1 Universal Policies

1.1 Personal Responsibility

1.1.1 Acceptable Use

With the freedom of access provided by our computing and telecommunications network comes the responsibility of good citizenship. As with any community, the electronic community of which you are now a member cannot function without some sense of order.
In general, the principles of MNU's Code of Conduct apply to network citizenship. Computer and network use, however, require further specificity to ensure appropriate behavior. Access to electronic information systems at MNU is a privilege, must be treated as such by all users, and may be revoked if MNU policies are not followed.
Your acceptance of any account and/or using our network constitutes your agreement to abide and be bound by the provisions of the applicable MNU policies regarding the MNU technology team use. Ignorance of the policy is not a valid or an acceptable defense.
The MNU computing resources and network are for the use of MNU faculty, students, and staff, and are to be used only for the academic, administrative, educational, and research purposes of the institution.
For any computers or devices for which support from the MNU technology team is requested or expected, now or in the future, once it has been configured by the MNU Technology team for accessing University resources then from that point forward no one except an authorized representative from the MNU technology team may make any changes to that computer or device that adversely affect its security, or the MNU technology team administrative or user access rights or permissions, or its network connectivity. Failing to adhere to this policy may result in one or all of the following:

- That computer, device, and/or the user(s) may be ineligible for continued support from the MNU Technology team
- It and/or the user(s) most likely will lose some or all access to University technology resources, without recourse
- It and/or the user(s) may receive other intentional consequences as may be deemed appropriate

MNU acknowledges that faculty, students, and staff use MNU computing resources assigned to them or to which they are granted access for non-commercial, personal use (e.g., email). Such occasional non-commercial use is permitted if (i) the use is not excessive, (ii) does not interfere with the performance of any faculty, staff member, or student's duties, (iii) does not interfere with the efficient operation of the MNU network or the MNU technology team computing resources, and; (iv) is not otherwise prohibited by this policy or any other MNU policy or directive.
Personal use of MNU computing resources by any user for personal financial gain in connection with non-MNU consulting, business, or employment is strictly prohibited except for specifically authorized faculty and staff. Any such personal use of MNU computing resources in conjunction with non-MNU professional consulting, business, or employment activities is permitted only when the use has been expressly authorized in writing by the MNU Administration at the appropriate level.
As general policy MNU employees will not read your email or private files, whether stored centrally or locally. Information and messages stored on or sent over the MNU network, however, are not secure and can be intercepted in a variety of ways. MNU faculty, students, and staff accessing the MNU network cannot and must not assume such information will be or remain inaccessible or confidential. Accordingly, MNU cannot and does not guarantee user privacy. Further, MNU expressly reserves the right to inspect and examine any MNU owned or operated computer system, computing resource, user account and/or file or information contained therein at any time in response to security threats to the system or MNU Community members, to investigate claims of violations of this policy or other MNU policies, and when routine system maintenance identifies possible security threats or policy violations.
All use of the network must abide by the following Guidelines. That is, the use:
1. Is consistent with MNU's lifestyle statement.
2. Is consistent with the purposes of the network.
3. Does not interfere with the work of other users of the network.

4. Avoids wasting institutional computing resources.
5. Is consistent with the ethics of computing at MNU.
6. Is consistent with applicable state and federal law.

Computer and network use at MNU are guided by the same principles, and subject to the same disciplinary sanctions, as for other campus activities.

Examples of Unacceptable Activities for each Guideline

Here are some examples of activities that would violate one or more of the Guidelines. They are meant to be illustrative, not exhaustive.

1) See MNU's Lifestyle Statement

Review the *MNU Student Handbook* for examples dealing with lifestyle issues.

2) Is consistent with the purposes of the network

Usage that is unacceptable because it conflicts with the stated purposes of the network includes, but is not limited to, these examples:

- Advertising of commercial products, services and businesses that are not affiliated with or sanctioned by MidAmerica Nazarene University is unacceptable.
- It is not acceptable to use our printing facilities to produce output that is not related to the University's mission (i.e., it is not acceptable to print announcements or fliers for outside agencies, materials for one's own or a spouse's business, etc.).
- Using MNU's network to support personal business interests is unacceptable.

3) Does not interfere with the work of other users of the network

Usage that is unacceptable because it may interfere with the work of other users includes, but is not limited to, these examples:

- Usage that is likely to result in the loss or disruption of another person's work is unacceptable. Examples of such activities include tampering with network electronics or interfering with an active client computer or network server.
- Messages which cause an ongoing interruption in the work of another person are strictly unacceptable (e.g., e-mail that is sent after the recipient has requested that it be stopped or is sent indiscriminately to large groups of users).

4) Avoids wasting campus computing resources

Usage that is unacceptable because it wastes computing and/or network resources includes, but is not limited to, these examples:

- In the library and in public labs, it is not acceptable to print multiple copies of output. Printing of large documents not directly related to course work or job function and of large numbers of e-mail messages is also unacceptable.
- Chain letters and broadcast messages to lists or individuals, and other types of use including transfer of large amounts of data (large files or large numbers of files such as multimedia files) which might cause congestion of the network or otherwise interfere with the work of others are not acceptable.

5) Is consistent with the Ethics of Computing at MNU

Usage that is unacceptable because it is not consistent with this statement includes, but is not limited to, these examples:

- It is not acceptable to alter, disable, or remove any software which resides on a machine in MNU's public computing areas or accessible via MNU's network.
- It is not acceptable under any circumstances to use another person's username and password to gain access to MNU's computing resources, including printing resources, even with that person's permission or cooperation, and not even at their own request.
- It is not acceptable to share your access information (e.g., your password) to an MNU account with anyone, including an employee, a spouse, a parent, a dependent, or a friend.
- It is not acceptable to physically tamper with, tap, disable, or remove any equipment, wiring, or networking hardware from the public computing areas, classrooms, offices, residence hall rooms, or equipment areas.
- It is not acceptable to possess or use any software or hardware designed to disrupt the security of the campus network and all devices attached to the network. Likewise, it is unacceptable to engage in any activities designed to spy on the network activities or communications of other users.

- It is not acceptable to scan machines which you do not own (or have administrative responsibility for) for security vulnerabilities, including both machines on the network and on the wider Internet.
- It is not acceptable to read or electronically bring to campus pornographic material of any type. Remember, just because you can find it on the net is not justification to read it.

6) Is consistent with applicable state and federal law

Usage that is unacceptable because it conflicts with state or federal law includes, but is not limited to, these examples:

- Messages which harass an individual or group are strictly unacceptable.
- Users of the network may not share over the network, software or multimedia materials (such as MP3 music files or video files, such as commercial movies) for which they do not have the license to share. A single-copy license is not a license to share copyrighted material over the network.
- Attempts to discover or obtain via coercion, hacking, or any other method user accounts and passwords. It is also against our policy for any unauthorized parties to utilize any so-called super-user (e.g. root, admin, administrator, etc.) accounts.
- Most software used in the academic arena is copyrighted. It is your responsibility to make sure that you have the proper license to use the specific software. A good rule of thumb is that you should never use commercial software that you did not purchase. This insures that you are operating within the law, and also protects your computer from possible viral infection.

