

## **University of Massachusetts Responsible/Acceptable Use of Computing and Data Resources Standards**

University data, computers and computer related resources are valuable assets that are relied upon heavily for academic, information and decision-making needs. University students and staff rely on the security of the computer systems to protect instructional, research, personal, operational and other sensitive data maintained in those computer systems. It is essential that these systems are protected from misuse and that both the computer systems and the data stored in them be accessed and maintained in a secure environment.

This document outlines the standards for the acceptable use of University data (regardless of the medium on which it resides and regardless of its form), and computing systems/resources which include, but are not limited to: hardware, software and communications equipment (e.g. voice and data networks, servers, routers, modems, etc.) used in the processing, transmission and storage of electronic data. This document does not waive any claim that the University may have to ownership or control of any hardware, software, or data created on, stored on, or transmitted through University computing systems.

These standards comply with and are based on the laws of the Commonwealth of Massachusetts and the United States and other regulatory agencies. Other University Standards/Procedures ([Data and Computing Standards](#), [Data/System Administrator Responsibilities and System Requirements](#), etc.) and/or campus procedures may impose certain restrictions that are not specifically covered by state and federal law, or other regulations.

Definitions related to this document can be found in the [Data and Computing Definitions](#).

These standards apply to all:

- a. Computer systems owned, leased or maintained by the University. This includes: mainframe, mini and microcomputers/PCs; servers; networks (regardless of type - LAN, WAN, wireless, etc.); routers; bridges; hubs; and various peripheral equipment including but not limited to printers and modems.
- b. Authorized Users - all students; employees including student, non-student, faculty, professional, classified, temporary, part-time, and full-time; and contracted consultants of the University of Massachusetts who are required to have access to data, University computer systems/networks or software applications (e.g., email, Internet, registration, etc.) to perform their job function, academic assignment, or contractual obligations.
- c. University data regardless of the medium on which it resides (e.g., tape, cartridge, disk, hard drive, etc.), and regardless of its form (e.g. text, graphic, video, voice, etc.).
- d. Electronic mail (e-mail) created within, sent to, maintained within, or administered by the electronic mail systems of the University of Massachusetts.

### **GENERAL**

Since many users share information data and technology, and because of legal and ethical requirements, all students and staff need to be aware of their responsibilities related to data and computing at the University of Massachusetts. Remember that observing these standards will help to make computing and use of the network services more pleasant for all. Please use the University data and computing [FAQ](#) to clarify policy, standard/procedure, and use questions.

Access may be given to: manual data processing systems, stand-alone micro, mini or mainframe computers; or to networked computer systems. Student access is primarily for work associated with their course of study, activities related to courses, or administrative tasks related to their association with the University (e.g., accessing their own academic/administrative data such as courses, grades). Staff are given access to perform their job functions. Students and staff may however, use their access to University computers to use worldwide networks such as the Internet. Information resulting from communication on University computer systems is University property. Authorized users are presumed to be responsible for any activity carried out under their University Logon Ids/Operator Ids/Accounts. Employees who access University or Campus networks for private purposes should subscribe to a commercial service provider.

Every employee and student at the University is responsible for implementing security in their daily interactions with people, data, systems, and facilities. As they perform their normal functions they should be alert and conscious of the security environment around them and notify the appropriate security/system administrators when they notice a security vulnerability, system/software malfunction, possible security incident (e.g., virus, system compromise/hacking), or if they have suggestions for improvement.

University employees, students and all users accessing University data or computing systems/resources **shall** exercise responsible, ethical behavior when using University data and computing systems/resources including, but not limited to:

- Adhering to all laws governing data security and use including Copyright Laws, Electronic Communications Privacy Act (ECPA), Digital Millennium Copyright Act (DMCA), Health Insurance portability and Accountability Act of 1996 (HIPAA), Computer Fraud and Abuse Act (CFAA), TEACH Act, etc.
- Complying with University acceptable use and other policies/standards and procedures when accessing any University data, computer systems/resources, networks. By accessing any University data or by using any University computing system/resource, University employees, students and users agree to comply with this and all University data and computing related policies/standards/procedures (e.g., [Data and Computing Standards](#), [Data/System Administrator Responsibilities and System Requirements](#), etc.) Full text of University data and computing policies/standards/procedures are located at [Data and Computing Policies, Standards and Procedures](#) web site.
- Complying with University acceptable use and other policies/standards and procedures when accessing any other networks or sites from University computing systems/resources. The University and/or Campus networks may enable authorized users to connect to computers at other educational and research institutions, and connect to many computers in organizations not related to the educational sector. The fact that you can connect to a computer system does NOT automatically give you authority to use that computer system. The mere lack of security on a network does not mean that a computer system is open and available for use by unauthorized users. Abuse of the networks or of computers at other sites connected to the University's computers or networks by authorized users are treated as abuse of computing resources at the University. Additionally, any network traffic exiting the University system is subject to the acceptable use policy/standards/procedures of the network through which it flows. Note that the laws of other states may apply depending on the actual location of the computer to which the authorized user is networked (e.g., If you have connected to a computer in California, California computing laws must be adhered to. You can be prosecuted in any state through which your access flows or in which it terminates.).

- Only accessing University data and/or computer systems/resources for which they have been authorized. Access to data is given to authorized users. This access should not be shared, transferred or delegated (e.g., authorized users should not access data and then let others use that data). Access to data classified as Confidential is based on legal requirements or on a need to know; job function; or course requirement basis. Many computers in the University are connected to the University and/or Campus networks. Individuals must have an authorized logon id/operator id/account to access any University computer system including networks.
- Using their access to University data and computing systems/resources for approved purposes only. Approved purposes include work related to student studies or instruction, the performance of duties by an employee, or other University sanctioned activities. Access to data, assignment of Logon Ids/Operator Ids/Accounts and deployed network connections are made available to benefit the entire University and support its missions of education, research and public service including instruction, research, administrative tasks and collaborative activities with other entities, including but not limited to colleges/universities and private businesses. The University does allow for employees' personal pages that provide information about an individual that is relevant to that individual's role at the University.
- Safeguarding the integrity, accuracy and confidentiality of University data by taking reasonable efforts to protect University data and computer systems/resources from theft; destruction; unauthorized creation, alteration or exposure (e.g., unauthorized updating, processing, outputting, or distribution); or any form of compromise resulting from inappropriate intentional, negligent acts, or omissions. This includes implementing appropriate physical security and data classification procedures, and periodically "refreshing" downloaded data to ensure you are working with accurate, up-to-date data.
- Properly creating, accessing, using and disposing of University data based on the data's classification (See [University Data and Computing Standards](#) and [University Records Management, Retention and Disposition Standards](#)). Users shall access University data for approved purposes only, and shall understand the data they are accessing and the level of protection required. Databases containing Operational Use Only or Confidential data should be secured. Extracts of Operational or Confidential data should be secured at the same level as the file/database from which the data was extracted. Aggregates of data should be classified as to the most secure classification level (e.g. when data of mixed classification exist in the same database, file, report, etc., the classification of that database, file, or report should be that of the highest level of classification). Reports containing Operational Use Only or Confidential data should be disposed of properly. Paper and microfiche/film should be shredded. Disks/ hard drives should be erased so as to be irretrievable.
- Implementing appropriate levels of security on all manual and computer systems/resources on which Confidential (As defined in the [University Data and Computing Standards](#)) or critical data is stored, maintained, or in the case of electronic systems, transmitted.
- Appropriately backing up data (e.g., business, personal/instructional, etc.), and computer system and applications software to allow for recovery if there is a disruption. Multiple generations of operating system, application and data backups should be maintained in both on-site and off-site storage facilities.

