Mount Wachusett Community College

Information Technology Acceptable Use Policies
and
Helpdesk Prioritization Practices

January 25, 2011

Contents

Information Technology General Acceptable Use Policy

Introduction

Mount Wachusett Community College provides information technology resources for students, faculty and staff.
This document:

- Provides guidelines for responsible use of Mount Wachusett Community College's technology resources by all members of the College Community.
- Provides policies that Mount Wachusett Community College uses in providing technology resources and network services to the College Community.
- Explains enforcement procedures of these policies.
- Applies to all those using College computing equipment[1] whether the individual is on or off campus.

This document provides high-level explanations of College policies regarding the use of information technology. For more detailed explanations refer to the appendices.

Guidelines for Responsible Use of College Technology Resources

Mount Wachusett Community College recognizes that free expression of ideas is central to the academic environment. For this environment to flourish, all users must adhere to the guidelines established in this Information Technology Acceptable Use Policy ("AUP").

Mount Wachusett Community College provides computing equipment and services. The primary purposes of this computing equipment are the ***academic, research, administrative and College business-related communication*** needs of its students, faculty and staff. All use of College computing equipment shall be consistent with the terms and conditions of the AUP and shall not violate or conflict with (a) any federal, state or local law; or (b) the College mission or policies. Access to all Mount Wachusett Community College owned and/or operated computing and electronic communications systems and equipment is a ***privilege and not a right***. Individuals who refuse to accept and follow the AUP will not be granted user accounts. All users of the College's computer equipment, including email, shall have NO EXPECTATION OF PRIVACY over such use.

[1] "Computing Equipment" shall mean all computers, software, wiring, network components and network services, including voice, data, and video facilities, owned, operated, or provided by The College.

Violations of the AUP by individuals with accounts may result in penalties including but not limited to closure of all accounts and revocation of all computing privileges. Other penalties may be levied up to and including dismissal from the College or termination of employment.

User responsibilities include, but are not limited to:

- Maintaining privacy and security by keeping all passwords confidential.
- Honoring all computing security procedures implemented by the College.
- Being reasonable and prudent in the consumption of College computing and network resources.
- Deleting old and unused e-mail and file(s) on a regular basis.
- Maintaining the accuracy of private mail groups by updating when members change.
- Developing adequate proficiency in the tools and technologies appropriate to his/her needs.

College Network Usage Guidelines include, but are not limited to:

- No one may misuse, abuse or otherwise damage College computer or network equipment.
- No one may install or use any software or hardware designed to disrupt the security of any computing equipment, whether owned by the College or by others.
- No one other than Media Services or Information Technology staff may download or install any software on any student-accessible College computer.
- No one may use College resources to support political or non-College related business interests.
- No one may sell or provide access to Mount Wachusett Community College's computing resources to individuals, groups or businesses outside the College Community except (1) as authorized in writing by an appropriate senior officer of the College and (2) for authorized College business relationships.
- Recreational uses – such as game playing or music or video file sharing – constitute an unacceptable use of College computing equipment except if such activities are part of an instructional plan.
- No one may engage in any activities designed to spy on network traffic or to access passwords, user IDs, files or programs of other users.
- No one may engage in software piracy or copyright infringement. All software installed on College computers must be used in conformance with the license granted by the developer. Unlicensed products will be removed from College computers.

- No one may send, store, print or solicit receipt of e-mail messages, files or programs that contain fraudulent, harassing, racist or obscene language, visual, or audio content. Exceptions may be made for legitimate academic research purposes with prior approval.
- Note that any e-mail message (other than official College business) sent to an individual after that individual has indicated through any method that they no longer want to receive e-mail from the sender constitutes harassment. Complaints are handled via the *Enforcement Procedures* section (see below).
- No one may use e-mail to engage in "chain letter" or "spamming" [bulk "junk" e-mail activity].
- No one may send, store, print or solicit receipt of e-mail messages, files or programs that are inconsistent with the terms and conditions of the AUP, in conflict with the Mission Statement of Mount Wachusett Community College, or that violate federal and/or state laws.
- No one may use College computing resources for illegal behavior or illegal activities as defined by federal, state and/or local laws.

College Technology Resources and Network Services Policies

Disclaimer: The responsibility for the content of personal files, programs, web pages and e-mail rests solely with the individual and not with the College. Mount Wachusett Community College does not monitor the contents of embedded links of personal user accounts or personal web pages although it expressly reserves the right to do so.

