

MOUNT OLIVE COLLEGE

INFORMATION TECHNOLOGY POLICIES & PROCEDURES

REVISED: AUGUST 2008

CONTENTS

1.0 USER RESPONSIBILITIES OF COLLEGE INFORMATION TECHNOLOGY RESOURCES

Preface

1.1 Respecting the Values Inherent in the College's Mission & Covenant

1.2 Abiding by Policies for the Mutual Benefit of All

2.0 INFORMATION TECHNOLOGY RESPONSIBILITIES AND PRIORITIES

2.1 Responsibility for Maintaining Information Technology

2.2 Priorities of Information Technology Use

3.0 INFORMATION TECHNOLOGY USE GUIDELINES

3.1 Use of Mount Olive College Information Technology Resources and Facilities

3.1.1 Facilities Usage

3.1.2 Internet Usage

3.1.3 Email Usage

3.2 Authorization and Security

3.3 Honor Code

4.0 COMMON FORMS OF COMPUTER ABUSE

4.1 Privacy Violations

4.2 Theft

4.3 Vandalism

4.4 Copyright Issues

4.5 Harassment

4.6 Chain Letters, Mass Mailings and Illegal Activities

4.7 Other Prohibited Acts

4.8 Penalties

4.9 Limits of Liability

4.10 Sanctions for Policy Violations

4.11 Distribution of this Policy

5.0 INFORMATION TECHNOLOGY EQUIPMENT ALLOCATION AND PURCHASE POLICY

5.1 Maintenance & Support

5.2 Allocations and Ownership

5.3 Reallocation of Equipment

5.4 New/Replacement Computer Requests

5.5 Standard Computers

5.6 Computers for New Employees

5.7 Purchasing Policy for Technology Equipment

6.0 WEB PAGE POLICIES AND PROCEDURES

6.1 Official web site

1.0 USER RESPONSIBILITIES OF COLLEGE INFORMATION TECHNOLOGY RESOURCES

Preface

Mount Olive College engages in the business of education. The College provides Internet, e-mail access, and various other IT systems as a business tool for employees and students, [hereafter referred to as 'Users' where appropriate, in this document] at significant cost. That means that the College expects Users to access the Internet, e-mail, and all IT systems only for the purpose of conducting College or College-related business. Limited use not related to College business must be kept to a reasonable level. Unauthorized access or excessive personal use of the Internet, the e-mail system, or any of the College's IT systems will subject the User to discipline, up to and including discharge, from the College.

[-portions excerpted from the Mount Olive College Employee Handbook, August 2008 revised edition]

1.1 Respecting the Values Inherent in the College's Mission & Covenant

All users are expected to respect the values inherent in the College's [Mission and Covenant](#) .

1.2 Abiding by Policies for the Mutual Benefit of All

This Mount Olive College *Information Technology Policy and Procedures* document has been developed to ensure that the College's information technology resources are utilized in ways that ensure the greatest possible benefit to all Users and to the institution. Responsible membership in the network community requires abiding by the rules and guidelines set forth in this policy statement.

2.0 INFORMATION TECHNOLOGY RESPONSIBILITIES & PRIORITIES

2.1 Responsibility for Maintaining Information Technology

The purpose of this policy is to define responsible and ethical behavior of all Users in order to preserve the availability and integrity of College resources.

Mount Olive College provides and maintains information technology, computing, and telecommunications technologies through the Office of Information Technology Services (OITS). The College relies heavily upon these systems to meet educational, informational, operational, and financial needs. These systems and machines must be protected from misuse and unauthorized access. The College's computers, computer systems, and computer networks, as well as the data they store and process, must be protected and maintained in a secure environment and in a responsible manner.

This policy applies to all College information technology and refers to all computers, hardware, software, data, and associated communication networks. This policy covers all equipment ranging from single User personal computers to those connected to the College network. Academic departments may have individual policies in addition to this general policy. In addition to this acceptable use policy, Users of these information technology systems are subject to applicable state and federal laws.