7) Is consistent with several additional key issues

- *Racial and sexual harassment via the network:* MNU has explicit policies regarding racial and sexual harassment. Neither of these forms of inappropriate behavior is acceptable on MNU's network, and all incidents will be dealt with according to established procedures.
- *Electronic mail:* E-mail is an important network service that allows the user to reach beyond the confines of the campus. Because of the relatively impersonal nature of the interaction, opportunities exist for misuse. Therefore, acceptable use requires the accurate and unambiguous identification of the source of all sent messages.
- *Computer accounts:* A personal e-mail account is automatically issued to all students and employees near the time they begin at MNU. Accounts on other specialized computer systems are provided as needed. Any account is for the use of the MNU-assigned owner only. Account names and passwords should not be shared, as any violations of network policies can and will be traced by login name. You are ultimately responsible for all violations committed under your login name, even if you claim the violations were committed by someone else who had either authorized or unauthorized access to your account.
- *Disk storage space:* Space for storing data on MNU's networked computer systems is a limited resource. You should not save unnecessary files and should delete files that are no longer needed. When the Technology team has evidence that you have stored files with inappropriate content (e.g. copyrighted materials without permission, pornography, etc.), those files are subject to review without notice by the appropriate computer center and/or administrative staff. Also, accounts of students who have not been actively enrolled in courses for over one year are purged periodically.
- *Use of external networks:* Computers connected to the network have access to the Internet. All users are expected to abide by MNU's policies when accessing the Internet through this connection.
- *Network integrity:* You may not tamper with any network cabling or routing devices beyond the wall plate in your office or room. Any problems with these devices or cabling will be serviced by the MNU technology team. Likewise, you may not extend the network from your wall plate to another room or building. Incorrect cabling can lead to significant lightning damage risk, and/or network performance problems beyond your local area.
- *File servers:* In general, we will not prevent users from setting up their own computers as file servers on our network. However, we have the right to revoke the privilege of running a service which is inappropriate or degrades network service. Also, the owner of the server is responsible for the content on the server. The content must be legal with respect to copyright and other laws, and must abide by all other principles contained in this document.
- *Student websites:* Students may create and originate individual websites using MNU computer resources, but must comply with all MNU policies as well as federal, state, and local laws and regulations, including copyright laws, obscenity laws, and laws relating to libel, slander, defamation, and software piracy. Further, the person creating a website is responsible for the accuracy of the information contained therein. Websites should include in

an easily identified location a valid email address of the person to whom questions/comments may be addressed, as well as the most recent revision date.

1.1.2 Ethical Use of Computing Resources

A. Computing Resources at MNU

MNU has invested considerable resources to develop a number of work areas supporting computing for all students (day, evening, online, graduate), faculty, staff, and guests who have accounts on our systems. Our computing community is quite large: potentially over 2000 users. It is also very diverse: beginning and experienced users often work side by side on tasks ranging from simple word processing to extensive user-created systems. The size of the institutional investment as well as the complexity of both the computing community and resource requirements clearly demand that all users approach computing responsibly and ethically. When an individual misuses our resources or acts in unethical ways, we all suffer. When we do our computing in a cooperative manner, we all benefit directly.

B. Ethical Use of Resources Based on Stewardship

MNU is a community of Christian scholars and staff seeking to serve the Lord through study and service. Our computing resources are not an end in themselves; they are a means to enable us to develop into effective servants of our Lord. Therefore, in order to be good stewards of this resource, we agree to:

- Seek to minimize paper use – e.g., multiple copies should be made on copy machines rather than computer printers; a year's worth of e-mail messages should not be printed, etc.
- Utilize the printers and computers fairly – e.g., logging out when leaving a public computing area; leaving computers in proper set-up mode; reprinting only those pages that have been edited rather than entire documents; and refraining from transferring large documents or multimedia materials during prime hours when the systems are heavily used, etc.
- Restrict recreational computing – courteous levels of sound, noise, and conversation in lab areas are to be maintained. Computer-generated sounds and computer games causing competitive user interaction are not allowed. Recreational computing must not compete for resources with administrative, instructional, or research computing, especially with regard to streaming media, which may consume significant amounts of network bandwidth and thereby degrade network performance and Internet speed for other users.
- Seek to minimize disk usage – those who store files on MNU's systems should practice good housekeeping by regularly removing e-mail messages and other files that are no longer needed.
- Refrain from viewing, displaying, or transferring inappropriate material such as pornographic photographs or videos.

C. Ethical Use of Resources Based on State and Federal Laws

Webster defines theft as the act of taking the property of another without right or permission, often done secretly. We usually have no problem applying this definition to money or possessions. However, unauthorized copying of copyrighted software or multimedia materials (such as MP3 music files) is also taking property without right or permission. Securing passwords of unsuspecting users is likewise stealing. At MNU, we agree to:

- Refrain from unauthorized copying or modification of programs (including commercial software) or data belonging to others.
- Notify the help desk if a way to break system security is discovered.
- Assist any users who have inadvertently left their accounts open, by either logging off the open account immediately or by immediately notifying the other user of the need to do so.
- Refrain from changing user interfaces or system setups, especially on shared computer resources (e.g. computer lab and classroom computers), out of courtesy and respect for the next user. Refrain from sending demeaning,

hurtful, or disrespectful messages. Refrain from attempting unauthorized access to systems on the MNU Campus or anywhere else in the world.
Scanning the devices on the University's networks or on the Internet to identify security vulnerabilities (e.g. by "port scanning" and other means) is often a prelude to compromising the security of the devices. It is therefore perceived by many systems administrators as a threat, and may be a violation of state and federal laws. Therefore, any such scanning activity from any University device or from any device connected to the University's networks is expressly prohibited.

D. Our Community Expectations

We are proud of MNU's long tradition of integrity and honesty. We commit ourselves to making our computing environment the best it can be for the entire community. It is important that we make a strong effort to pass this legacy on to those users who will follow.

E. Consequences of Unethical Use of Computing Resources

Violations of the MNU Computing Acceptable Use Policy shall subject users to the regular disciplinary processes and procedures of MidAmerica Nazarene University for faculty, students, and staff, and may result in loss of their computing privileges. Illegal acts involving computing resources may also subject violators to prosecution by federal, state, or local authorities.
Decisions as to whether a particular use of computing resources conforms with policies shall be made by: the office of the Vice President for Academic Affairs Office if the use involves faculty or student academic issues; by the Office of Student Life if the use involves non-academic student use; or by the Department of Human Resources if the use involves administrators or staff.

1.1.3 Copyright Infringement

Reporting Potential Copyright Infringement

In accordance with the Digital Millennium Copyright Act (DMCA) MidAmerica Nazarene University has designated an agent to receive notice of unauthorized online use of copyrighted materials. If you believe that your copyrighted work is being infringed, please notify our copyright agent specified below.
E-mail may be sent to: ledagley@mnu.edu
Mail may be sent to:
Copyright Agent
MidAmerica Nazarene University Library
2030 College Way
Olathe, KS 66062 Phone: (913) 971-3563
Please notify us in writing and include all of the following:

- Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site is covered by a single notification, a representative list of such works at that site.
- Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit MidAmerica Nazarene University to locate the material.
- Information reasonably sufficient to permit MidAmerica Nazarene University to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.
- A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, the MNU technology team agent, or the law.
- A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

- A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

Process for Handling Notification of Copyright Infringement related to Movie, Music, and Television program Downloads

When the university's Copyright Agent receives notification that a movie, music, or television program file has been downloaded the Copyright Agent takes the following steps:

- The Copyright Agent sends a response to the notifying agent that the matter is being handled according to internal policies.
- The Director of IT is notified regarding the copyright infringement notice;
- The Director of IT tracks the IP address listed in the infringement notice and provides the name of the person who owns the computer on which the IP address is registered;
- The Copyright Agent notifies the person as to the infringement and provides the information on how to remove the files from one's computer. It is further stated that failure to comply may result in the loss of Internet and network access.
- Persons who repeat the offense following the notification may lose access to the university's network and Internet access.

