mail or e-mail systems. Such uses include, but are not limited to, the use of e-mail services to:

- Send or forward e-mail chain letters;
- "Spam," that is, to exploit list servers or similar broadcast systems for purposes beyond their intended scope to amplify the widespread distribution of unsolicited e-mail;
- "Letter-bomb," that is, to resend the same e-mail repeatedly to one or more recipients to interfere with the recipient's use of e-mail.

The district email will be delivered to a user's district managed mailbox. Email is not considered a secure mechanism and should not be used to send information that is not considered public.

3.3 Message Content

The official bulk service is restricted to those messages that meet one of more of the following tests:

- The message is essential to the proper execution of daily business.
- It notifies the community of significant events or changes in governance, policy, and practice.
- It alerts the community to situations around health and safety (examples include crime, weather or natural disaster alerts).
- It keeps segments of the community informed of their business. For example, in the case of official committees, the messages could contain minutes, updates, and announcements. This would include instructors who send official email to the students in their courses.

Announcements that do not meet these requirements of urgency and/or critical information, should seek other methods of relaying their information.

3.4 List ownership

It is acknowledged that the membership list of particular groups belongs to the offices that maintain them. As such, these list owners have the right to communicate with their constituents as they deem best, and may send out bulk email to those groups without need of further authorization. In addition, these offices can delegate to other offices or individuals the authority to communicate with these groups. In general, it is expected that this delegation will parallel the existing delegation models of paper-based mailings.

3.5 Requests for Bulk Email

Requests to send out bulk email to the following populations must have the approval of the owning offices and must meet the criteria listed above. Contact the Help Desk to coordinate any requests only if they meet these requirements. Bear in mind that a request will not be honored if it does not meet the requirements specified above.

The following chart indicates the authorizing offices and provides a summary of acceptable use bulk emailing:

Authorizing Department	Mailing Lists	Examples of General Use
President's Office	All faculty All staff All students	Alerts, significant announcements, policy changes impacting all or most of the community
Vice-Presidents of Finance and Administrative Services, Academic Affairs, and Student Services	All faculty All staff All students	High level announcements not including routine or repetitive announcements, related to respective area
Director of Human Resources	All faculty All staff	Matters related to employment (benefits, payroll, campus closure)
Director of Communications or Executive Director of Development and External Relations	All faculty All staff All students	Alerts, significant announcements, policy changes impacting all or most of the community
Chief Information Services Officer	All faculty All staff All students	High level announcements not including routine or repetitive announcements

3.6 Security and Privacy of Email

The district attempts to provide secure, private and reliable email services by following sound information technology practices. However, the district cannot guarantee the security, privacy or reliability of its email service. Such confidentiality may be compromised by law or policy, including these guidelines, by unintended redistribution, or because of inadequacy of current technologies to protect against unauthorized access. Users should exercise extreme caution in using e-mail to communicate confidential or sensitive matters.

3.7 Archiving and Retention

The District does not maintain central or distributed electronic mail archives of all electronic mail sent or received. Electronic mail is normally backed up, only to assure system integrity and reliability, not to provide for future retrieval, although back-ups may at times serve the latter purpose incidentally.

3.8 Best Practices in Use of Email

The following guidelines describe best practices for email use.

- Confidential Information - When sending confidential information, it is strongly recommended that the user encrypt the message. Users transmitting confidential documents as email attachments must password protect them.
- Viruses and Spyware - District email users should be careful not to open unexpected attachments from unknown or even known senders, nor follow web links within an email message unless the user is certain that the link is legitimate. Following a link in an email message executes code that can also install malicious programs on the workstation.
- Identify Theft - Forms sent via email from an unknown sender should never be filled out by following a link. Theft of one's identity can result.
- Password Protection - The district requires the use of strong passwords for the protection of email. A strong password should contain digits or punctuation characters as well as letters. Administrative procedure AP 3721, Computer and Network Account and Password Management, describes the procedures for password creation and management.

3.9 Electronic Mail Standards

The district provides central electronic mailbox services, with spam and virus filtering, and a @citruscollege.edu email address. The following are the current standards for handling the inbound and outbound delivery of email through the central services.

Inbound email is scanned for content that may be characterized as SPAM. Where SPAM characteristics are found, the message may be tagged or quarantined. Email is also routinely scanned for viruses and other malware. The scanning for malware may also lead to a modification of email, or further consequences, as explained below.

Because of the potentially harmful nature of the content of many messages or attachments, the district:

- Does not deliver messages containing attachments that have been identified as worms by our current anti-virus solution;
- Deletes attachments that are identified as containing viruses by our current anti-virus solution;
- Blocks messages from external mailers that do not provide the proper identification per DNS. (Some spammers make use of improperly configured SMTP servers in an attempt to mask their true identity.)
- Blocks other incoming email that exhibits characteristics of spam, viruses, trojans, or anything else when it could threaten campus network infrastructure or services.

Outbound email Messages up to 10 MB in size (including attachments) may be sent through the district's email services. Outbound email will be scanned for viruses.

Board Approved 05/04/10