

October 2011

## 8.103 Email Use Policy

Follow this and additional works at: [http://aura.antioch.edu/policies\\_800](http://aura.antioch.edu/policies_800)

---

### Recommended Citation

"8.103 Email Use Policy" (2011). *8.000 Information Technology*. 3.  
[http://aura.antioch.edu/policies\\_800/3](http://aura.antioch.edu/policies_800/3)

This Article is brought to you for free and open access by the Antioch University Policies at AURA - Antioch University Repository and Archive. It has been accepted for inclusion in 8.000 Information Technology by an authorized administrator of AURA - Antioch University Repository and Archive. For more information, please contact [dpenrose@antioch.edu](mailto:dpenrose@antioch.edu), [wmcgrath@antioch.edu](mailto:wmcgrath@antioch.edu).



Type of Policy <input checked="" type="checkbox"/> <b>University</b> <input type="checkbox"/> <i>Campus</i> <input type="checkbox"/> <i>Department/Unit</i> <input type="checkbox"/> <b>Interim</b>		<b>Email Use Policy</b>  <b>Policy 8. 103</b>	
<b>Information Technology Policies</b>		Effective date: <b>June 7, 2008</b>	
<b>Policy History:</b>	<b>Approved by:</b>	<b>Resolution #</b>	<b>Date</b>
Approved	Board of Governors	6.7.08:5	June 7, 2008
Revised (Non-substantive)	Office of University Counsel	N/A	May 31, 2017
<b>Responsible Office</b>	<b>Responsible Administrator:</b>	<b>Contact information</b>	<b>Applies to:</b>
University Chief Financial Officer	University Chief Financial Officer	937-769-1304	All Faculty, Visiting Faculty, Staff, Students and all external persons as indicated in this policy

## I. Introduction

### A. Purpose

The email system at Antioch University is for the use of students, faculty and staff. The purpose of the system is to facilitate teaching and learning and to conduct University business.

This policy provides rules and regulations for the use of Antioch's email system. However, Antioch's Policy #8.101 Acceptable Use of Computing Resources is the overriding policy for use of Antioch's Computing Resources. That policy also applies to email. If there are inconsistencies between Antioch's Acceptable Use Policy and this policy, the Acceptable Use Policy will take precedence.

## **II. Who May Use the System**

A. All students, staff, and faculty will be assigned email accounts and may have general access to the system as long as they maintain their relationship with the University. These accounts will typically be generated and deleted automatically based on a person's status within the Datatel information system. In exceptional circumstances, faculty email accounts may be set up before their status is confirmed within Datatel.

B. If it is in the best interest of the University, other persons may be given temporary or permanent Antioch email accounts. Examples would include visiting faculty, contractors or consultants.

C. Students who graduate from the University will normally be allowed to maintain and use their Antioch email accounts as Alumni. However, Alumni accounts that remain inactive for a period of 420 days or longer will be deleted. Students who leave the University without graduating will have their email accounts disabled. These accounts and their contents will be deleted one month after access has been disabled.

D. Staff and faculty who leave the University will have their email accounts disabled. Supervisors of departing staff or faculty will have access to these disabled accounts. The supervisor will be expected to review the contents of the email accounts and determine which emails are required to be preserved. The email account and its contents will be deleted three months after the departure of the staff or faculty person or when the supervisor has indicated that they have finished reviewing the contents of the email account. If a person who leaves the University holds multiple roles (e.g. a staff member who leaves is also an active student), then access to their email account will not be disabled.

E. Each user will only be allowed a single account; however each account may have more than one associated email address. The only exceptions to this rule will be persons who require multiple accounts as part of their responsibilities for maintaining the system or if departments or programs need multiple accounts for conducting their business.

F. A person's access to the email system may be suspended if their use contravenes any provisions of this policy or of the University's Acceptable Use Policy 8.101, or at the request of the appropriate authorities within the senior administration of the University.

## **III. Use of the Antioch Email System**

A. Antioch University email is provided for purposes related to the University's mission of education, research, and public service. Email should be used for purposes related to studies, instruction, discharge of duties as employees, official business with the University, and other University sanctioned activities. Incidental personal use of email is allowed only if that use does not interfere with the primary purpose of the system, does not interfere with the individual's primary job function, and does not cause any appreciable additional or direct cost to the University.

B. The University's email system cannot be used for personal monetary gain or for commercial purposes that are not directly related to University business.

C. The Antioch email system is an official means of communications for Antioch University. The University will consider faculty, staff or students to be duly informed and in receipt of notifications and correspondence sent by the University to user email accounts. Faculty, staff and students should frequently access their University assigned email account for official information.

D. Individuals who elect to have email message forwarded to an off-campus account are responsible for the proper functioning of the off campus account. Antioch is not responsible for delivery problems related to forwarding to off-campus accounts. Email addresses which may receive messages containing confidential information should never be forwarded to email addresses outside the Antioch Email system.