To preserve the integrity and maintain efficient functioning of the College's computing facilities, the College enforces the following policies:

- The creation of public mail groups is limited to College departments, committees and official student organizations.
- Email users should exercise prudent judgment when sending "All MWCC" emails. Use of this list for any commercial purpose not directly connected to College sponsored events requires approval of the President or his designee prior to sending the email.
- Computing resources are provided for academic, research, administrative and College business-related communications uses.
- The College reserves the right to establish time limits on the use of public workstations as needed.
- Mount Wachusett Community College realizes that the free expression of ideas is central to academia, but will not tolerate the display of pornographic, obscene, abusive, racist, or other inappropriate material at any public workstation. The College reserves the right to determine the appropriateness of material displayed on public workstations.
- The Mount Wachusett Community College computing facilities constitute a private system. As such, the information stored on the

College equipment is the property of the College and the Commonwealth of Massachusetts with the possible exception of material expressly developed by faculty, staff, and students for publication. Copyright and ownership of such content must be expressly and clearly stated in such works. Individuals who place content owned by others on computers under their control accept full responsibility for maintaining compliance with copyright laws.

- Users of the College's computing equipment, including email, shall have NO EXPECTATION OF PRIVACY over such use. The College reserves the right to access the personal files or monitor the system usage of any authorized user without that individual's consent, under the following circumstances:
    - A subpoena, or other properly served request from enforcement officers. All such requests must be served by an officer of the court that has jurisdiction and be reviewed and approved in writing by a senior officer of the College. Review by College counsel may be appropriate.
    - A written request from an appropriate senior officer of the college to provide information as part of an ongoing investigation and or disciplinary matter.
    - A written request from a Systems Administrator, based on reasonable evidence that files or programs stored in an authorized user's directory are the source of interference with the efficient functioning of the College computing facilities, that such files are violations of any part of this policy, or are infringing on copyright or intellectual property rights. The Executive Director of Information Technology must endorse such a request.
    - A written request from the President of the College.
    - A written request from College Counsel in support of an ongoing investigation or inquiry.
    - A written request from the appropriate College officer as a part of a termination of employment action.

Information Technology will maintain records of all of these requests for access and will report the number of requests annually to the College administration.

- Electronic files are treated like paper files and subject to subpoena or discovery in legal actions and disclosure if such files constitute public records under Massachusetts law.
- Employee accounts are disabled as soon as the IT Department is notified of termination of employment. Human Resources should notify the Executive Director immediately when such personnel actions are imminent.

- Passwords to terminated employees accounts will not be provided to other individuals. File access can be provided through system delegation facilities.

Enforcement Procedures

The College retains right without restriction to monitor, authorize, control, or stop the use of any technology found on its computers or networks.

Violations of the Acceptable Use Policy will be referred to the appropriate senior officer of the college for action through the established disciplinary processes of the College. The results of such referral may include but is not limited to:

- Files and/or programs may be deleted.
- User access privileges may be inactivated.
- User accounts may be removed
- Users may be suspended, expelled or terminated from College employment.

If a member of the College Community believes that another has violated his or her rights, he/she should report the incident to the Executive Vice President and his/her department head.

MWCC Administrative Computing Use Policy

The Family Educational Rights and Privacy Act of 1974 (FERPA), plus its amendments, set forth rights and responsibilities regarding the privacy of student record information. FERPA governs release of student records maintained by the College and access to these records. For detailed information about FERPA contact the Office of the Registrar or visit the American Association of Collegiate Registrars and Admissions Officers (AACRAO).

All employees of the Mount Wachusett Community College are required to abide by the regulations of FERPA and those of the College regarding access to and use of student information, College financial information and College alumni development information. **Student access to Banner for data entry purposes is expressly prohibited.**

Department heads, Division heads, Directors and other supervisory personnel are responsible for ensuring that their respective employees follow the FERPA and College guidelines.

The College houses its administrative data on its servers. The software package includes Admissions, Registration Records, Grading, Financial Aid Management, Billing, Accounts Payable, General Ledger and Alumni Development Records. Employees who have access to administrative system data must understand and accept the responsibility of working with confidential data. In addition to FERPA, College rules apply to all employees with an administrative system account.

1. Each employee is given a username and password. This account is for the employee's use only and should not be shared with supervisors, co-workers, family, or friends. In no case is the sharing of access accounts or passwords authorized.

2. Each employee will be held responsible for any data input into or retrieval from the administrative system via his/her account. Employees are fully responsible for any system actions initiated under the employee's user id and password.