Full text of the Digital Millennium Copyright Act (DMCA): www.copyright.gov/legislation/dmca.pdf

1.1.4 Media File Ethics

MNU is sometimes contacted by representatives of the Recording Industry Association of America (RIAA) and of the Motion Picture Association of America (MPAA) regarding the use and sharing of digital MP3 music and digital movies. As you can see, the letter reprinted below illustrates the dangers associated with the misuse of copyrighted media. It is important for each of us to realize that even though there are Internet websites which offer free music and video downloads it is not necessarily legal to do so. It is often a direct violation of copyright laws, which can carry very stiff and stringent penalties.

For perspectives on this important topic, you are encouraged to read this article from eCampus News: Movie Industry to Colleges: Remember Copyright Rules. Also, please review this letter to university campuses from the president of the MPAA.

With the technology employed by MNU, it is possible and probable for students violating this policy to be identified and disciplined. Actual disciplinary action will be determined on a case-by-case basis, but the normal procedures involve first a notification of violation along with a cease-and-desist demand. Even one subsequent violation may result in restrictions or suspension of all University network and computer privileges, and/or other sanctions or penalties up to and including expulsion from the University.

As members of a Christian learning community, we should encourage one another to live with integrity, according to biblical principles, and to abide by federal and state laws as well as by MNU's computer acceptable use policy.

1.1.5 Social Media

Definitions regarding Social Media:

- **Social Media**: Includes all methods of interaction online in all forms of user generated and distributed content, including but not limited to, blogs, social networking sites (e.g., Facebook, Twitter), and wikis.
- **Professional Use**: Refers to using social media to advance a segment or function of MidAmerica Nazarene University as part of your job responsibilities.
- **Personal Use**: Refers to things you may do to socialize or advance yourself personally, although this may include some professional activities such as networking or promoting your academic research or writing.

Purpose

It is in MidAmerica Nazarene University's interest—and we believe, in each employee's interest—to be aware of and participate in social media — the information, interactions, and idea exchange available via the Internet. As an institution of higher education, we believe in the importance of open exchange, learning, and honest discourse.
In addition, MidAmerica Nazarene University has always encouraged employees to be champions on behalf of the organization by spreading the word about MNU's mission, vision, and values. The rapidly growing phenomenon of blogging, social networks, and other forms of online electronic publishing are emerging as unprecedented opportunities for outreach, information-sharing, and advocacy.
The goal of this policy is to guide employees regarding how their use of social media interacts with their responsibilities as a MNU employee, with the goal of ensuring positive experiences and consistent brand representation for the university. This policy is not related to student or prospective student use of social computing.

Personal Use

While social media offers great opportunities for MidAmerica Nazarene University employees to communicate and collaborate, both internally and externally, it also brings equally great responsibilities. Social media blurs the lines between personal and professional as no other technology has before. By virtue of identifying yourself as a MidAmerica Nazarene University employee within a social network, you are now connected to your colleagues, managers, and even MidAmerica Nazarene University's students, prospective students, donors, parents, and other friends.
As an employee of MidAmerica Nazarene University, your online postings always have the potential to impact the university, even those you make on a personal level. As such, please conduct your online engagement in accordance with MNU's Statement of Belief, and the MNU Network and Computer Acceptable-use Policy.
Your online postings should always represent your personal point of view and not necessarily that of MidAmerica Nazarene University and this distinction should be clearly indicated. When posting your point of view, you should neither claim nor imply you are speaking on MidAmerica Nazarene University's behalf. When appropriate, please be clear to indicate that the views expressed on your posts are your own and do not necessarily reflect the views of MidAmerica Nazarene University.

Professional Use

As mentioned above, professional use refers to using social media to advance a part or activity of MidAmerica Nazarene University, such as a department (i.e., alumni, admissions, academic schools), as part of your job responsibilities. The guidelines in this area are meant to ensure consistency and quality in representation of MidAmerica Nazarene University in social media, and also to ensure that departments and offices are not creating redundancies, or sending competing or mixed messages to valued MNU audiences.

- Representing MidAmerica Nazarene University as a whole is reserved for the Office of Communications and Marketing and the Office of the President. No unauthorized person or group should seek to speak for the university or secure an account or name that represents the entirety of MidAmerica Nazarene University.
- Representing segments of MidAmerica Nazarene University (i.e., admissions, alumni, church ministries) are best done by the office most closely related to these functions. Those seeking to represent their area in social media should first contact the Office of Marketing and Communications, which will advise on naming (to avoid duplication and ambiguity both internally and externally) and provide best practice tips and resources for representing a segment of MidAmerica Nazarene University. In addition, the Office of Marketing and Communications will maintain a list of official social media accounts, the offices that maintain them, and contact information for each. If an office or department already has an official group or account at the time of this policy creation, please contact the Office of Marketing and Communications.
- Accounts and other electronic contacts created and disseminated for offices and departments should not be tied to any employee's personal information—email addresses, passwords, etc. Rather, accounts should be established

that can be shared by multiple individuals in each area. This will ensure smooth transitions for the accounts as employees' duties and responsibilities change over time.

- If use of a MidAmerica Nazarene University logo is desired, contact the Office of Marketing and Communications, which will supply an approved and appropriately sized logo. Do not resize, crop, personalize, or otherwise distort the university logo.
- Any online advertising (paid and free) needs to be approved by the Office of Marketing and Communications for consistency and quality.
- Any use of photography must adhere to photography use guidelines established by the Office of Marketing and Communications.
- Remember that you are legally responsible for anything you post online. Ensure you abide by copyright and fair use laws. Always cite sources and references and, whenever possible, link back to them.
- Online postings should not disclose any information that is confidential or proprietary to the university, or to any third party that has disclosed information to MidAmerica Nazarene University.
- If a member of the news media or a blogger contacts you about an online posting that concerns the business of MidAmerica Nazarene University, please refer that person to the Office of Marketing and Communications.
- If you make an error, be up front about your mistake and correct it quickly. In a blog, if you choose to modify an earlier post, make it clear that you have done so. The key with social media is to be as transparent as possible.

MidAmerica Nazarene University gratefully acknowledges the following sources in the creation of the MNU social computing policy: BurellesLuce, IBM, and Easter Seals

1.2 Technology Access and Usage

1.2.1 Website Design Standards

MNU has invested significant resources to develop and implement comprehensive branding, design, and publishing standards and guidelines that govern any and all internal and external communication (e.g. print, electronic, video, etc.). These are to be followed and used at all times.
A comprehensive set of resources and other useful information regarding all University communications, including websites, is available on the MNU Marketing and Communications website at http://www.mnu.edu/marketing.
A discussion of MNU's brand is at:
https://365mnu.sharepoint.com/Employees/Marketing/SitePages/The%20Brand.aspx
MNU graphic design standards may be reviewed at
https://365mnu.sharepoint.com/Employees/Marketing/SitePages/The%20Standards.aspx.

1.2.2 Email

The use of e-mail for departmental or college-wide information

In addition to its use in individual communication, e-mail at MNU is also a primary vehicle for the transmission of official information to the members of the MNU community. Official email communications are intended only to meet the academic and administrative needs of the campus community, and are distributed through endorsed mailing lists. The institution has the right to expect that such communications will be received and read in a timely fashion.

Availability of e-mail accounts

Official MNU email accounts are available for all enrolled students, and for all faculty and staff. Official email addresses will be directory information unless the account user requests otherwise.