2.2 Priorities of Information Technology Use

Information Technology resources are provided to support the educational, research, and operations of its Users. The priorities for use of these resources are:

- **HIGHEST:** All education, research, and administrative purposes of the College.
- **MEDIUM:** Uses indirectly related to the College's purposes with education or research benefit.
- **LOWEST:** Recreation and/or social networking.

3.0 INFORMATION TECHNOLOGY USE GUIDELINES

To ensure continued compliance with computer usage guidelines Mount Olive College designates certain personnel to investigate alleged computer abuses. The College reserves the right to examine files in such cases:

Mount Olive College reserves the right to monitor *traffic* and *application usage*, across all systems, computers and peripheral devices on our Mount Olive College network.

The College reserves the right to *remove or limit access* to materials posted on College-owned computers and/or websites when applicable College policies or state or federal laws are violated. Individuals who believe that a violation of this policy has occurred should contact the Office of Information Technology Services.

3.1 Use of Mount Olive College Information Technology Resources and Facilities

3.1.1 Facilities Usage

Student Users have access to Mount Olive College-owned computing facilities at each of the College's locations. The following guidelines assure respect for other Users and these facilities. Users should:

- Recognize that academic use of the workstations has priority over all other uses. Recreational and social networking use in computing facilities is permitted during periods of light usage; however, Users may not play games or engage in other recreational or social networking activities when others are waiting to use the workstations for academic purposes.
- Refrain from bringing any food or drink into computing facilities
- Place cell phones in silent mode prior to entering the facilities
- Report any malfunction to the person on duty or to the organization responsible for the facility immediately.
- Refrain from moving, repairing, reconfiguring, modifying or attaching external devices to the systems without prior approval from the Office of Information Technology Services (OITS).
- Refrain from loading any software onto any hard drive without specific prior permission of the system administrator or custodian of the files.
- Realize that individual computing center facilities and other College facilities may post additional operational rules and restrictions that are considered part of this policy.

3.1.2 Internet Usage

The College expects that Users will use the Internet to improve their job knowledge; to access scientific, technical, research, marketing, or other information that has relevance to the College's business. Users should be aware that when accessing the Internet using Internet addresses and domain names registered to the College, our institution is legally responsible for content downloaded or stored on its computers. Therefore, Users cannot use the Internet for any purpose that would reflect negatively on the College or its representatives, or infringe on copyright with respect to the intellectual property of others. This includes using college information technology to engage in peer-to-peer file sharing of any illegally obtained intellectual property (including, but not limited to, audio/video media or software) using BitTorrent or similar protocols.

The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. It may be difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. Users accessing the Internet do so at their own risk. Finally, use of the College's information technology to access the Internet constitutes consent to monitoring by the User.

3.1.3 E-mail Usage

The College maintains an electronic mail system to assist in the conduct of business within the College. The use of the e-mail system for personal purposes is discouraged. E-mail is subject to the same restrictions on its use, and the same review process, as any other College-furnished resource provided for the use of Users.

The e-mail system hardware is College property, and all e-mail transmitted by, received from, or stored on the e-mail system resources (i.e., servers, personal computers, or printers) is the property of the College. Consequently, the College reserves and intends to exercise the right, through personnel authorized by the President, to review, audit, and access any messages created, received, or sent over the e-mail system for any purpose. The contents of e-mail properly obtained for legitimate business purposes may be disclosed within the College without permission of the employee. The privacy of any message should not be assumed or expected. Even if a message is erased, the message may still be retrieved and read. Further, the use of passwords does not guarantee confidentiality, and all passwords must be disclosed to the College. Use of the College's e-mail system constitutes consent to monitoring by the User.

3. 2 Authorization and Security

For each User, authorization to computer resources includes, but is not limited to, electronic mail, administrative records, library services and departmental-specific programs. Each User:

- Must have a valid, authorized account and may only use those computer resources which are specifically authorized.
- May only use his/her account in accordance with its authorized purpose.
- Is responsible for safeguarding his/her computing accounts and should change passwords often to ensure privacy and security.

