POLICY MANUAL

INFORMATION TECHNOLOGY

Revision Date: May 25, 2007

Table of Contents

1.1 Authorized Use of Technology Systems

1.1.1 Technology Use Policy

The University is committed to excellence in teaching. In an effort to support the University community in these endeavors, the institution has assembled a wide variety of technology resources for general use. These resources are for use by persons with a current, active affiliation with the University, including but not limited to students, faculty and staff.

The technology resources that are owned by the University are to be used for University-related activities for which they have been assigned. University technologies are not to be used for commercial purposes or non-University-related activities

Access to technology resources at the University is a privilege and must be treated as such by all users. Like any other campus resources, abuse of these privileges can be a cause for campus disciplinary procedures and/or legal action. Furthermore, the University reserves the right to extend, limit, or restrict technology privileges and access to information resources.

The University has the right and responsibility to provide the University community with information technology resources and services. While providing these services is of primary importance, there are other areas of importance aside from physical resources. The following is a general description of the responsibilities, the rights and obligations of the University.

1.1.2 Electronic communications: Email, Voicemail, and Campus News Utilization

1.1.2.1 The use of email as an official means of communication within the University community

A. **Purpose of this Policy**

There is an expanding reliance on electronic communication among students, faculty, and staff at Dominican University motivated by the convenience, speed, cost-effectiveness, and environmental advantages of using email rather than printed communication. Because of this increasing reliance and acceptance of electronic communication, email will from this point forward, be considered an official means for communication within the university.

B. **Scope**

This email policy is not inclusive of all aspects of email, rather it provides guidelines regarding email as an official means of communication including:

- University use of email;
- Assignment of email addresses;
- Use of and responsibilities associated with assigned email addresses; and
- Expectations of email communication between faculty and student and staff and student.

C. **Policy**

1. University use of email

   E-mail is an official means for communication within Dominican University. Therefore, the University has the right to send communications to students, staff, and faculty via email and the right to

2. Assignment of email addresses
   The Department of Information Technology will assign everyone an official University email address. It is to this official address that the University will send email communications. This official address will be the address listed in the University's Global Address List found in the Exchange/Outlook Address Directory and will be the official email address included with personal information within the administrative computing system.
3. Redirecting of email
   It is permissible to have email electronically redirected to another email address. However, those persons who use email redirection from their official address to another email address (e.g., @aol.com, @hotmail.com) do so at their own risk. The University will not be responsible for the handling of email by outside vendors. It is up to the individual to take whatever steps may be necessary with their personal email account to allow for the receiving of email forwarded from their dom.edu email account. These steps may include, but are not necessarily limited to adding the dom.edu address to a 'safe-senders' list and/or adjustment of any spam filters. Having email redirected does not absolve anyone of the responsibilities associated with communication sent to his or her official email address.
4. Expectations regarding student use of email
   Staff, faculty and students are expected to check their official email address on a frequent and consistent basis in order to stay current with University communications. For students and faculty we recommend checking email at least as often as your most frequent class meets in a week, in recognition that certain communications may be time-critical. Staff should check their email regularly during the normal work day.
5. Educational uses of email
   Faculty may determine how email will be used in their classes. It is highly recommended that if faculty have email requirements and expectations they specify these requirements in their course syllabus. Faculty may expect that students' official email addresses are being accessed and faculty may use email for their courses accordingly.
6. Appropriate use of email
   In general, email is not appropriate for transmitting sensitive or

confidential information unless an appropriate level of security matches its use for such purposes.

- Confidentiality regarding student records is protected under the Family Educational Rights and Privacy Act of 1974 (FERPA). All use of email, including use for sensitive or confidential information, will be consistent with FERPA.
- E-mail shall not be the sole method for notification of any legal action.

A. **Procedures**
The Director of Information Technology will review this policy as needed. The President's Cabinet, as appropriate, will authorize changes. Students, staff, and faculty with questions or comments about this policy should contact the Director of Information Technology.

B. **Responsible Organization**
The Director of Information Technology will be responsible for this policy.

1.1.2.2 The use of email messages to transmit University-related information

The use of email messages to transmit university related information will be used for targeted mailing only. Information to be sent to the entire university community should be posted on the Campus news Web page. Information geared toward specific groups should be sent by individuals.