Redirecting of email

Redirecting or automatic forwarding of MNU email accounts is not allowed. MNU students, faculty, and staff are expected to interact directly with the MNU email system.

Expectations about community use of email

Students, faculty and staff are expected to check their email on a frequent and consistent basis in order to stay current with MNU-related communications. They have the responsibility to recognize that certain communications may be time-critical. "I didn't check my email", errors in forwarding mail, or email returned to the University with "Mailbox Full" or "User Unknown" are not acceptable excuses for missing official MNU communications via email.

Privacy

Users should exercise extreme caution in using email to communicate confidential or sensitive matters, and should not assume that email is private and confidential. It is especially important that users are careful to send messages only to the intended recipient(s). Particular care should be taken when using the "Reply" and “Reply All” options during email correspondence.
While the University respects the privacy of electronic communications and makes every attempt to keep email messages secure, privacy is not guaranteed. MNU does not routinely monitor or access the content of email messages whether stored on University equipment or in transit on the University network. The content of electronic communications will not be accessed during the execution of systems support, network performance, and related security functions; but system administrators may access and disclose such contents when access and disclosure are necessary to protect the integrity of information technology resources, to ensure that these resources are equitably shared, to respond to health and safety emergencies, or to respond to subpoenas, court orders, or other valid forms of legal process. Where there is evidence of a criminal offense, the matter will be reported to MNU’s judicial systems and/or law enforcement. The University will cooperate with the justice system in the investigation of the alleged offense.
In addition, with appropriate authorization, the University may investigate complaints received from both internal and external sources about unacceptable use of email that involves MNU’s email facilities and/or MNU’s computer network. Requests to access or disclose the content of email will be handled within the following guidelines:

If the email account belongs to a:	Then written permission must be obtained from:
Faculty Member, Student	Provost
Staff Member (including student employees)	Director of Human Resources
Alumni	Vice President for University Advancement

All requests to access or disclose the content of email, including detailed information on why the request is being made, should be sent from the appropriate person authorized above to the Chief Information Officer for processing. If the request is the result of a court order, then written permission from the above authorized person is not required.
With the exception of content covered by the University's intellectual property policy, all electronic information residing on University-owned systems and all Internet traffic generated through or within these systems, are the property of the University. They are not the private property of any University employee, faculty, staff, contractor, student, or other person.

Mailing lists

At MNU, there are mandatory and voluntary mailing lists.

- *Mandatory lists*, departmental or institution-wide, convey information central to academic or administrative responsibilities, and the student, staff or faculty member is accountable for that information. No one can opt out of a mandatory list.
- *Voluntary lists*. Voluntary lists are of two types: opt-out and opt-in.
- *Opt-out lists* are lists in which the community member is enrolled by default, but has the opportunity to unsubscribe by request. Such lists transmit important information (i.e. career services information), though most often not essential to day to day tasks.
- *Opt-in lists* are based on areas of interest. Community members request to join them.

Mailing lists creation and administration

Lists are created by the Technology team at the request of other departments and/or organizations. E-mail lists that include students require the approval of the Vice President of Academic Affairs. The list-owner is the department or organization's head or his/her delegate. Technical management of the list resides in the Technology team.
Some lists (e.g. class lists, advisee lists etc.) are automatically created by software such as Banner or Moodle.

Mailing lists usage

Discretion is advised in the sending email to lists to avoid giving users the sense that they are being unnecessarily spammed. Also, senders should use discretion when attaching files to email directed to lists. Large file attachments are strongly discouraged. Some lists may be moderated, in that they require review and approval by specific individuals before an email will be released to be delivered to the list members.

1.2.3 Use of Non-MNU Servers and Technology Vendors

Policy: It is MNU's policy to restrict the use of external technology service providers for services including but not limited to email, email lists, email accounts, chat rooms, and web hosting for any official communication regarding MNU. Requests for exceptions to this policy must be discussed and approved by the Technology Advisory Council and by the marketing department. Contact MNU's webmaster at marketing@mnu.edu to discuss your needs.
Rationale: As technological capabilities expand, MNU continues to evaluate the ways in which technology can help promote our mission. Unfortunately, the electronic communication of official MNU information through outside vendors and servers that provide Web pages, email listservs, discussion boards, email accounts, and other forms of electronic communication can distract from our goals and reflect badly on MNU. We have found that outside vendors often use the information given to them to distribute advertising or other communication that is not in keeping with our values.

1.2.4 Pre-Purchase Policy for Acquisition of Technology Resources

In order to (1) provide the best service possible; and (2) maintain the integrity of MNU's strategic data network, MNU maintains the following policy regarding acquisition of technology resources.
Policy. The MNU technology team must pre-approve all MNU purchases of computing resources for which either support from the MNU technology team or connection to MNU's data network is desired. The MNU technology team will certify eligibility for support and connection to the network by putting MNU inventory stickers on equipment. The MNU technology team may refuse to support or to connect to the campus network any equipment that does not have prior authorization. Additionally, the Accounts Payable department is not authorized to pay for any such purchases that have not obtained prior the MNU technology team approval.
Included Resources. This policy covers any MNU equipment and software for which either the MNU technology team support or connectivity to the data network is desired. Examples include but are not limited to computers, peripherals, software, printers, tablet devices, phones, and copiers. Web applications (e.g. hosted or cloud-based

software) that will be used by any MNU audience also require the MNU technology team approval even if they are hosted by outside vendors and/or paid though departmental accounts or grant funding.

Restricted Purchases. This policy prohibits independent purchases and/or operation of printers and copiers at university expense for any reason, including all associated consumable supplies and maintenance. Any deviation from this restriction requires written approval from the MNU technology team even if they are intended to be paid though departmental accounts or grant funding. Otherwise, Accounts Payable is not authorized to reimburse an individual, department, or cost center for any direct expenditure committed for equipment purchases or operating expenses for any university printing/copying and no such device may be connected to the university network or any other university computer equipment, including individual computers, without the express approval of the MNU technology team.

Rationale. The mission of the MNU technology team is to help all MNU users fulfill their goals and responsibilities through the provision and appropriate use of information-technology. To succeed, users must have reliable computer systems and a reliable network. The reliability of current systems is largely dependent upon successful communication among a large number of extensive, expensive, and very complex networks, software programs, and related hardware. Allowing unknown and untested products into the environment greatly increases the probability of incompatibilities that cause problems for one or many users. Thus, for the benefit of all we must limit our support to those combinations of products that we have successfully tested in our environment. This policy is based upon good business practices that are associated throughout higher education with the delivery of reliable, secure services. We appreciate your support of and compliance with this policy.

The MNU technology team Commitment. Faculty, staff, and students share many common needs for information technology and telecommunications services. They also have different requirements based upon varying goals and responsibilities. The MNU technology team will strive to provide (1) institution-wide services and tools to support shared needs and (2) additional services and tools to support unique needs.

We do not intend for this pre-purchase policy to detract from our commitment to the MNU community. We will strive to meet both the common and different needs of our user groups. However, we do require that we be given opportunity for input before purchases are made.

Pre-Purchase Contacts. Please contact the Chief Technology Officer for pre-purchase consultation:
Dr. Marty Crossland, Chief Technology Officer (913-971-3514, mcrossland@mnu.edu)

Questions. If you have questions about this policy please contact one of the following:

- Dr. Marty Crossland, Associate VP for Technology, Chief Technology Officer, and Professor (913-971-3514, mcrossland@mnu.edu)
- Mr. Kevin Gilmore, VP for Finance and Chief Financial Officer (913-971-3273, kgilmore@mnu.edu)

1.2.5 Blocked Web Sites

In support of the mission of MNU may block access to web pages involving pornography, gambling, and/or other content found inconsistent with the mission and values of the University. The following procedures outline how appropriately-blocked web pages can be unblocked for academic purposes and how inappropriately-blocked pages can be unblocked.

