
Subject:	<i>Internet & E-mail Use Policy</i>	Policy Section #	1
Applicable to:	<i>All faculty, staff, and students</i>	Pages:	3
Author:	<i>Administration/Information Services</i>	Submitted Date:	11/6/02
Review:	<i>Administrative Council</i>	Review Date:	11/6/02 12/12/02
Approval:	<i>Faculty Council Cabinet</i>	Approval Date:	2/13/03 2/20/03
		Replaces version Dated:	New

POLICY:

The University of Minnesota provides access to e-mail and Internet to eligible students, staff, and faculty. Email accounts and passwords are assigned to individuals and are not to be shared. It is the responsibility of individuals to make sure their passwords are secure. The CVM has developed the following guidelines to supplement the U of M's e-mail and Internet policies. All authorized users of these resources are required to use them in an effective, efficient, and responsible manner.

PROCEDURE:

- Users must be aware of User Rights and Responsibilities, which outline liability for personal communication, privacy and security issues, and consequences of violations.

Review the complete policy online at:

www.fpd.finop.umn.edu/groups/ppd/documents/policy/Acceptable_Use.cfm

Related guidelines are online at:

www.fpd.finop.umn.edu/groups/ppd/documents/appendix/useguidelines.cfm

To report suspected policy violations:

www.fpd.finop.umn.edu/groups/ppd/documents/procedure/rept_violations.cfm

- The College of Veterinary Medicine will use the following procedures:

A. Email

The principal purpose of electronic mail (email) is for educational and business communications. Use of e-mail for personal gain, personal business, or to commit fraud is prohibited. Email should be treated like all other verbal or written business communications. Appropriate language and standards of decency must be used. Offensive, demeaning, defamatory, harassing or disruptive messages are prohibited.

Email that contains confidential or proprietary information must be treated as confidential. No one shall provide email access to an unauthorized person or access another user's email without authorization.

- Students, faculty, and staff will be notified of collegiate information via their U of M account.
- Certain faculty and employees have access to send global CVM messages. Only messages pertaining to seminars, meetings, public relations, student activities (fundraising or other student related activities), collegiate activities, or Hills Pet Food Product, may be sent.

- ii. No emails soliciting funds (other than Campaign Minnesota, Annual Fund Drive, or CVM Fundraising activities), sales of products, or personal items are allowed. A bulletin board is available across from the CAPS Departmental Offices for posting notices concerning adoptions of pets, sale of items, etc.
- iii. Emails should include the topic in the message line.
- iv. Global emails should include the notice within the body of the email. Attachments should not be used.
- v. No personnel issues should be communicated through e-mail without first consulting Human Resources.

B. Internet Access

Any connection between the CVM and the Internet presents an opportunity for non-CVM employees or students to access University systems and information. Internet is to be used for increasing productivity rather than for non-business purposes or to increase educational knowledge.

Anti-virus software is installed on all CVM computers. Users are responsible for using the software to explicitly check file attachments and downloaded files.

Examples of permitted uses:

- i. Sending and receiving business or educational-related email.
- vi. Sending and receiving short personal email.
- vii. Subscription to an Internet mailing list if the subscription is educationally related and does not generate numerous messages.
- viii. Downloading files from business or educationally-related sites must be scanned for viruses.
- ix. Reading pre-approved newsgroups for business or educational purposes.

Examples of discouraged/non-permitted uses:

- i. Sending or arranging to receive file attachments in personal email.
- ii. Posting, viewing, downloading or otherwise receiving or transmitting offensive, defamatory, pornographic or sexually explicit material.
- iii. Engaging in computer "hacking" or other related activities.
- iv. Conducting personal business such as buying and selling personal items.
- v. Downloading files containing software, games, and attachments.
- vi. Sending sensitive information through Internet email.
- vii. Posting submissions to non-professional newsgroups.

C. Adding Software

Most proprietary software licenses have legal restrictions prohibiting unauthorized use and copying. Each user is responsible for compliance with these legal restrictions. CVM Information Services (Helpline: 5-7700) is available to install, configure, and track all software and associated licenses loaded on CVM computer equipment. It is recommended that only Information Services staff load software.

OVERSIGHT/FOLLOW THROUGH:

1. Each user will be responsible for activity performed using their password and keeping their password secure.
2. Users should contact Information Services before downloading any file if the user has questions about, a potential virus, or reason to believe that the file poses particular risks.
3. Alleged policy violations of the CVM or U of M policies will be referred to appropriate University investigative and disciplinary units.
4. Misuse in sending global e-mail messages will result in privilege withdrawal.