- Ensuring that antivirus software is installed and continuously enabled on any computer system they use which accesses University data or computing systems/resources. This will ensure the spread of viruses within the University networks and computer systems is prevented.
- Obtaining authorization for the processing of University data or conducting University business on home computer systems from the appropriate Data Custodian. Additionally, the latest version of anti-virus software shall be installed and running on any home computer system used to process University data or to conduct University business.
- Scanning software downloaded from an email, network or installed from a disk/CD-ROM for possible virus infection before you use it.
- Properly using shareware and public domain software. The University encourages the use of shareware and public domain software, however, the use of such software should be predicated on the fact that it has been scanned for computer viruses.
- Using all non-software proprietary information (e.g., text, images, icons, programs, etc.) retrieved from computer or network resources in conformance with laws.
- Addressing issues of incompatibility to hardware or previous versions, etc. of all supported software running on the affected computer system when performing hardware or software upgrades.
- Using standard systems development life cycles and include system testing and documentation when developing on a microcomputer/PC, critical or impacting applications (As defined in the [University of Massachusetts Business Continuity and Planning Guidelines](#)) or applications used to process administrative data.
- Only performing remote/distributed access to administrative or research computer systems via a virtual private network (i.e., VPN) or other equally secure method (i.e., via HTTPS, etc.).
- Contacting the appropriate system, network and/or security administrators(s) prior to performing any academic game development, computer security research, or the investigation of self-replicating code as part of an academic or instructional activity. This will allow the administrator to determine and evaluate possible effects on the system being used for these activities.
- Following the same standards of intellectual honesty and plagiarism in regards 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.
- Notifying the appropriate system, network and/or security administrator(s) of any suspected or actual security violations/incidents.
- Being aware that the University disclaims any loss or damage to software or data that results from its efforts to enforce this and other data and computing Standards/Procedures.

File Sharing provides a convenient way to transfer information, and facilitate collaboration on projects. It can also make it convenient for a hacker or virus to invade a computer. Many of the latest viruses take advantage of shared directories that aren't adequately protected. Today's hackers can take advantage of these same vulnerabilities to place Trojans in a computer to use in gathering information and attacking other machines. The University allows file sharing, but recommends that this tool be used only when other, safer solutions, such as Secure FTP are inadequate, and that the shared folders be protected by secure passwords which are only shared with trusted friends and associates.

University students and employees shall:

- Attend a data security orientation,
- Sign a computing the [University Computing Awareness and Data Security Compliance Statement](#) and
- Reaffirm annually that they know and understand University policies/standards/procedures and Campus procedures regarding data and computer use.

### **ELECTRONIC COMMUNICATIONS**

The University works in a large, complex information technology environment requiring communication related to both confidential and public data. New technologies offer the University methods to make this communication easier between students, staff, departments, campuses, colleges, and the world. The University has several types of electronic communications systems on its various computer systems enabling its students and employees to take advantage of these technologies. However, with this open communication network, vulnerabilities to the privacy of electronic messages possibly containing confidential or proprietary material arise. University electronic communication users need to be aware of the vulnerabilities in electronic mail communication and of the legal responsibilities that accompany the use of this medium.

University policies/standards/procedures and Campus procedures related to communication shall also apply to web-based communication and conversation (e.g., "chat", instant messaging, on-line conferencing, class discussions, etc.).

The University makes e-mail facilities available to both students and staff. University E-Mail Users are encouraged to use these communications resources to share knowledge and information in furtherance of the University's missions of instruction, research, and public service. Students are free to use e-mail for personal use. E-mail 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 employees' job function.

The University considers a personal e-mail message to be private correspondence within the limits set forth in this and other applicable standards/procedures and policies, 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.

Due to information technology, the privacy, security and authorship/source of documents and messages stored in and transmitted via electronic media cannot be guaranteed. Users of electronic communications are cautioned that such messages might become available to others. Emails can be stored, copied, printed or forwarded by recipients. As such, email users should not write anything in an email that they would not feel just as comfortable putting in a memo.

The University can not control the content of electronic mail. If an individual receives electronic mail that they consider harassing, threatening or offensive, they should contact the appropriate University Office for assistance.

University E-mail Users **shall** use e-mail in a responsible manner consistent with other business communications (e.g., phone, correspondence) including, but not limited to:

- Safeguarding the integrity and confidentiality of University electronic mail.
- Only using mail IDs assigned to them.
- Removing mail from their mailbox consistent with University, campus, departmental or electronic mail administrator message retention procedures and these Standards.