Procedure to request access for academic purposes to blocked web pages

Occasionally and usually for a short time, access to appropriately-blocked sites is required for academic purposes. In that event, the person desiring access should follow this procedure.

- Secure the approval of a faculty member for unblocking the page.
- Ask that the department chair send to the Chief Technology Officer an email request to unblock the site(s). The request should include
- the URL for the site
- the time frame (likely for a specified period of time such as a week or a semester) during which it should be unblocked
- a rationale for this action

Procedure to request access to inappropriately-blocked pages

Occasionally, a web page will be inappropriately blocked by our commercial web filter. If you identify a page as being inappropriately blocked, please follow the following procedure. For their own protection, those who manage

this procedure will not look at pages to make judgments on whether the page should be blocked. They will respond to your request only if they are confident, based upon both your description and the URL, that the page is inappropriately blocked.

- Students and employees present the request to the help desk.
- Provide the URL and a description of the content and purpose of the site(s) to be unblocked.
- Approved requests will be directed to the appropriate the MNU technology team personnel to unblock the site(s).

Note on Procedure to request access to inappropriately-blocked pages: Anyone who requests a website to be unblocked and that website is subsequently found to involve inappropriate material will be referred to the appropriate university office for possible disciplinary purposes.

1.2.6 Personal Computer Connections On Campus

MidAmerica Nazarene University students and employees are welcome to bring personal computers for use on campus and in the classroom. However, since campus systems and settings may be different from settings used for connection to your home Internet Service Provider, compatibility with campus systems is not a certainty. The following lay out University information technology policy.

- The MNU technology team will not set up your personal computer for you for use on campus. The reason for this is that often the settings that are needed for you to connect to your home ISP could be inadvertently affected by changes made to accommodate the University's networks. Only you understand these settings and if we changed them, you could spend hours on the phone to your ISP trying to undo the changes. So if you make your own changes to your system, you are liable for those changes if problems should arise.
- The MNU technology team will provide you with written instructions on how to set up a typical system to connect to the campus network and in class projection systems. You may also request a TA or a Faculty Instructional Technology Consultant to walk you through and/or coach you on the proper set-up procedure.

1.2.7 Data Access

Introduction:

Institutional data is information that supports the mission and operation of MidAmerica Nazarene University. It is a vital asset and is owned by the University. It is likely that some institutional data will be distributed across multiple units of the University, as well as entities outside. Institutional data is considered essential, and the MNU technology team quality must be ensured to comply with legal, regulatory, and administrative requirements. Business Owners[1] will assess institutional risks and threats to the data for which they are responsible, and accordingly classify the MNU technology team relative sensitivity as Level I *(low sensitivity)*, Level II *(moderate sensitivity)*, or Level III *(high sensitivity).* Unless otherwise classified, institutional data is Level II. University personnel may not broaden access to institutional data without authorization from the Business Owner. This limitation applies to all means of copying, replicating, or otherwise propagating institutional data.

Data Classification

Authorization to access institutional data varies according to the MNU technology team sensitivity (the need for care or caution in handling). For each classification, several data handling requirements are defined to appropriately safeguard the information. It is important to understand that overall sensitivity of institutional data encompasses not only the MNU technology team confidentiality (need for secrecy), but also the need for integrity and availability. The need for integrity, or trustworthiness, of institutional data should be considered and aligned with institutional risk; that is, what is the impact on the institution should the data not be trustworthy? Finally, the need for availability relates to the impact on the institution's ability to function should the data not be available for some period of time. There are three classification levels of relative sensitivity which apply to institutional data:

Level I: Low Sensitivity:

Access to Level I institutional data may be granted to any requester, or it is published with no restrictions. Public data is not considered sensitive. The integrity of "Public" data should be protected, and the appropriate Business Owner must authorize replication or copying of the data in order to ensure it remains accurate over time. The impact on the institution should Level I data not be available is typically low, (inconvenient but not debilitating).

Examples of Level I “Public” data include published “white pages” directory information, maps, departmental websites, and academic course descriptions.

Level II: Moderate Sensitivity:

Access to Level II institutional data must be requested from, and authorized by, the Business Owner who is responsible for the data. Access to internal data may be authorized to groups of persons by their job classification or responsibilities (“role-based” access), and may also be limited by one’s employing unit or affiliation. Non-Public or Internal data is moderately sensitive in nature. Often, Level II data is used for making decisions, and therefore it is important this information remain timely and accurate. The risk for negative impact on the institution should this information not be available when needed is typically moderate. Examples of Level II “Non-Public/Internal” institutional data include project information, official university records such as financial reports, human resources information, some research data, unofficial student records, and budget information.

Level III: High Sensitivity:

Access to Level III institutional data must be controlled from creation to destruction, and will be granted only to those persons affiliated with the University who require such access in order to perform their job, or to those individuals permitted by law. Access to confidential/restricted data must be individually requested and then authorized by the Business Owner who is responsible for the data. Level III data is highly sensitive and may have personal privacy considerations, or may be restricted by federal or state law. In addition, the negative impact on the institution should this data be incorrect, improperly disclosed, or not available when needed is typically very high. Examples of Level III “Confidential/Restricted” data include official student grades and financial aid data; social security and credit card numbers; individuals’ health information, and human subjects research data that identifies an individual.

Policy Statement:

Institutional data must be protected from unauthorized modification, destruction, or disclosure. Permission to access institutional data will be granted to all eligible University employees for legitimate university purposes.

Authorization for access to Level II and Level III institutional data comes from the Business Owner, and is typically made in conjunction with an acknowledgement or authorization from the requestor’s department head, supervisor, or other authority.

Where access to Level II and Level III institutional data has been authorized, use of such data shall be limited to the purpose for which access to the data was granted.

University employees must report instances in which institutional data is at risk of unauthorized modification, disclosure, or destruction.

Business Owners must ensure that all decisions regarding the collection and use of institutional data are in compliance with the law and with University policy and procedure.

Business Owners must ensure that appropriate security practices, consistent with the data handling requirements in this policy, are used to protect institutional data.

Users will respect the confidentiality and privacy of individuals whose records they access, observe ethical restrictions that apply to the information they access, and abide by applicable laws and policies with respect to accessing, using, or disclosing information.

Data Handling Requirements:

Type of Data	LEVEL I *Low Sensitivity* *(Public Data)*	LEVEL II *Moderate Sensitivity* *(Non-Public/Internal Data)*	LEVEL III *High Sensitivity* *(Confidential/Restricted Data)*
Mailing & Labels on Printed Reports	None	May be sent via Campus Mail; No labels required	Must be sent via Confidential envelope; Reports must be marked "Confidential"
Electronic Access	No controls	Role-based authorization	Individually authorized, with a confidentiality agreement
Secondary Use	As authorized by Business Owner	As authorized by Business Owner	Prohibited
Physical Data/ Media Storage	No special controls	Access Controlled area	Access controlled and monitored area
External Data Sharing	No special controls	As allowed by Iowa Open Records Law, FERPA restrictions; or Non-UI project/study participants	As allowed by Federal regulations; Kansas Ope Records Law; FERPA restrictions; and Busines Associate Agreement (for PHI);
Electronic Communication	No special controls	Encryption recommended for external transmission	Encryption required for external transmissio
Data Tracking	None	None	Social Security Numbers, Credit Cards, and PHI locations must be registered
Data Disposal	No controls	Recycle reports; Wipe/erase media	Shred reports; DOD-Level Wipe or destructio of electronic media
Auditing	No controls	Logins	Logins, accesses and changes
Mobile Devices	Password protection recommended; Locked when not in use	Password protected; Locked when not in use	Password protected; Locked when not in use Encryption used for the Level III data

Control Definitions:

Mailing & Labels on Printed Reports – A requirement for the heading on a printed report to contain a label indicating that the information is confidential, and/or a cover page indicating the information is confidential is affixed to reports.