3. An administrative computing account is for use for work-related activities only. Access at other times is prohibited.

4. Information that does not relate to the work assigned by your supervisor should not be viewed (e.g. looking up friends or co-workers) or altered (e.g. changing a friend's address) in any way.

5. Since administrative data is confidential, no employee will discuss or share any data with any other person except as is needed to carry out his/her job responsibilities.

6. All access to electronic data and reports shall be secured. Sign off the system, put reports away in drawers and/or cabinets when leaving your work areas, especially for long periods of time. Ensure that your computer uses a password protected screen saver to minimize unauthorized disclosure of confidential information.

Mount Wachusett Electronic Communications Acceptable Use Policy

Introduction

Mount Wachusett Community College works in a large, complex information technology environment requiring communications involving both confidential and public data. New technologies offer the College methods to make this communication easier between students, staff, departments, campuses, other colleges, and others. The College has several types of electronic mail systems on its various computer systems, enabling its students and employees to take advantage of these technologies. In addition several types of electronic communications services, including chat, discussion lists, voice mail, and instant messaging services are used by the College Community.

However, with this open communication network, vulnerabilities to the privacy of electronic messages possibly containing confidential or proprietary information arise. College electronic communications users need to be aware of the vulnerabilities in electronic communications and of the legal responsibilities that accompany the use of this medium.

Purpose

These standards:

- Define who may use the electronic communications systems controlled and administered by the Mount Wachusett Community College,
- Outline responsibilities related to maintenance and use of such systems.
- Provide guidelines for the security and confidentiality of College electronic mail, and other forms of electronic communications.
- Provide methods for monitoring, enforcing and dealing with exceptions to this policy.

Scope

College Electronic Communications Polices shall apply to all:

- Electronic mail (email) created, sent or maintained within, administered by or networked to the electronic mail systems of the Mount Wachusett Community College.
- College email users.
- All other forms of electronic communications, including voice systems and instant messaging services, and other forms of electronic communications

listed in the introduction and to any new forms of electronic communications that may be introduced.

Responsibilities

The President, together with the senior officers of the College, determines what categories of individuals (e.g., full time, part-time, staff, students, economic partners, other educational institutions, general public, etc.) may access College electronic communications systems.

These individuals will determine which College department(s) shall be responsible for administering electronic communications systems and security, and procedures for monitoring.

Campus Electronic Communications Policies will ensure that Electronic Communications Administrators are responsible for:

- Determining what categories of individuals, within the guidelines set by the President and campus administrators, may access the communications system under their control.
- Ensuring that a security plan for the email system for which they are responsible, has been developed, implemented and is maintained. The security plan should include an analysis of whether message encryption is needed.
- Ensuring that a backup plan to allow for message/system recovery in the event of a disaster has been developed, tested and implemented.
- Periodically assessing the level of risk within the mail system.
- Ensuring that filters to keep text from view of system maintenance personnel have been installed, when technologically possible.
- Ensuring that appropriate steps are taken to prevent a system break-in or intrusion through the electronic communications application.
- Providing information regarding electronic mail vulnerabilities to email users so that they may make informed decisions regarding how to use the system.
- Ensuring that all electronic mail ids for individuals with email accounts on College systems have been deleted when: an authorized user has terminated employment, graduated or withdrawn from the College, and when a "courtesy accounts" is inactive or no longer needed.
- Ensuring that email message retention standards, within the guidelines of these and other College policies, have been developed and are implemented for their electronic mail system.
- Campus Electronic Mail Policies will ensure that employees responsible for maintaining, repairing and developing email resources will exercise special care and access email messages only as required to

perform their job function. These employees will not discuss or divulge the contents of individual email messages viewed during maintenance and trouble-shooting.

Campus Electronic Mail Policies will ensure that College Email Users will:

- Use email in a responsible manner consistent with other business communications (e.g., phone, correspondence).
- Safeguard the integrity, accuracy and confidentiality of College electronic mail.
- Only use mail ids assigned to them.
- Remove mail from their mailbox consistent with College, campus, departmental or electronic mail administrator message retention policies and standards.

Campus Electronic Mail Policies prohibit College email users from :

- Sending any unsolicited mail or materials that are of a fraudulent, defamatory, harassing, or threatening nature.
- Posting materials that violate existing laws or College codes of conduct, are inconsistent with the College mission, or are commercial advertisements or announcements on any electronic bulletin boards.
- Forwarding any other form of unnecessary mass mailing (such as chain letters) to College or external email users.
- Using their email access to unlawfully solicit or exchange copies of copyrighted materials in any form.