3.3 Honor Code

Users:

- Must not use information technology systems to violate any rules in the *Employee Handbook*, the *Faculty Handbook*, the *Student Handbook*, or any local, state, or federal laws.
- Should disclose to the appropriate authorities misuses of the computing resources or potential loopholes in computer systems security and cooperate with the systems administrator in the investigations of abuses.

4.0 COMMON FORMS OF COMPUTER ABUSE

Misuse or abuse of the College information technology systems, computers, networks, programs, and data is forbidden. Violations in the areas listed below will be considered academic misconduct, misdemeanor, or felony as appropriate to the situation and will be dealt with accordingly.

4.1 Privacy Violations

Violations of the College's or another User's privacy include, but are not limited to the following:

- Unauthorized attempts to access another User's computer files without permission.
- Supplying or attempting to supply false and misleading information or identification in order to access another User's account.
- Unauthorized "borrowing" or examination of another User's output.
- Deliberate, unauthorized attempts to access or use the College's computers, computer facilities, networks, programs, data, or any system files other than those designated for public access.
- Unauthorized manipulation of the College's computer systems, programs, or data.
- Unauthorized capturing of computer network data directly from the network backbone or networking media.

4.2 Theft

Violations in this area include, but are not limited to:

- Abusing specific computer resources such as the Internet.
- Attempting unauthorized access to computers outside the College using the College's computers or communications facilities.
- Removing any computer equipment (hardware, software, data, pictures, articles, or books) without proper authorization.
- Copying, attempting to copy, sharing or distributing copyrighted or licensed software, data, files, pictures, articles, or books without proper authorization. For more information, see <http://definetheline.com> .

4.3 Vandalism

Alteration or attempted alteration of programs, digital data or other files, as well as resource or equipment destruction or disruption is considered vandalism. Violations include, but are not limited to:

- Installation of software or the intentional spreading of viruses, worms, trojans, etc., which can potentially cause harm to computer systems, networks, or to another User's account.
- Tampering with or obstructing the College's computer systems.
- Inspecting, modifying, or distributing data or software without proper authorization or attempting to do so.
- Damaging computer hardware and software

Vandalism will result in immediate cancellation of User privileges and possible restitution. (Vandalism is defined as any intentional attempt to harm or destroy data or equipment.)

4.4 Software Copyright Issues

The College owns licenses to a number of proprietary programs. Users who redistribute software from information technology systems break agreements with the College's software suppliers as well as applicable federal copyright patent and trade secret laws. Therefore, the redistribution of any software from information technology systems is strictly prohibited except in the case of software, which is clearly marked as being in the public domain. Mount Olive College will not provide legal defense for individuals who may be accused of making unauthorized copies. If the College is sued or fined because of unauthorized copying or use by any Users, the College may seek payment from the individuals as well as subject them to disciplinary action that may include expulsion or dismissal.

Violations include, but are not limited to:

- Copying, transmitting, or disclosing data, software or documentation without proper authorization.

4.5 Harassment

Harassment of others may be the sending, viewing, or printing of obscene or unwanted messages or files.

Violations include, but are not limited to:

- Interfering with the legitimate activities of another User.
- Sending abusive or obscene messages via computers.
- Use of information technology resources to engage in abuse of College personnel or other Users.

4.6 Chain Letters, Mass Mailings, and Illegal Activities

Unethical or illegal use is prohibited, and includes but is not limited to:

- Sending chain letters or unauthorized mass mailings.
- Using information technology for illegal purposes, which may include obscenity, child pornography, threats, harassment, copyright infringement, defamation, theft, or unauthorized access.