Electronic Access – How authorizations to information in each classification are granted.

Secondary Use – Indicates whether an authorized user of the information may repurpose the information for another reason or for a new application.

Physical Data/Media Storage – The protections required for storage of physical media that contains the information. This includes, but is not limited to workstations, servers, CD/DVD, tape, USB Flash drives, laptops, notebook computers, and PDAs.

External Data Sharing – Restrictions on appropriate sharing of the information outside of the MidAmerica Nazarene University.

Electronic Communication – Requirements for the protection of data as transmitted over telecommunications networks.

Data Tracking – Requirements to centrally report the location (storage and use) of information with particular privacy considerations.

Data Disposal - Requirements for the proper destruction or erasure of information when decommissioned (transfer or surplus).

Auditing – Requirements for recording and preserving information accesses and/or changes, and who makes them.

Mobile Devices – Requirements for the protection of information stored locally on mobile devices. This includes, but is not limited to laptops, tablet computers, PDA's, cell phones, and USB flash drives.

2 Student-Specific Policies

2.1 Compliance with the Higher Education Opportunity Act Peer-to-Peer File-Sharing Requirements

Legal use of Copyrighted Material and File Sharing at MidAmerica Nazarene University

The Department of Education has issued final regulations (Oct. 29, 2009) detailing the steps institutions are expected to take in order to comply with the requirements of H.R 4137, the August, 2008, reauthorization of the Higher Education Opportunity Act (HEOA). Information Technology Services (the MNU technology team) at MidAmerica Nazarene University has taken the following steps to comply with the HEOA regulations. The technological issues in HEOA all relate to concerns surrounding the illegal distribution of copyrighted materials. The four main requirements are listed below with a brief description of MNU's response to each.

1. Make an annual disclosure that informs students that the illegal distribution of copyrighted materials may subject students to criminal and civil penalties and that describes the steps that institutions will take to detect and punish illegal distribution of copyrighted materials.

MNU's response:

- Annually at the start of each new academic year a joint message to students will go out from the Dean of Students and Community Life and the Associate Vice President for Technology informing students about college policy related to the use of copyright-protected materials and the steps MNU will take to enforce the MNU technology team policies.
- In order to use college computing resources, all members of the MNU Community must endorse a Network-Use Policy that includes a section on copyright compliance.
- Each fall new students will attend a workshop during which copyright law and these requirements are discussed.
- Annually residence life staff members discuss formally and informally our policies regarding the distribution and use of copyrighted materials.

2. Institutions certify to the Secretary of Education that they have developed plans to “effectively combat” the unauthorized distribution of copyrighted material.

MNU's response:

- At the recommendation of the Technology Advisory Council, MNU the MNU technology team has implemented a system designed to block peer-to-peer traffic between the Internet and residence halls. While this system is not perfect, it effectively prevents most inappropriate uploading and downloading of copyright-protected materials in the halls.
- Violations of copyright law can lead to criminal charges and civil penalties. Under current copyright law, criminal cases of copyright violation carry a penalty of up to five (5) years in prison and a $250,000 fine. Civil penalties for copyright infringement include a minimum fine of $750 for each work. While criminal prosecution for illegal downloading is rare, civil law suits are quite common for some institutions.
- In addition, MNU takes the following steps when a user is alleged to be illegally file-sharing:
- Their computer(s) may be "black holed"; i.e., the computer(s) will be rendered unable to connect to MNU's network.
- They will be required to set up an appointment with a Student Life dean or other appropriate staff member.
- Upon satisfactory removal of offending materials from their computer(s) (assuming the accusation is accurate), students will be required to pay a $100 fee to reconnect to MNU's network. This fee will help defray the cost of connecting a personal computer to the network.

3. To the extent practicable, institutions offer alternatives to illegal file sharing.

MNU's response:

The MNU web site includes a link to the Educause page that maintains a current set of links listing legal alternatives for obtaining digital content such as movies, music, and games.

4. Institutions identify procedures for periodically reviewing the effectiveness of the plans to combat the unauthorized distribution of copyrighted materials.
MNU's response:
The institution will assess the overall effectiveness of the University's policy and procedures to promote the legal use of copyrighted materials based upon the volume of DMCA notices MNU receives. Any changes to the policy and/or procedures will take effect at the commencement of the following academic year.

2.2 Student Printing on University Printers

This policy was developed to allow students adequate printing resources for course needs while also to encourage good stewardship of both campus and natural resources.
From the technology fee a student pays, a certain amount (currently $25.00, and reviewed for possible modification annually) will be allocated toward a quota of printing on MNU's printers. Printing beyond this quota will require, in advance, a replenishment of the printing funds available in the student's account. The amount charged may be changed at any time without notice, but as of the adoption of this policy students will be charged $0.05 per page for black-and-white printing, and $0.25 per page for color printing (where available). The quota amount will be renewed, without rollover of any outstanding balance, three times per year in August, January, and May. Any remaining cash replenishment funds the student has deposited *will* be rolled over to the next period. Prior to printing each print request from a computer, the student normally will be presented with an electronic accounting of their current balance and of the charges they are about to incur with the current print request.

2.3 Student Account Deactivation

All students automatically receive a MNU network and computer account. This account controls access to e-mail, MNU Virtual Campus and online classrooms, student academic information, and potentially other resources controlled by the MNU authentication system.
Student accounts are maintained until the student is no longer enrolled at which point the accounts are deactivated (locked). They may be removed after a waiting period, with or without notice to the student. Students that have completed their course work, but need their account to remain active to complete additional requirements (e.g. graduate students working on a thesis) need to contact their program office for an extension.

3 Faculty and Staff Policies

3.1 Personal Responsibility

3.1.1 Intellectual Property

Introduction

New emphases on classroom research and online courses may allow a faculty member to simultaneously teach, carry out classroom research, and publish courses, course materials, data, scholarly papers and creative works to the Internet. New questions thus arise as boundaries of teaching, research, creativity, and publication are becoming much less defined. Even more relevant is the possibility of the movement of some faculty work from the traditional educational venues (e.g., campus classrooms, labs, theaters, studios, and mnu.edu) to the commercialization of educational materials.
MidAmerica Nazarene University encourages its administration, faculty, librarians, staff, and students to engage in scholarly activities that support and further the university's mission. Faculty members should aspire to break new ground in discovery, invention and application. The MNU faculty member's commitment extends to full

participation in the larger community of scholars, active involvement in learned societies, publication of scholarly books, essays and reviews, and the development and publication of online educational resources and courses. The school may support such scholarship with released time, equipment, clerical assistance and travel funds, as resources are available. While MNU does not have any vested interest in patents, faculty may develop patentable products and ideas out of this research, and while such patents remain the sole property of the individual involved, the ownership of educationally related materials is more complicated. The following policy governs this complex arena.

Definitions of terms

The following definitions concern creative works about which the question of copyright or patent ownership by the faculty and/or the institution may arise.