Electronic Communications Security And Confidentiality Standards

Campus Electronic Communications Policies will ensure that those who access and use these systems are aware and understand that:

- The College considers electronic communications message to be a personal or business correspondence that should therefore, be dealt with in the same manner as paper correspondence items.
- Although electronic communications may be considered the property of the sender and/or receiver, these messages are stored on College computer systems. Therefore, administration of electronic communications systems may require that administrative staff read or access in other ways message contents. Users shall have NO EXPECTATION OF PRIVACY over the content of electronic communications maintained on the College's computer system.
- The College will not routinely monitor the content of electronic documents or messages. Electronic documents and messages may be accessed by

technical maintenance, security and troubleshooting staff while performing their duties. Such access may occur when a problem in the software or network arises. Additionally electronic mail may pass out of one computer environment, across a network, and into another computer environment even within the College system. This transport becomes increasingly complicated as mail travels between departments, campuses, universities, states, or nations. The level of security over your messages is affected each time the computer hardware, software and environment changes. Untraceable leaks may occur.

- If there is a College investigation for alleged misconduct, the President or his designee may authorize that electronic communications or files may be locked or copied to prevent destruction and loss of information. Additionally, the College may monitor the content of electronic documents and messages, or access email backups or archives as a result of a College investigation, legal discovery, writ, warrant, subpoena, or when there is a threat to the computer systems integrity or security.
- The confidentiality of the contents of email messages that include certain types of information (e.g., student related, medical, personal) may be protected by the Family Educational Rights and Privacy Act of 1974 (as amended) and/or the Electronic Communications Privacy Act of 1986. Additionally the contents of email messages may be classified as public by the Massachusetts Fair Information Practices Act (MGL Title X, c66A, refer to http://www.state.ma.us/legis/laws/mgl/gl-66A-toc.htm) and/or the Massachusetts Public Records Act (MGL Title X, c66, refer to http://www.state.ma.us/legis/laws/mgl/gl-66-toc.htm). Further recent federal legislation, referred to as the Patriot Act, may require the College to disclose to law enforcement officers information previously considered to be privileged without notification.
- The authenticity of an email message cannot be assured due to the state of present email technology. This means that the authorship or source of an email message may not be as indicated in the message. Methods exist to provide to authentication of email messages. Email clients who require this level of security are to contact the Help Desk for assistance in obtaining a digital certificate.
- College Email Users may retain active mail files for the retention period instituted by the Electronic Mail Administrator. Deleted and expired email messages will be unretrievable after 90 days.

Electronic Mail Use Standards

The following policies govern the use of College email equipment/systems :

- Individuals are prohibited from using an electronic mail account assigned to another individual either to send or receive messages. If it is necessary to read another individual's mail (e.g., while they are on vacation, on leave, etc.),

delegation or message forwarding should be requested from the email administrator.

- College Email Users are encouraged to use these communications resources to share knowledge and information in support of the College's mission. Occasional and incidental social communications using electronic mail are not prohibited; however such messages should be limited and not interfere with an employee's job function.
- Individuals with email ids on College computer systems are prohibited from sending messages which: violate existing laws or College codes of conduct or policies; are inconsistent with the College mission; or are advertisements or announcements for a commercial business without prior approval of the President or his/her designee.
- Authorized users should not "rebroadcast" information obtained from another individual that the individual reasonably expected to be confidential.
- Bulletin Boards used for soliciting or exchanging copies of copyrighted software are not permitted on College systems.
- Authorized users are prohibited from sending, posting, or publicly displaying or printing unsolicited mail or material that is of a fraudulent, defamatory, harassing, abusive, obscene or threatening nature on any College system. The sending of such messages/materials will be handled according to current College codes of conduct, policies and procedures.
- The College accepts no responsibility for the content of electronic mail received. If a student, faculty, or staff member receives electronic mail that is considered harassing, threatening or offensive, he/she should contact the appropriate College Office for assistance.
- Federal and state laws, and College policies against racism, sexism and sexual harassment apply to electronic communications. Additionally, the College 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.

Social Media Use Standards

In an effort to foster a professional work environment for all employees and to protect the interests of Mount Wachusett Community College the following policies govern the use of all social media by the employees at Mount Wachusett Community College. The term "social media" is intended to address personal networking sites including, but not limited to, MySpace, Twitter, YouTube, or Facebook.

- Only authorized individuals may send or post messages on social networking sites on behalf of MWCC.