A. Use of any emails distributed to the university system must deal with university information or university sponsored events only. Emails for non-university purposes are not permitted.
B. Individual emails regarding general information to the entire university community are not permitted. The includes emails to all students, faculty, and staff (what was formerly done through Network Broadcast).
C. Individual emails may be sent from the President or designee regarding a university situation or emergency.
D. Certain departments and individuals, upon completion of training regarding proper use, will have the ability to send email to the main distribution lists for faculty, staff and students, individually or collectively. These privileges will be revoked if inappropriately used.
E. Any email sent to a group within the community must have a deletion date set for immediately after the event in question or within two weeks of distribution.

F. Emails for events are for information only and a maximum of one electronic communication per event can be sent.

1.1.2.3 Voicemail Utilization

The number of campus messages distributed through the university voicemail system has grown considerably with multiple messages being left on a daily basis. With so many messages, they become transparent as the recipients often delete the message before it has been heard. This new voicemail policy addresses this issue with the intent of streamlining the use of voicemail to address the distribution of urgent information to the university community.

1. Voicemail will be used only to inform the faculty, staff and students about critical news such as a campus closing, a special message from the president and other information approved by a cabinet member.

2. All voicemail requests must be sent from an approved representative to extension 6990 for the main campus and 9127 for the Priory campus, with a notification given to Telephone Services at x.6750.

1.1.2.4 Campus News Web Site

In an effort to facilitate timely communication, a new Campus News Web page has been developed which will be used as the primary communication tool for university events and activities. This Web page will include daily or upcoming news/activities on campus as well as serve as a portal like page for online services and campus events. This portal replaces the Network Broadcast email system as most of the items currently being sent from Network Broadcast would instead be posted on the Campus News Web page.

1. Campus News Web page is for passing university-related information to the entire university community. The postings are considered to be informational messages as opposed to official electronic email correspondence.

2. Any faculty, staff or approved student group can submit items to be posted on the Campus News Web page. Postings are restricted to activities on campus or DU sponsored events. Information should be submitted to the page at http://www.dom.edu/campusnews .

3. Information geared toward a specific group and not the entire university community will be disseminated through the specific audience link on the Campus News Web page.

4. The Campus News Web page will be set as the default page on all university owned computers.

1.1.3 Technology Initiative for Faculty

Approved by Academic IT Committee
May 2, 2007

The Academic IT Governance Committee would like to explore the idea of starting a program to provide new faculty with new equipment, as well as a program for current faculty to request replacement equipment.

Since the program intends to help faculty use technology to enhance learning, we propose that the equipment replacement cycle should include desktop computers and laptops. The faculty would have a choice as to what equipment meets their needs the best. Considering the budget and the ability of IT to successfully deploy the units, 40 offerings can be made each year. Of those 40, no more than 30 can be laptops. There will be a standard equipment offering. Anything other than the standard, including an upgrade request other than a full system, must be justified in writing by the faculty member. The Director of IT has the ultimate budget approval.

1. **Eligibility**
   Full-time faculty; priority set by the deans.

2. **When will faculty receive the equipment?**
   New faculty, upon hire, will choose from the standard offering sheet.

   Current faculty can start requests now, with the first round of distribution after July 1, 2007.

   An equipment sign off sheet with the details of what is delivered will be signed by the faculty member and IT. This document will be filed with the Provost's office.

3. **Standard offering**
   a. Desktop – Dell Desktop with 17" flat panel monitor, keyboard, & mouse.

   OptiPlex 745 Desktop
   Intel® Core™ 2 Duo Processor E6300 (1.86GHz, 2 GB Ram, 250GB Hard drive)

   b. Laptop – Dell Laptop with NO peripherals (external monitor, keyboard, mouse) except for an additional power supply, one to leave in the office and one in the bag.
      - peripherals can be added at cost to the department

   Latitude D420 Laptop (lighter for travel)
   Intel® Core™ Duo Processor ULV U2500 (1.2GHz, 1 GB Ram, 60 GB Hard drive)

12.1 inch Wide Screen WXGA LCD Panel

Latitude D820 Laptop (bigger screen, but heavier)
Intel® Core™ Duo Processor ULV U2500 (1.67GHz, 1 GB Ram, 60 GB Hard drive)
15.4 inch Wide Screen WXGA LCD Panel

c. Software – deployed with the standard image. Faculty can install their own software. However, if at any time there is a conflict or the machine must be serviced, it will be set back to the standard image.

4. **Security issues**
   a. Theft and liability – a locking kit will be provide that enables securing the laptop to a heavy object (such as a desk). Provided that faculty take due care, they will not be held responsible for loss or theft of the laptop.

   b. Data storage – Network storage provides several benefits. First, files will be backed up on a daily basis. Second, those files are accessible from any computer connected to the Internet. Finally, storing sensitive and personal data, especially student data, on any computer or removable device that could be lost or stolen is a serious security risk. Using network storage for that data eliminates that risk.