Creative works (for the purposes of this policy) are academic, artistic, or scholarly works, products or inventions of potential commercial value (thus involving issues of economic benefit and control), which are generated by faculty members. The production of these works may involve the use of ordinary or extraordinary institutional resources.

Ordinary resources: The general resources of time, salary, staff assistance, travel funds, internal grants, release time, equipment, etc., available to any faculty member.

Extraordinary resources: Allocations of resources, either qualitatively or quantitatively, beyond those available to most or all faculty members under normal circumstances.

Economic Benefit: Income, potential income, or other benefits that might accrue to an individual or an institution through the publication and/or marketing of a work. Examples of such works might range from traditional text-based publications to supplemental course materials, to entire online courses.

Control: The legal right to say what happens with and to a work. Issues of authorship and ownership are intertwined in control.

Categories

Creative works can be divided into the following categories:

- **Employee initiated works**

  These works, resulting from the faculty member's personal initiative, are a part of the way the faculty member, while fulfilling his or her contractual responsibilities, grows professionally as part of both the MNU community and the larger community of scholars and higher education professionals. Such works typically include scholarly publications, books, plays, poems, music compositions, works of art, textbooks, anthologies, and online scholarly, professional or educational materials and publications, and course-packs, supplemental instructional materials in any format, manuscripts, musical compositions, web pages, and computer software.

  There are two general categories of such works:

- Works supported by ordinary resources
- Works supported by extraordinary resources.
- **MNU (Employer) initiated works**

  Works resulting from the initiative of the institution that utilizes an individual's (e.g., Faculty, Staff, Administrator, or Student) expertise and time to produce materials and resources, and generally falling under one of the following categories:

- Works supported by ordinary resources: Examples might include a work commissioned by a college publication, a performance, and materials resulting from the normal teaching process, e.g. syllabi, study guides, course packs, supplemental instructional materials in any format, manuscripts, musical compositions, web pages, and computer software.
- Creative Works for hire: Works produced by an employee or independent contractor at MNU's request, which are fully funded and supported by MNU.

Policy Principles

- Faculty normally retain full copyright privileges, economic benefit, and control of work that is not initiated by the institution and that uses only those types and/or quantities of resources that are generally available to all faculty.
- The institution normally holds the copyright for materials that are deemed works for hire, are initiated by the institution, or that use types and/or quantities of resources not generally available to all faculty members. However, for each such work, control and any economic benefit MUST be individually negotiated in advance. Failure to negotiate such agreements in advance will result in a default 50:50 control and economic benefit split between the institution and faculty member if/when such benefits accrue.
- Works that are created due to the normal expectations stated by promotion/tenure policy shall not be considered as works for hire.
- In the event of use of types and/or quantities of resources beyond those generally available to all faculty, the extent of such use shall be considered in determining the level of equitable sharing of any revenues.

Policy Administration

Intellectual property rights issues and policies shall be administered by the office of the Provost.

3.1.2 Use of Video in Online Courses

In many ways, video is like any other element you use in a course. If you "distribute" materials to students in your class, then you need appropriate copyright permissions for such use. This is true for ANY copyrighted media you use in your course if you "distribute" the materials. Placing a document, video clip, or audio clip for use in your course, regardless of the source could be considered distribution.
There are exceptions when an institution purchases a blanket license for materials like MNU has done with full text articles found in our Library databases or for eBooks, or for licensed media delivery. These are essentially use-with-permission as the permissions are "pre-purchased" by the institution. Therefore, links to an eBook, to a library database article using the persistent URL, or to a licensed video are permissible.
We have developed a media process for currently-owned library media to ensure legal use of multimedia as online components of both online and face-to-face courses. This process is subject to change over time as law, interpretations of law, and demands of the educational process change. We are also requesting that the University provide funds for legal licensing of copyrighted multimedia (movies or educational video) as online components of courses to enhance a deeper learning experience.

Process:

- Submit a Copyrighted Media Request Form. You must supply a budget number and have approval from your budget manager for up to $350, before we will proceed with the next step.
- Upon receipt of your form we will initiate a permissions query to the publisher/vendor. This may take two weeks or even longer as not all vendors respond right away. If we already have permissions for the item requested, then we will add a link to your Blackboard course or explain the process for your learners to gain access to the media.
- Once a vendor responds about permissions, we will contact you to let you know the cost if it exceeds $350. If less than $350 we will proceed and will bill the account number you have provided. We are hoping to have access to a budget line to cover permissions, however if the University does not provide funding, we will ask you for a budget number prior to purchasing the permissions for the use of the media in a course.
- Once we have permissions then we will link the media to your course. Clips may be permissible for use for classes without permissions under fair use guidelines (up to 20% of the full work). We still need the submission of the Copyrighted Media Request Form and in addition need the timeline (from:/to:) of the clip and an explanation of start and stop points helps as well. We do NOT recommend that instructors try to upload clips directly to the learning management system, as these should be streamed (no download allowed) from a media server.

References about video copyright

Kolowhich, S. 2010 "Hitting Pause on Class Videos". Inside Higher Ed Newsletter. Available online: A trade group goes after UCLA for posting copyrighted videos on course Websites -- and hints that other colleges might be next. (January 26, 2010)
Xavier University Copyright Video
Crews, K. D. 2003. Crews, K. D. 2003. Copyright and distance education: Making sense of the TEACH act. Change 35 (6):34-39.
Shaw, M. H., and B. B. Shaw. 2003. Copyright in the age of photocopies, word processors, and the Internet. Change 35 (6):20-27.

3.1.3 Damaged or Lost Computers

In the event of either theft or accidental damage to the computer (dropping, spilling liquids, etc.) provided by the institution to the faculty member, the faculty member's department will be responsible for the cost of repair/replacement of the system.
The cost of repairing/replacing system components that fail under normal wear and tear normally will continue to be covered fully by the MNU technology team under warranties and/or maintenance agreements.

3.2 Technology Access and Usage

3.2.1 Purchases of Hardware and Software

Requests for new software or hardware by faculty and staff in an Academic Department will be addressed in the following manner.

- Departments should anticipate future software and hardware needs and submit them as part of a coordinated Departmental Technology Request in the spring of each academic year, no later than May 1 unless otherwise announced or arranged with the Provost or Chief Financial Officer. In this manner, normal software and hardware needs are approved for the requesting department as a whole.
- Needs may arise at other times of the year for other software and hardware. In such cases the requests will be evaluated via the following criteria:
- Is other software or hardware already available to the department capable of meeting the need until the next annual Departmental Technology Request (e.g., Excel for personal database or grading, scanner or software already available and accessible in in another office or on the server)?
- Is the need for software departmentally based and supported, or is this an individual request? Is the intended use:
- Instructional?
- Research?
- Personal productivity?
- What is the cost of the software/hardware related to the anticipated use and benefits -- is the cost justifiable?
- If the software or hardware request appears to be a valid need for the current academic year, based upon the answers to the three criteria above, and the department chair approves the purchase of the hardware or the software for installation on a department member's computer, and the purchase is approved by either the Provost or the Chief Financial Officer, then the MNU Technology team will assist in acquisition of the item(s), to be charged to a budget account supplied by the requesting department.
- In ALL cases of acquiring any technology using any University funds, no matter which budget is being charged, including funding from external grants, the MNU technology team MUST oversee the purchase and ordering process, and will install the software or set up the hardware as needed.

3.2.2 University-owned personal computers

Overview

This section outlines MNU's policy for acquisition and funding of University-owned personal computers. This includes desktop computers, laptop/notebook computers, and tablet devices.

