



**FAS**  
INFORMATION  
TECHNOLOGY

---

# **FAS Information Technology**

## **Email Guidelines for FAS Accounts** November 2008

---

---

## Table of Contents

Quotas .....	3
Mailbox Maintenance/Data Management.....	4
Automatic Backups.....	4
Retention.....	4
Attachments .....	4
Mailing Lists.....	5
Email Clients and Webmail .....	5
Spam Blocking.....	5
Antivirus Scanning.....	5
Passwords.....	6
Confidentiality/Security .....	6
Acceptable/Appropriate Usage .....	6
Account Support .....	7

*To ensure that email services remain accessible and reliable for all FAS users, the following Policies and Guidelines apply to all FAS accounts.*

## Quotas

An FAS email account is restricted by three separate quota limits; the disk quota, the inbox quota, and the file quota.

The overall *disk quota limit* applies to the total server space allocated to each unique account. Disk quota usage is comprised of all the files in an account's home directory on the server, including the inbox, saved email folders, and any other files saved in the account, such as website files or research work (possibly copied to the server using an SFTP program such as SecureFX or MacSFTP).

Exceeding the disk quota limit will prompt an automated warning message to be sent from FAS Information Technology (FAS IT) to the account holder. At that time, the user account will also automatically receive a temporary quota extension of an additional 50 MB. As long as the account remains over its original quota, the user will continue to receive daily automated warning message. *Exceeding the 50 MB extension will prevent the account from receiving any new email messages.* All messages intended for the recipient will be returned to the sender as undeliverable. Email will remain non-functional until the account is brought back within the disk quota limit.

Independent of the overall disk quota, each FAS email account is also subject to an *inbox quota limit* of 40 MB. This limit exists to ensure email client software can open the inbox without suffering lengthy delays or crashing. If an inbox exceeds the 40 MB limit for more than two days, the user will be sent automated email warnings for each of the next 14 days while the inbox is over quota requesting that the user reduce the inbox size below 40 MB. Failure to reduce the inbox below the 40 MB threshold in the allotted time will result in the contents of the inbox being moved to a separate email folder named "Old-Inbox-[date]" where [date] is the date the messages were moved from the inbox. *No messages will be lost by this process, as the old inbox will remain accessible on the mail server.*

Accounts are also subject to a *file quota limit* of 10,000 files. Exceeding this limit will prompt automated warning messages, as well as an automatic quota extension to 20,000 files. As long as the account remains over its original quota of 10,000 files, the user will continue to receive daily automated warning messages. Exceeding the quota extension will prevent the user from adding additional files. Email, however, will continue to function normally. Each mailbox folder, including the inbox, is considered a single file by the email server.

## Mailbox Maintenance/Data Management

It is the responsibility of the user to implement such maintenance steps as are necessary to keep the user's inbox below the 40 MB threshold and the overall disk usage below the account disk quota. FAS IT recommends that users regularly archive all mailbox folders, including their inbox.

## Automatic Backups

All user accounts are backed up by FAS IT on a nightly basis between midnight and 4:00 AM. The backup process captures the entire contents of the user's home directory. FAS IT currently maintains a 14-day backup window. Requests for restoration of an account backup should be made via the FAS IT Service Desk at 5-9000 or via email to [help@fas.harvard.edu](mailto:help@fas.harvard.edu). Because backups happen only once a day, users need to be aware that any email or files that arrive or are created after the previous night's backup and are subsequently deleted prior to the next night's backup will not be available for restoration.

## Retention

Per the Harvard University General Records Schedule (GRS), the University mandates **no** minimum retention period for email. Users are not required to save any email message or attachment for any period of time.

## Attachments

The FAS email system automatically rejects emails messages with attachments that are considered dangerous. This includes attachments with the following file extensions:

.bat	.cpl	.pif	.vb	.wmf
.cmd	.exe	.scr	.vbs	.wsf
.com	.inf	.shs	.wcs	.wsh

Email messages containing an attachment with one of the above extensions will be rejected, with the sending system receiving an explanation as to why the email was rejected.