E. Users should become familiar with and follow the safe email practices outlined in Appendix A to this Policy.

F. The Antioch email system will not be used for:

- Sending documents in violation of copyright laws.
- Sending messages to harass or intimidate others or to interfere with other people's legitimate use of the email system.
- Constructing an email communication so it appears to be from someone else (i.e. "spoofing").
- Sending an excessive number of unsolicited email messages (spam) or participating in electronic chain letters.
- Any purpose restricted or prohibited by federal, state, or local laws or regulations.

#### **IV. Privacy and Confidentiality**

A. An email account may only be used by the person to whom it is issued.

B. Each person issued a password for accessing their account is required to keep the password secure and confidential (i.e. not share it). If a person suspects that their password has been compromised they should change their password immediately. A person is responsible for any email sent from their email account. Although the email system is for official University communication and all messages remain the property of the University, the University does not routinely monitor the content of email or search email archives. However, there are circumstances when the University will access email or release email to other parties. These situations may include, but are not limited to, the death of the account holder, when an absent or terminated employee's email account contains email associated with his or her job responsibilities, or during the course of legal or disciplinary investigations.

C. Email records in either electronic or printed form are subject to federal and state laws as well as University records management policies, including their provisions regarding retention and disclosure. The majority of email is ephemeral correspondence that should be retained until read and then deleted. Other email that contains records and documents identified in the Records Retention Policy – Record Retention and Disposal Schedule should be retained and disposed of as defined in that schedule.

D. System administrators will manage the email system in a manner that is consistent with the system’s importance. In connection with their responsibilities, professional staff members may on occasion need access to or monitor parts of the system and thereby gain access to certain electronic mail messages. System Administrators will respect the privacy of personal communications encountered on the system, however if during the course of routine duties they encounter information that indicates a breach of this policy or of any laws, they will report the existence and source of the information to the proper authorities.

E. Email sent to email addresses outside the Antioch email system is not considered to be secure. Therefore email sent outside the Antioch email system should not be used for transmitting confidential information (for example social insurance numbers or passwords) unless that information is encrypted.

**V. Email Retention and Reliability**

A. Email messages are stored on a central server. The Antioch email system is normally backed up to assure system integrity and reliability, not to provide for future retrieval of individual communications, although backups may at times serve the latter purpose incidentally. System Administrators are not required by this policy to routinely retrieve electronic communications records from such backups for individuals. A person should not assume that all record of an email message is gone if it is deleted from his or her account. Antioch does not wish to be the arbiter of the contents of electronic communications. However, the amount of unsolicited and often times offensive emails being sent (spam) requires the University to take steps to filter email being delivered to University email accounts. The University cannot always protect users from receiving email messages they might find offensive. There may also be occasions when email gets filtered out that is legitimate and that the user wished to receive.

B. State and Federal law and court rules may provide that email sent or received by University personnel must be retained for some period of time. The system administrators will endeavor to retain or archive email as required by law or rule.

**VI. Review Schedule:**

This policy will be reviewed annually by the Office of University Counsel.

**Policy Cross Reference**

Acceptable Use of Electronic Resources	Policy # 8.101
--	----------------

## Appendix A

### Safe Email Practices

1. Do not use University email to send any of the following information to recipients outside the Antioch.edu domain:

- Student grades or assessments;
- Student SSN or Datatel ID numbers or other FERPA protected information;
- Employee SSN or Datatel ID numbers;
- Financial information such as bank routing/account numbers or credit card numbers;

(Even for communications within the Antioch.edu domain, use email for sending the above information only when absolutely necessary and no reasonable alternative exists. If the email recipient has their email forwarded, you may be sending the Email outside the Antioch.edu domain without realizing it.)

2. Do not use the University email account for personal email when possible.

(Your email account is provided to you by the University. The University retains ultimate ownership over the account and any information/emails held within it.)

3. Do not access your University email from an unsecured machine (i.e. public machine) unless you are sure that your session is not being cached. Be sure that you are signed out of your session and close down the web browser when finished.

4. Do not access your University email from an unprotected machine (i.e. without spyware/antivirus protection). You are required to take steps to ensure the protection and integrity of the email in your account including ensuring that such information is protected from spyware and computer viruses.

5. Do not share your University email password with anyone. Your University password is more than just the key to your email. It would give the user access to any number of University systems and data. It is a restricted practice to share passwords between University employees and others.

6. Do not open attachments in your University email unless you are absolutely sure about what they are and who they came from. Opening an unfamiliar attachment can leave your machine vulnerable to a virus attack.

7. Do not allow your web browser (Explorer, Firefox, etc.) or email program to “remember” your University email password. If you do, anyone who gains access to your computer will gain access to your email account.

8. Do call the help desk if you have any questions concerning your email account or any security practices which you should be exercising.