- Employees must be clear that they are speaking for themselves and not on behalf of MWCC when using social media. Employees should refrain from identifying MWCC in personally owned or controlled social media sites or personal commentary posted to social media discussions or pages, or their messages should have clear disclaimers that

the views expressed are personal to the author and do not necessarily represent the views of MWCC. Employees are reminded that they bear personal responsibility for the content of their posts, blogs or other social media content.

- Employees may not use MWCC logos or other trademarks or branding associated with MWCC's identity without prior, written approval from the Vice President of Marketing and Communications.

- All MWCC policies, including those related to harassment, discrimination, respect for diversity, retaliation, workplace violence, ethics, and conflicts of interest apply to an employee's postings and social media content.

- MWCC reserves the right to monitor employee use of social media. Employees may be disciplined for violating the confidentiality of MWCC, of fellow employees, posting harassing or defamatory content, or other infractions of MWCC's normal workplace standards of conduct. This applies to postings and blogging occurring at any time on any computer.

- MWCC employees are reminded that they should be respectful of co-workers, students, management, and other colleges and universities. It is recommended that you obtain authorization from individuals or colleges and universities prior to posting their picture, using their trademark, or identifying them by their name.

- Social networking that is not part of your official duties should be done on personal time using personal computers supported by commercial network assets and not college or other State owned resources.

- Personal Facebook profiles may not be used by supervisors or subordinates to communicate work related matters, This is not to be confused with participating in Facebook groups or pages.

- Employees are reminded to use discretion when using social networking media. If unsure about how policy or guidelines apply to your posting or social media site, employees are encouraged to consult with their supervisor before taking action whenever possible.

This policy is not intended to interfere with rights under the First Amendment or the National Labor Relations Act.

Compliance and Enforcement

Any individual found breaching the confidentiality of electronic communications, disclosing confidential College data, or otherwise violating this policy, may be denied future access to computer resources and may be subject to reprimand, suspension, dismissal, or other disciplinary actions by the President or his/her

designee consistent with College delegations of authority, codes of conduct, personnel policies, and union agreements.

Helpdesk Prioritization Practices

The Mount Wachusett Community College Information Technology Help Desk is chartered to provide a broad range of support services to the College Community. Within each prioritization band, incidents are handled in a first-in, first-out manner. Due to the large number of computers installed in the College [nearly 800] and the challenges of maintaining them, the Help Desk prioritizes its support requests according to this structure:

Support Call Priorities:

Priority	Description	Resolution Time
Urgent	A problem impacting a significant group of clients or a mission critical client support issue.	4 hours or less
High	A service issue is impacting a single user or a small group of users that warrants prompt attention because it severely damages or decreases the productivity of the user(s).	By the close of the current business day
Medium	A minor service issue that impacts a single user, non-critical software, or hardware without impacting user productivity.	By the close of the next business day
Low	Normal requests for information, new accounts, scheduled PC installations, upgrades, etc.	Two business days
Projects and Work Orders	A service request or special project of long duration that requires the interaction of multiple clients and technicians or is dependent upon the completion of multiple tasks. This includes software upgrades across computing labs or the creation of specialized reports from Administrative Systems. Projects must be requested and are worked based on College priorities.	As agreed upon at project initiation.

IT management uses the Helpdesk Online system to track open requests and to assess technician productivity. Individuals who bypass the Help Desk cannot be assured of a timely response to requests.

In addition to these general categories, we also consider the following when setting priority:

Safety of Personnel:
Any incident that puts the safety of members of the College Community at risk is our highest priority.

Safety of College Assets:
The protection of college assets, and the investment in those assets, is our next highest priority. Assets include physical assets, data assets, and intellectual property. However, at no time will the protection of material assets take priority over safety of personnel.

Class-in-progress incidents:
Technology problems that arise during a scheduled class period will receive an immediate response, subject to the availability of support staff. Our mission is to support the delivery of high quality instruction.

Administrative systems and support staff incidents:
An incident that affects the administrative systems will be addressed immediately, subject to the availability of support staff and the resolution of any higher priority incidents.

Accessing Helpdesk Services

As a shared service, the Helpdesk works across the College Community to assist our clients in the use of technical tools in their day-to-day jobs.

When desktop computers, administrative systems, voice systems, and networks fail to perform as expected, please alert the Helpdesk via telephone or email.

Upon receipt your request will be prioritized and assigned to a technician for resolution. Many requests are resolved over the telephone during the first contact. If it is not possible to resolve the request this way, a technician will be assigned and dispatched to provide on-site assistance. Technicians are only allowed to respond to requests on Mount Wachusett campuses. Technicians are expressly prohibited from traveling to individual's homes to correct problems. This is true even if the problem involves College systems.