## **SECURITY**

Be particularly careful of your password. Do not give/share your password to/with anyone or type your password when someone is watching. This includes logging on for another person and allowing them to access computer systems under your logon/operator id. 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. Do not hard-code passwords or pin numbers used to protect access to University data in software or scripts. Once someone has your password it is possible both to look in your directory and to use your username for malicious purposes.

Follow password security standards including, but not limited to periodically changing your computer system passwords, selecting a password that is difficult to guess and when possible, includes letters, digits and special characters (e.g., #, %, \$). Logon/Operator Ids, names, birth date, employee or social security number, repeating characters (e.g., 111111 or ababab), common character sequences (e.g. "123456" or "abcdef"), or common words that can be found in a dictionary are prohibited. You should also avoid using any personally related information (e.g., pet's, child's or spouse's/partner's name; favorite sports team or car; etc.).

Log off computer systems/resources if you leave your pc unattended or will not be accessing data for an extended 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. Additionally, any person attaching a wireless client to any University network (wired or wireless) is responsible for the security of the device and for any intentional or unintentional activities from or to the network pathway that the device is using.

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. Programs and files are considered confidential unless they have explicitly been made available to authorized users.

Possible loopholes in computer or network system security shall not be used to damage computer systems, obtain extra resources, take resources from another user, or gain access to any University computer system or any computer system networked to the University.

The University recommends the installation of personal firewalls on all University owned systems and any computer accessing University computer and network systems. The University offers inexpensive personal firewall software to all employees and students for work and personal use.

## **PRIVACY**

University computer systems/resources 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.

The University does not routinely monitor the content of computer systems/resources including files, programs and electronic communications/emails. The University has the responsibility and authority to access, review and release University data, electronic information that is transmitted over or stored in University systems or facilities, and to monitor individual accounts to the extent the University determines to be reasonably necessary for legitimate administrative purposes, including but not limited to a determination by appropriate University officials that there is a reasonable basis to believe that such action:

1. Is necessary to comply with legal requirements or process, including but not limited to subpoenas, writs or warrants;
2. May yield information of use in the investigation of a suspected violation of law or of University policies, procedures and codes of conduct; or when a system security or system operation has been compromised or used for unauthorized activities;
3. Is needed to maintain or protect the integrity or operations of University computing systems;
4. May yield information needed to deal with an emergency; or
5. In the case of University employees and officials, may yield information that is needed for the ordinary business of the University.

Additionally, the University has the responsibility and authority to scan computers attached to the University's wired and wireless networks to ensure appropriate security, and support network operations and performance.

The University does not routinely examine files of authorized user accounts however, to protect the integrity of the computer systems and to protect legitimate users from the effects of unauthorized or improper use of the University's computing facilities, system, network or security administrators may inspect, copy, remove or otherwise alter any data, file or resource that may undermine the proper use of the computer system. Such action will be based on reasonable suspicion, authorized by the system, network or security administrator's supervisor and may be taken with or without notice to the user. Additionally, computer center personnel may access others' files when necessary for the maintenance of the computer system. When performing maintenance, every effort is made to insure the privacy and confidentiality of authorized user files.

The University will take reasonable steps to protect the rights to privacy granted by the Federal Family Educational Rights and Privacy Act of 1974, as amended, 20 U.S...C. Sec. 1232g, the Electronic Communications Privacy Act of 1986, Pub. L. 99-508, the Massachusetts Fair Information Practices Act, M.G.O. c. 66A, and other applicable laws. The content of some electronic communications may be deemed public records under the Massachusetts Public Records Act, M.G.L. c. 66.

Remember that any printouts in public places are likely to be seen by others.

**WORKSTATIONS AND MICROCOMPUTER/PERSONAL COMPUTERS (PC)**

Although micro-computing offers improved productivity and cost-effectiveness, it requires the implementation of additional controls in those areas in which Confidential (As defined in the [University Data and Computing Standards](#)) or critical University data or hardware/software may be at risk. University employees, students and computer system/resources users shall exercise appropriate pc security including, but not limited to:

- Microcomputer/PC keys shall not be left in the computer when unattended. These keys shall be properly secured.
- All workstations and microcomputer/PC systems shall be outfitted with uninterruptible power supply (UPS) systems, electrical power filters, or surge suppressers, as appropriate.
- If environmental conditions pose a significant risk of static electricity discharge, all potentially effected workstations and microcomputers/PCs shall be outfitted with static protection equipment. This ensures that the discharge of static electricity does not damage computer equipment or data.
- Appropriate hardware and software security (e.g., cable lockdowns; password access control; data compression and encryption; audit log of access, updates; etc.) shall be placed on all microcomputers/PCs and transportable computers that have Confidential data (As defined in the [University Data and Computing Standards](#)) stored in them (i.e., on the local drive).
- There shall be a copy of all un-networked microcomputer/PC software prior to its initial usage, to the extent consistent with applicable licenses and laws. These copies (i.e., master copies) shall be stored in a safe and secure location separate from that of the microcomputer/PC (preferably off-site). These master copies shall not be used for ordinary business, but must be reserved for recovery from computer virus infections, hard disk crashes, and other computer problems.
- Whenever a hard disk is sent for repair, the vendor shall be required to comply with [University Data and Computing Standards](#) regarding the handling of data.
- When disposing (e.g., recycling, salvaging, transferring ownership to another party, etc.) of microcomputer/PC hard disks, the hard disks should, at a minimum, be low level formatted so as to erase all data on the hard drive.
- Staff and students loaned or using University owned/funded transportable computers shall make every reasonable effort to secure and safeguard the physical integrity of the computer and to comply with all [University Data and Computing Standards](#).
- Security tokens shall not be stored with the microcomputers/PC's (including transportable computers).
- Passwords, University assigned pin numbers (excluding telephone pin numbers) or logon /operator ids shall not be programmed in any computer accessing University networks or Confidential data (As defined in the [University Data and Computing Standards](#)). This includes transportable computers. Additionally, microcomputers/PCs shall not be configured to allow a third party to access any University network or data without being prompted and required to enter a password.

- All Confidential data (As defined in the [University Data and Computing Standards](#)) stored on workstations or microcomputers/PCs and not backed up centrally on a network, shall be backed-up on separate storage media after changes to the data have occurred. As noted previously, backups should be stored in an off-site location when possible.
- Confidential data (As defined in the [University Data and Computing Standards](#) which has been backed-up shall not be used for data restoration purposes unless another back-up copy of the same data exists. This will prevent the only current copy of Confidential data from being inadvertently damaged in the restoration process.
- Proper disk maintenance practices shall be followed (e.g., clearly label diskettes; back up data, application and operating system diskettes; store away from extreme cold/heat; protect from dust, excessive moisture or water; keep away from magnetic devices including radios, telephones, keys, wall magnets; etc.)

All devices connected to the University and/or Campus networks must conform to these Standards, Campus procedures, and specific network requirements. Devices which do not comply, or which disrupt other network clients may be disconnected at the discretion of the appropriate system, network or security administrator.

#### **DATA, COMPUTER SYSTEM/RESOURCE ABUSES**

You can expect to lose your computer account; be disconnected from the network; be denied or given limited (i.e., to allow for the performance of required academic or employment related tasks) access to University data, applications and/or computer systems; and/or be subject to reprimand, suspension, dismissal/termination, or other disciplinary action. Additionally, these individuals may be charged with criminal offenses or have civil action taken for computer abuses. Conduct which may constitute misuse or abuse includes, but is not limited to:

- Providing false or misleading information to obtain access to University computing facilities or resources.
- Unauthorized access to University data, computer systems/resources, or another's computer or email account. This includes using computing systems/resources to access any other computer system (on or off-campus) without authorization. If it is necessary to read another individual's mail (e.g., while they are on vacation, on leave, etc.), surrogacy or message forwarding should be utilized.
- Accessing or copying files, regardless of media (e.g., paper, diskette, etc.), of another user without prior consent from the file owner. Accessing the "private" files of others without permission, even if those files are unprotected, is prohibited. Altering another user's files or systems files without permission is vandalism and destruction of University property.
- Attempting to compromise or tamper with user passwords. This includes, but is not limited to cracking, decoding, copying password files, "sniffing" packets to search for passwords or otherwise attempting to discover passwords belonging to other individuals. This also includes taking advantage of another user's naiveté to gain access to computer systems/resources or data, or preventing someone from using their account by changing the password or by other tampering.
- Attempting to intercept any network communication for purposes including, but not limited to: reading message/file content; rerouting packets; or packet "sniffing".