- Computer platforms.
- It is recognized that individuals may have strong preferences for a particular computer technology platform, such as Microsoft Windows or Apple Mac. In the University environment, such preferences must be balanced against the resources available for both acquiring the technology and for supporting it in the future.
- In most cases, employees need only basic communication capabilities (e.g., email, instant messaging, Internet browsing) and abilities to create, edit, save, and share documents of various kinds (e.g. word processing, spreadsheets, presentations, etc. – "Microsoft Office" is currently the designated platform for University use). For the choice of technology to provide such basic capabilities, the personal preferences of employees normally will not be part of the decision.
- When acquiring new computers for employees, either for new positions or for replacements, the University will use the following criteria for selecting the computer platform to be purchased from any University funds, including grants:

1. Lower initial purchase cost, for the computer and all required peripherals , including a maintenance agreement (see #2 below), that meet the minimum requirements for the intended use
2. Availability of a manufacturer-certified multi-year maintenance agreement that includes onsite repair (preferred) or a fast depot exchange service
3. Availability of University helpdesk resources to properly support the technology

- Tablet computers and other consumer devices
- Tablet computers and other personal devices, including "iPads," are considered consumer devices in the category of "Bring-Your- Own-Device" (BYOD). The computer industry is still evolving for defining the proper role of such devices in an enterprise environment such as the University.
- The University is still evolving its own environment for being able to accommodate, but not yet support, such devices. Therefore, such devices, even when purchased with University funds, will be considered personal devices from a practical support standpoint. As such, they are not eligible for direct support (e.g., specific configuration, troubleshooting, or repairs). The MNU Technology Team can only provide basic guidance in how to connect to available networks and basic configuration coaching.

3.2.3 Classroom Software Installation Requests

Summary:

This Policy deals with installation of non-standard (image) software on Instructor Workstations and Student Workstations in MidAmerica Nazarene University Classrooms.

Policy:

- Software Installations take time, and significantly so for multiple-station areas such as labs. Therefore, a minimum of THIRTY DAYS advance notification is requested before your first-time use in the classroom.
- Software Installations require properly licensed and validated software. If a software license must be ordered prior to installation, please allow an additional two weeks. Multiple versions will not be installed UNLESS evidence of open source status or appropriately licensed status is provided.
- The inventory tag number of the computer(s) and classroom location must be provided. Classroom Software Installation Requests (single installations) should be submitted via the Classroom Software Installation Request Form.
- Information Technology Services will leave the software on the classroom computer only for the period indicated in the request. If software is needed on an ongoing basis and is open source or we have a site license, then it should be submitted for testing and installation as part of the standard Classroom Computer setup.

3.2.4 Storing and Accessing non-ERP (Banner) Data Outside of the MNU Servers

In some cases an employee or department may perceive a need to organize and store information outside the University's database system (currently Banner) for justifiable University purposes. Any and all such proposed solutions must be reviewed and approved by the MNU Technology team prior to committing any University resources to the project. Requests will be handled according to the following guidelines:
First, the request will be evaluated by the Chief Technology Officer to determine if the identified data belongs in MNU's ERP (Banner) system:

- Does the data have significance for more than one MNU department or office?
- Is this long or short-term data storage?
- Is the information confidential, and if so, what security measures will be observed?
- Does the needed information already exist in the system?

The Information Services team will respond to the request based on these criteria. If approved, continue to the next steps.
The MNU technology team will offer solutions for departments/offices to follow depending upon their needs. In any resulting scenario, the MNU technology team will order/arrange for and install any required hardware, operating system, web server application if needed, and database application. The non-the MNU technology team department will be responsible for all costs related to design, develop, and maintain the application software. That department will also be responsible for all other monetary costs of the project.
Database solutions that employ personal database products such as Access and Filemaker are strongly discouraged. The MNU technology team experience with such personal products confirms that they are not designed to function in multi-user environments. They are neither robust enough nor have adequate security provisions to support the expansion of applications that departments/offices inevitably desire to create. This lack of flexibility leads to frustration and the inability to support expanded goals, resulting in loss of time and other resources. Thus, the MNU technology team in most cases will not support such solutions.
The MNU technology team will develop the protocols for making data from our ERP and/or the departmental/office database available. Data access may be made available to persons in the department/office or to appropriate constituents outside the department/office.
The MNU technology team and the department are jointly responsible for reviewing the security design of the departmental database and application, to ensure that institutional data is appropriately protected.
The MNU technology team will provide consultation to the departments for this process. This service will help define the project, define the structure of the database, and in the use of the database tools.

3.2.5 Loan of Notebook Computers to Faculty and Staff

Loan of notebook computers is a service facilitated through the MNU Mabee Library. The MNU technology team provides notebook computers to the library to check out for general use to the members of the university according to policies developed by the MNU technology team and the library. An MNU ID card is necessary to check out equipment.
On occasion notebook computers may be requested for groups or individuals who require more support than the MNU technology team and library together can supply. The MNU technology team will evaluate the situation to identify an appropriate solution. When these exceptional cases arise, the faculty or staff requiring the equipment should call the service desk. These requests will be directed to the Chief Technology Officer.
The administration of this service is governed by the following guidelines:

- Reservations should be made at two weeks in advance.
- Loans are subject to inventory on-hand
- Requests beyond the normal checkout (e.g., overnight or extended times when employee is traveling) will require a written request by the employee's department head or dean, and approval by the Chief Technology Officer. Granting of any such request may be limited by other existing, approved requests for the inventory on-hand.

- Only full-time faculty members are eligible to check out University-owned computers. Adjunct faculty may not take possession of university computer equipment or use university computer equipment outside the normal on-campus classroom and/or office environment.
  In the event of failure of, damage to, or loss of the equipment:
- The MNU technology team normally will pay the cost associated with any normal component failure.
- In the event of either theft or accidental damage: such as dropping the computer, spilling liquids into the computer or other accident to the computer provided by the university to the faculty member, the faculty member's department will be responsible for the cost of repair or replacement of the computer.

Loan of Computers to Faculty on Sabbatical

For their sabbatical activity, MNU faculty members may be authorized to take their notebook computers with them.

However, those with desktop systems may also authorized to take them away from their offices to a different location within the continental United States. This policy is authorized to facilitate the accomplishment of sabbatical projects. However, since the movement of desktop computers usually entails risk to the safety and integrity of the system, the faculty member assumes the following responsibilities:

- The faculty member must complete an applicable form and submit it to the Chief Technology Officer.
- The faculty member will be responsible for any accidental damage, loss, or theft of the system. Information Technology Services will continue to assume responsibility for any component failures caused by normal wear and tear. Any repairs of the system will be done by the MNU technology team on campus.
- The computer will need to be carried or shipped to the campus for repairs. If shipping is required, please make arrangements with the MNU technology team before actually sending the system.
- Provision and maintenance/repair of any additional components (such as a software application) that are not part of a normal office configuration will be the responsibility of the faculty member. However, prior to taking the system off-campus, approval for any addition must be secured from the Chief Technology Officer, in order to maintain system compatibility.

3.2.6 Electronic Resource Access for Retirees

MNU recognizes the valued service retirees (e.g. emeritus professors) have given the university. Therefore, in order to enable them to enjoy appropriate electronic services and to stay in contact with the university, and to be able to facilitate ongoing communication with them, MNU may provide retirees continued off-campus access to the following resources via their MNU accounts.

- Library access, which includes reference service and searching the online catalog. For contractual reasons, proprietary databases will be available only on-campus. When on campus, retirees are welcome to visit the library to access resources available to all library guests.
- Email account.

---

[1] The senior official within a School or departmental unit (or his/her designee) accountable for managing information assets