University Policies

- Active Policy List
- Instructions for Creating a Policy
- Policies Under Consideration
- Archive Policy List
- Frequently Asked Questions
- How to use this page
- Contact Us
- Board of Trustees Policies

Responsible/Acceptable Use of Computing Services

Policy Number	ITS-001
Effective Date	January 11, 2006
Responsible Office/Person	CITS
Related Policies	
Additional History	
Additional References	

Responsible/Acceptable Use of Computing Services

Summary of University Data and Computing Use Requirements
Since many users share information data and technology, and because of legal and ethical requirements, all users need to be aware of their responsibilities related to data and computing at the University of Massachusetts. Please familiarize yourself with summary information below as well as the University of Massachusetts Data and Computing Policies and Guidelines for use of information technology at:

http://www.massachusetts.edu/policy/datacomputingpolicies.html.

Remember that observing these guidelines will help to make computing and use of the network services more pleasant for all users. Please use the University data and computing FAQs (available at http://www.massachusetts.edu/SecurityAwareness/securityawareness.html) to clarify policy, guideline, and use questions.

General
The computing resources of the University are provided to support academic and administrative users. Users should use their access to University data for approved purposes only.

The same standards of intellectual honesty and plagiarism apply to software as to other forms of published work. For example, individuals should not copy another's computer file and submit it as theirs nor should they work with someone else on an assignment, sharing the computer files and then submit that file, or a modification thereof, as their own individual work.

University data and computing users should properly create, access, use and dispose of University data based on the data's classification (e.g., Confidential, Restricted, Unclassified, etc.). See:
http://media.umassp.edu/massedu/policy/DataComputingStandard.pdf
for classification information.

All computer systems accessing University data and networks must have antiviral software installed and continuously enabled so the spread of viruses within the University computer systems is prevented. Authorized users downloading software from a network or installing software from a disk/CD-ROM, must check the software for possible virus infection before they use it.

Email Accounts
All students and employees may obtain an email account. Students are free to

use email for personal use. Email is made available to employees for the purpose of conducting University related business, but occasional social/personal use is allowed providing it does not interfere with an employee's job duties or University business or operations.

The University considers a personal email message to be private; however, the University has the right to look at any documents/files including emails stored, sent or received on/across University computer systems and networks if necessary for University business. Please note that due to information technology, the privacy, security, and authorship of documents and messages stored in and transmitted via electronic media cannot be guaranteed. Additionally, emails can be stored, copied, printed or forwarded by recipients. As such, you should not write anything in an email that you would not feel just as comfortable putting in a memo. Signature files should follow the same professional guidelines as a business card. The University does not routinely monitor the content of electronic communications. The University has the responsibility and authority to access, review and release electronic information that is transmitted over or stored in University systems. The University also has the responsibility and authority to monitor individual accounts if the University determines this monitoring is necessary for legitimate administrative purposes.

Email users must use email and any other electronic communications tool in a responsible manner consistent with other business communications (e.g., phone, correspondence, business cards, etc.). Responsible email use includes: not "rebroadcasting"/sending an email to a third party obtained from another individual that the individual reasonably expects to be confidential; not posting materials that are of a fraudulent, defamatory, harassing, or threatening nature; not sending chain emails or spamming; and not unlawfully soliciting or exchanging copies of copyrighted software via email.

Security
Be particularly careful of your password. Do not give your password to anyone or type your password when someone is watching. Do not write down your password or store it in batch files, automatic login scripts, terminal function keys, or in other locations where another person might discover them. Once someone has your password it is possible both to look in your directory and to use your username for malicious purposes.

Do not log on to a computer/network with your ID/password and let another person use your access. Make sure you log off the computer while you step away from your desk for an extended period of time. Staying logged on leaves your ID and the system vulnerable for misuse. You are responsible for all activities that take place from your account.

Although the University makes a reasonable effort to protect files stored on the university systems from being accessed by anyone other than authorized individuals, the University cannot guarantee the confidentiality of any of these files.

The University recommends the installation of personal firewalls on all University owned systems and any computer accessing University computer and network systems.

Privacy
The University systems may record information about each user session. Information recorded includes the username/operator ID associated with the session, the login and logout dates and times, and the amount and kind of computer resources used during the session. This information is used for legitimate University purposes including issues of law, abuse, security or system managements.

When the University has reasonable belief that system security or system operation has been compromised or it has been used for unauthorized activities, the University has the responsibility and authority to review the

contents of all computers including files, programs and emails.
Remember that any printouts in public places are likely to be seen by others.

Computer Abuses
You can expect to lose your computer account, be disconnected from the network, face disciplinary action up to and including termination, possibly be charged with criminal offenses (either by the University or third parties such as the Record Industry) or have civil action taken for computer abuses such as:

- Unauthorized access of another person's computer or email account
- Unauthorized access of University data or systems
- Misrepresenting either the University or your role at the University to obtain access to data or computer systems
- Using computing resources to access any other computer system (on or off-campus) without authorization
- Disseminating any confidential information unless such dissemination is required by the individual's job at the University
- Deleting or copying files from another person's computer account
- Taking advantage of another user's naiveté to gain access to his/her files
- Preventing someone from using his/her account by changing the password or other tampering
- Sending offensive, harassing or threatening messages or repeated unsolicited mail
- Abusing the networks to which the University belongs
- Use of the computer or network for monetary gain, political purposes or illegal activities
- Illegal use of downloaded copyrighted materials including print, audio, and video
- Intentionally writing, producing, generating, copying, propagating or attempting to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer's memory, file system, or software unless such action is part of authorized research or testing. Such software is often referred to as a virus, worm, Trojan Horse, or some similar name
- Illegally distributing copyrighted software within or outside the University through any mechanism, electronic or otherwise.
- Any activity that interferes with the rights of others

If any individual receives an email that he or she considers harassing, threatening or offensive, please contact the Director of Human Resources, 508-999-8061; the Assistant Chancellor for Equal Opportunity, 508-999-8008; or the University's Information Technology Security Officer, 508-999-8528.
Reports of abuse to your account can be made by contacting your system administrator: email Computing and Information Technology Services at cit_am@umassd.edu or call 508-999-8532.
Procedures to insure the responsible use of technology

University of Massachusetts Dartmouth • 285 Old Westport Road • Dartmouth, MA 02747-2300
Phone: 508 999-8000 • Privacy • Contact UMass Dartmouth

+