

University Policy 600.03
E-MAIL

Responsible Administrator: Vice President for Planning, Assessment and Information Services

Responsible Office: Office of Information Technology

Originally Issued: October 2011

Revision Date:

Authority: Office of the President

Policy Statement

The e-mail system at Claflin University is an official means of communication. Emails are routinely sent to the “Claflin University Family” and the Claflin University “Student Body” and /or other subgroups of individuals affiliated with the University. It is the policy of Claflin University to ensure appropriate, safe, and effective e-mail use.

Statement of Purpose

6.

Other Relevant E-mail Usage includes (but is not limited to):

1. Auto Responder Feature - As a means to provide good customer service, University management recommends the use of the auto responder feature if the user will be out of the office for a minimum of a workday. The auto-response should notify the sender that the user is out of the office, the date of the user's return, and who the sender should contact if immediate assistance is needed.
2. Confidential Data – E-mail is an insecure means of communication. The University requires that any e-mail containing confidential information, regardless of whether the recipient is internal or external to the University network, be encrypted. A user should consult personnel in the Office of Information Technology regarding the encryption of confidential data.
3. Data Leakage - E-mail poses a particular risk to the control of the University's data. Unauthorized e-mailing of University data, confidential or otherwise, to external e-mail accounts for the purpose of saving this data external to the University's systems is prohibited. If a user needs access to information from external systems (such as from home or while traveling), rather than e-mailing the data to a personal account or otherwise removing it from the University's systems, the user should notify his or her supervisor who in turn will notify the Office of Information Technology.
4. E-mail Contents – University e-mail users should not open e-mails that appear suspicious. If a user is particularly concerned about an e-mail, or believes that it contains illegal content, he or she should notify his or her supervisor.
5. E-mail Deletion - To reduce the University's need to store and to backup unnecessary email messages, University management encourages users to periodically delete e-mails which are no longer needed. However, the University strictly prohibits deleting e-mails in an attempt to hide a

9. E-mails to Multiple Recipients – The clarity of communications is important. Users should use caution in sending e-mail to make sure that all recipients included in an e-mail are necessary; for example, some recipients may need to be aware of parts of an e-mail but not the e-mail in its entirety; in such cases, it may be beneficial to verbally communicate with those individuals rather than communicating through e-mail.
10. Opening E-mail Attachments - Viruses, Trojans, and other malware can easily be delivered as an e-mail attachment. University users should be careful when opening attachments that are unexpected and/or from unknown sources.
11. “Reply All” E-Mail Feature –E-mail users should use the “reply all” e-mail feature sparingly. The feature should not be used if only the original sender(s) or particular (not all) persons need to receive the reply.
12. Sending E-mails - Careful sending of an e-mail will help the University avoid the unintentional disclosure of sensitive or non-public information. An e-mail must be addressed and sent carefully. Users must take extreme caution when typing in addresses, particularly when email address auto-complete features are enabled.
13. Sending Large E-mails - E-mail systems are not designed to transfer large files and as such e-mails should not contain attachments of excessive file
mail users limit
attachments to 10 megabytes or less.
14. The Three Email Rule - If you exchange

20

set up an auto-response to notify the sender that the user is no longer employed by the University.

Any individual found to have violated this policy is subject to disciplinary action which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the University may report such activities to the applicable authorities. If any provision of this policy is found to be unenforceable or voided for any reason, such invalidation will not affect any remaining provisions, which will remain in force.

An individual who has questions about this e-mail policy should contact the University's Office of Information Technology.

E-mail Use/Etiquette

E-mail has a unique protocol r