- Connecting dial-up modems to workstations or microcomputers/PCs that are simultaneously connected to a network.
- Remotely logging into (or otherwise using) any microcomputer/PC not designated explicitly for public logons over the University and/or Campus networks, even if the configuration of the computer permits remote access, unless you have been given explicit permission from appropriate authorized personnel.
- 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 or email account.
- Posting, sending or publicly displaying or printing unsolicited mail or materials that violate existing laws or University policies/codes of conduct. Such material includes, but is not limited to those that are of a fraudulent, obscene, offensive, defamatory, harassing, abusive, or threatening nature. Additionally, the University has special concern for incidents in which individuals are subject to harassment or threat because of membership in a particular racial, religious, gender or sexual orientation group.
- Repeated sending of unsolicited mail.
- "Rebroadcasting" information obtained from another individual that the individual reasonably expects to be confidential.
- Abusing the networks to which the University belongs.
- Using University computer systems/resources, networks or web sites for monetary gain, political purposes or illegal activities. This includes using University Internet resources to create web pages for personal business or financial gain, except as permitted by other University policies, or to endorse or otherwise support a specific political campaign, candidate, party or referendum.
- Illegally using of copyrighted materials including print, audio, and video.
- Illegally soliciting or distributing copyrighted software within or outside the University through any mechanism (e.g., email, bulletin boards, disk, etc.), electronic or otherwise. Employees and students shall not copy copyrighted software unless explicitly allowed in the software license agreement, except for one backup copy to be made and maintained by the original licensee. The University and its departments license many copies of software. The University does not own this software. Employees and students are required to comply with software licenses and the U.S. Copyright Act.
- Using personally owned software on University computer systems/resources unless the software is properly licensed for such use and system administrator approval has been obtained.
- Adding, copying or removing software to/from University computer systems/resources in violation of the software license. This includes copying software from or to University computer systems/resources.

- 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.
- Modifying the configuration of the University or Campus computing infrastructure by adding or removing network links, computers, or peripherals (e.g., external disks, printers, modems, video systems, etc.); reconfiguring any control switches or parameters; upgrading processors, expanding memory, installing extra circuit boards, etc., except as authorized by the appropriate system or network administrator. The University is the sole provider of network "services" such as DNS and DHCP on University networks. Any computer or equipment that replicates or disrupts these services will be immediately disconnected.
- Unnecessarily or inappropriately using limited computer systems/resources including but not limited to such inappropriate uses as sending chain emails, spamming, mail bombing, generating unnecessary excessive print, etc. Chain letters have been illegal if sent through the United States Postal Service (USPS) for many years.
- Attempting to develop or use any mechanism to alter or avoid charges levied by the University for computing resources.
- Performing or assisting in the performance of any act that will interfere with the normal operation of computer, terminals, peripherals, networks, etc. or in any activity that interferes with the rights of others (e.g., Using public, lab or departmental equipment for personal entertainment when other authorized users need access to perform University related tasks; intentionally damaging or misusing any University computer system/resource including terminals, microcomputers/PCs, networks, printers or other associated equipment; etc.)
- Any use which in the University's determination is contrary to its mission, goals, and values, or which is detrimental to the University's good name and reputation, and/or which adversely impacts the University and/or the University community

In the event that a University network experiences significant degradation due to excessive utilization of resources or a network based attack from internal/external computers or networks, the University reserves the right to take any measure necessary to insure stability and performance. These measures may include rate-limiting, filtering, or disconnection of any computer, network, or building that is involved. Whenever possible, prior notice will be given; however in emergency, after-hours, or widespread network disruptions this may not always be possible.

When the University receives a notice of infringement from a copyright holder or designated agent in compliance with the Digital Millennium Copyright Act (i.e., DMCA), the University will take any measures necessary to remove the ability to access the infringing material via the network without prior notice.

Reports of abuse to your account can be made by contacting your system administrator. Please also note that your campus may have additional acceptable use requirements. Contact your system administrator for more information.