Additionally, to ensure successful transmission and reception of emails with attachments, the FAS email system limits the total transmission size to 15 MB. This limit applies to the total size of the email message and all of its attachments.

*Note:* When sending email using FAS webmail, the transmission size is limited to 2 MB.

## Mailing Lists

FAS IT provides mailing list capabilities for Faculty and Staff. A list administrator application, along with further information about list functionality, can be found at <http://www.fas.harvard.edu/fasit/myaccount/forms/MailingList.pdf>

## Email Clients and Webmail

FAS IT currently recommends the following email clients:

- Outlook (Windows)
- Entourage (Macintosh)

Users who are not using the current versions of this software should contact the FAS IT Service Desk to obtain the latest version. Users wishing to switch to a different email client, such as from Thunderbird to Outlook, should contact the Service Desk for assistance with moving existing mail folders to the new software.

FAS email accounts can be accessed via the Internet using any web browser at <http://webmail.fas.harvard.edu>. Webmail is secure and works over both broadband and dial-up connections.

## Spam Blocking

FAS IT uses an industry-standard external spam blocking list to automatically reject email sent from the IP addresses of known spammers. When spam is blocked, the sending system is sent a message explaining the reason for the rejection.

In addition, the FAS email system provides server-based spam filtering on an “opt-in” basis. Details about the available spam protection, as well as instructions for enabling the filtering software can be found by selecting the “Block Email” link at <http://www.fas.harvard.edu/fasit/myaccount/>

## Antivirus Scanning

Desktop antivirus (AV) software is available from FAS IT for both Windows and Mac operating systems. All users are strongly encouraged to install desktop AV software and maintain current virus definitions. Please visit the FAS IT software downloads page at <http://downloads.fas.harvard.edu/download> for more information.

As a supplement to desktop AV software, FAS IT also provides an “opt-in” server-based virus scanning process for email messages. Details and configuration instructions can be found at <http://www.fas.harvard.edu/fasit/myaccount/> by selecting the “Scan Email for Viruses” link.

## Passwords

The FAS email system has the following minimum requirements for password acceptability:

- Passwords must be a minimum length of 8 characters, and a maximum length of 16 characters.
- Passwords must be a combination of upper and lower case letters including at least one numeric and/or special character.
- Passwords must contain at least five different characters.
- Passwords must NOT be names or words.
- Passwords must NOT contain more than four consecutive numbers.
- Passwords must NOT be a date.
- Passwords must NOT be based on a single word, or consist of two words separated by a space, hyphen, or underscore character.
- Previous passwords cannot be reused within 12 months where password changes are required.

In addition, FAS IT encourages all users to increase their account security by periodically changing their password. An FAS IT employee will never ask a user for their account password.

Password resets can be requested through the FAS IT service desk at 5-9000, but the user must provide proof of identity. FAS IT will not reset passwords for third parties calling on behalf of an FAS account user, nor will password reset information be sent via email.

## Confidentiality/Security

To meet Harvard security and privacy requirements for transmission of confidential information (including passwords), FAS IT requires the use of SSL encryption for all client connections to the inbound mail servers (both IMAP and POP). Additionally, webmail access is also secure, as the client connection is made via HTTPS.

## Acceptable/Appropriate Usage

Use of the FAS email system is subject at all times to the general FAS “Computer Rules & Responsibilities” as well as the “Additional Policies from FAS Information Technology”, as documented at [http://www.fas-it.fas.harvard.edu/services/student/policies/rules\\_and\\_responsibilities](http://www.fas-it.fas.harvard.edu/services/student/policies/rules_and_responsibilities)

---

## **Account Support**

FAS IT provides service desk support for all FAS users between 8:00 AM and 6:00 PM Monday through Friday, with the exceptions of University recognized holidays and recess periods. During extended holidays and recess periods, FAS IT will provide emergency contact information for major outages and mission-critical technical problems. Recorded network status information can also be obtained by calling 617-495-9000. Calls that are not deemed to be emergencies during non-business hours will be queued for service during normal business hours.