4.7 Other Prohibited Acts

In addition to the above, the following acts are also prohibited under this policy:

- Failing or refusing to comply with applicable software licenses, copyrights, and any other state and federal laws governing intellectual property;
- Selling College resources or engaging in other commercial activities not sanctioned by the College;
- Intentionally denying or interfering with IT service;
- Reading or modifying files without proper authorization;
- Using the College's IT technology to impersonate another; and
- Engaging in Ponzi schemes (e.g. a chain letter that requests recipients to send money to people on a list)

4.8 Penalties

Misuse or abuse of computing services is not simply unethical; it can be a violation of User responsibility as well as Federal Law. The United States Supreme Court has determined that Ponzi schemes are inherently fraudulent. The U.S. Criminal Code, 18 USC 1341-1346, prohibits the use of mail or wire in any attempt to defraud. Under the wire

fraud statutes, the attempt to defraud is a violation, and all who are involved in the attempt, whether intentionally or not, may also be in violation.

Therefore, Mount Olive College will take appropriate action in response to User misuses, unethical use, or abuse of information technology services. Actions may include, but are not limited to the following:

- Access to all facilities and systems may be suspended temporarily or removed permanently.
- Legal action may be taken to recover the damages.
- The matter may be referred to law enforcement authorities outside Mount Olive College.
- Students alleged to misuse information technology services will be referred through normal channels to the College's disciplinary system (see *Student Handbook*). If found to be in violation of College policy, including but not limited to *Information Technology Policies and Procedures*, the sanction imposed will be in accordance with the policies and procedures outlined in the *Student Code*.

4.9 Limits of Liability

Mount Olive College may not be held liable for loss incurred with the use of the computing facilities. Such losses include but are not limited to destruction of data and software brought about by natural disasters and intentional sabotage that are beyond the College's control. Users assume liability for their own physical and emotional well-being and may not hold the College liable for injury sustained on campus facilities. The College has installed sufficient anti-virus software to promote a clean work environment. It is the User's responsibility to make a conscientious effort to ensure that viruses are not transferred into the system. Users are encouraged to scan disks for possible virus infections prior to and after each use.

4.10 Sanctions for Policy Violations

Violations of this policy will be treated as academic misconduct, misdemeanor, or felony as appropriate.

For non-criminal matters, penalties may range from a warning to loss of User's account to termination of employment.

A warning will be issued after a User's first policy violation, and the User will be asked to sign a copy of this policy statement to document that he/she understands and is willing to comply with these policies. A second violation will result, at a minimum, in the suspension of the User's account for one week. A third violation will result, at a minimum, in the suspension of the User's account for three months. A fourth violation will result in the permanent loss of privileges.

Misdemeanor or felony violation charges will be prosecuted to the fullest extent of the law and may result in the immediate and permanent loss of privileges. Disciplinary proceedings may also be initiated against violators. Violators of federal and state statutes may expect legal sanctions from the appropriate authorities.

A student User has the right to a fair hearing by the Judiciary Committee concerning the policy violation and the disciplinary action recommended. Appeals of disciplinary actions should follow the procedures set forth in the *Student Handbook*.

4.11 Distribution of this Policy

Mount Olive College will insure that all Users are aware of the policy by publishing and distributing it in appropriate media to reach all Users.

5.0 INFORMATION TECHNOLOGY EQUIPMENT ALLOCATION & PURCHASE POLICY

5.1 Maintenance & Support

The Office of Information Technology Services (OITS) provides support for computers that use Windows operating systems. Such support includes hardware maintenance, repair, and network services, operating system upgrades, applications software consulting, and documentation. See Section 2.2 Priorities of Information Technology Use

5.2 Allocations and Ownership

Primary Computers: The College will provide to each employee, upon request, a primary computer capable of running all supported applications, including those for word processing, spreadsheet, database, electronic mail, Internet access, and library catalogue access. The exact configuration of primary computers will evolve along with the evolution of technology. Each machine will come bundled with a basic application suite and electronic mail package and Internet browser. Maintenance and repairs will be provided at no cost to employees. Replacement will usually occur on a 3-4 year cycle or as the College's budget permits.

Instructional Support Equipment: The College will endeavor to provide, or assist academic and outreach units in obtaining computers for instructional purposes, courseware development, and laboratory automation, through start-up funds, external grants, and the annual Information Technology equipment request process. Replacement cycles for computers in this category will be determined on a case-by-case basis. Maintenance and repairs will be provided at no cost to departments.

Privately-Owned Computers and Information Technology Equipment: Employees may purchase computers through Mount Olive College or may use computers purchased elsewhere. The College will not provide maintenance and repair for privately owned computers. Computers purchased outside of Mount Olive College must be approved by OITS before being connected to the college-wide network.

5.3 Reallocation of Equipment

All computers and IT equipment considered the property of Mount Olive College are under the management of the Office of Information Technology Services. Computers that are allocated to individual employees cannot be re-deployed or modified without prior OITS approval. Computers that are replaced must be returned to the OITS allocation pool for re-distribution. The equipment may be reallocated to the original User via the standard equipment request process, if there are no other requests of higher priority at that time and if not obsolesced beyond scope of current Information Technology support policies.

5.4 New/Replacement Computer Requests

Requests are routed from individual employees in the fall of the current academic year for new or replacement computers to be purchased in the following school year. These requests are organized and routed to the appropriate Vice President with suggested priorities. Requests are evaluated by the area Vice President and the Director of Information Technology Services, and approved, denied, or deferred according to justification and funds available.

5.5 Standard Computers

Due to the rapid change in computer development, it is impossible to define a standard computer in detail. However, the OITS does establish and publish a standard during each fiscal year. This standard computer is capable of meeting the business productivity needs of employees. These needs generally include word processing, spreadsheet, e-mail, Internet, and other productivity software along with sufficient excess capacity to meet expansion for the next several years.

5.6 Computers for New Employees

New employees, as appropriate to performance of their duties, will receive a standard computer package. Any costs above the cost of the standard package are to be paid for by departmental funds, with approval from the area Vice President and the Director of Information Technology Services.

Computers and other information technology equipment, which were used by departing employees, are reallocated according to the decision made by the divisional head and the Director of Information Technology Services. This equipment does not necessarily remain in the same department or division.

5.7 Purchasing Policy for Technology Equipment

It is the goal of the Office of Information Technology Services to assure the College community of computer hardware, peripherals, and software that can be supported. Information Technology Services employees have the primary responsibility for maintaining the networks, computers, servers, printers, peripherals, videoconferencing equipment, and VoIP phones to be certain that quality is maintained at reasonable costs.

All equipment, computers and peripheral devices (e.g. printers, scanners, LCD projectors, digital cameras, software, video cards, and network cards) which are attached to or used with a computer must be ordered only after consultation with the appropriate Vice President and the Director of Information Technology Services. The review procedure for purchasing any technology equipment and software is intended to provide:

- a centralized point of information about technology items
- a campus-wide inventory of hardware and software
- Pricing advantages
- License compliance for software purchases
- Hardware and software that can be supported

In order to coordinate and standardize on technology equipment and software purchases in a uniform and planned way so as to avoid duplicate selection which could make the maintenance and operations of the technology program difficult and costly, the following purchase procedure is to be used:

- Requisition submitted to the Director of Information Technology Services for review.
- Requisition initialed and sent to the area Vice President and Business Office for final processing
- Purchase order approved and signed by the Vice President for Business-Finance and the item ordered, if within the departmental budget constraints, and subject to the general availability of funds.

6.0 WEB PAGE POLICIES & PROCEDURES

6.1 Official web site

The Office of Information Services-Web Services maintains the College's official web site. The official Mount Olive College home page address is www.moc.edu .

The primary audience of the official web site is current students. Secondary audiences include prospective students, employees, alumni, media, and the general public searching for information about the College.

Official web pages for academic and administrative units are initially created by the College Webmaster in adherence to official College web and graphic design policies. College web pages utilize the standard template(s) provided by the College Webmaster and content is updated by designated departmental editors via the College's distributed web content editor. All content is subjected to the approval processes as set by the College's Office of Information Services prior to posting.

The College reserves the right to *remove or limit access* to materials posted and/or linked on official College websites when applicable College policies or state or federal laws are violated. Individuals who believe that a violation of this policy has occurred should contact the Office of Web Services or click on the 'Report a Problem' link located at the bottom of each official Mount Olive College web page.