5. **Training**
   a. Mandatory workshops for participants choosing the laptop option, in which the unit will be delivered.

   b. Training will also be provided for using the laptop with a projector.

   c. All faculty will be provided written instructions and personal consultation on file management and utilizing network storage.

6. **Support and Maintenance**
   a. Dell has 24x7 telephone support for hardware and operating system problems. During normal business hours we suggest you first call the IT HelpDesk for assistance. 708-524-6888

   b. IT will stock a pool of laptops that will be available for checkout.

7. **Viruses and spyware**
   Laptop users will need to regularly plug into the network on campus to receive updates to the anti-virus software and operating system. This is essential to keeping the machine safe from viruses and spyware.

8. **What happens if the faculty member leaves the university?**

The Provost office will have the inventory sheet that was signed by the faculty member. The final paycheck will be held until the equipment is returned to IT.

9. **Will a new printer be assigned also?**
   Only if the current printer that is being used is not functioning.

1.1.4 Moral and Ethical Standards

Along with the privilege of using the University's technology resources come responsibilities on the part of the user.

It is expected that all users of all University technology resources be guided by the ethics, morals, and Catholic values and standards of this institution. Every user must respect the rights and dignity of others by using the technology resources responsibly and in accordance with the highest ethical and moral standards. Therefore, certain behavior not consistent with the ethics, morals and values of this institution and/or any reasonable person will not be tolerated. Following are some, but not all uses considered unacceptable:

- Harassment that would cause distress, embarrassment, discomfort of intimidation based on race, national origin, disability, religious belief, gender or other types of intimidation.
- Offensive, tasteless, sexually explicit materials and images.
- Using the institution's resources as a conduit to attempt unauthorized access to on-campus or off-campus resources.
- Vulgar, abusive or offensive language.
- Violation of copyright laws by using, copying, distributing or storing copyrighted programs and materials without compensation to author/owner.
- Academic dishonesty, including but not limited to plagiarism (copying of the work of others in violation of authorial integrity).
- Behaving in any way that demonstrates a lack of respect for the rights and privacy of others.

If anyone is witness to or the victim of any of the above abuses, it is that person's responsibility to report the situation to the Director of Information Technology, who may handle the individual situation to a satisfactory conclusion, or refer the action for disciplinary action to appropriate administrators or governing bodies.

1.1.5 Precautions Relative to the Misuse of Technology Resources

It is imperative that all users of the University's technology resources be aware of the risks and dangers that can occur from using these resources for non-academic, non-research purposes. We strongly discourage users from using the technology resources for purposes of establishing personal contact with individuals previously unknown to the

user. The possibility of the user being put in danger of physical harm, or another type of compromising position, cannot be overstated. Therefore, users are strongly urged not to use technology resources for purposes of pursuing personal relationships.

1.1.6 Individual Responsibilities

Since certain privileges are given to each member of the University community, individuals are held accountable for their actions as a condition of continued membership in this community.

1.1.6.1 Common Courtesy and Respect for Rights of Others

Each person is responsible to all other members of the University community in many ways, including to respect and value the rights of privacy for all, to recognize and respect the diversity of the population and opinion in the community, to behave ethically, and to comply with all legal restrictions regarding the use of information that is the property of others.

1.1.6.2 Privacy of Information

Files of personal information, including programs, regardless of the medium on which they are stored or transmitted, may be subject to the Illinois Open Records Act if stored on the University's computer system. That fact notwithstanding, no one should look at, copy, alter or destroy anyone else's personal files without explicit permission (unless authorized or required to do so by law or regulations). The ability to access a file or other information does not imply permission to do so. Similarly, no one should connect to a host on the network without advance permission in some form. People and organizations link computers to the network for various reasons, and many consider unwelcome connections to be attempts to invade their privacy or compromise their security.

1.1.6.3 Intellectual Property

Each person is responsible for recognizing (attributing) and honoring the intellectual property rights of others. Violation of this is plagiarism.

1.1.6.4 Harassment

No member of the community may, under any circumstances, use technology to libel, slander, or harass any other person.

Examples of computer harassment:

- Using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm.
- Using the computer to contact another person to harass, or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease.
- Using the computer to contact another person repeatedly regarding a matter for which one does not have legal right to communicate, once the recipient has provided reasonable notice that the recipient desires such communication to cease (such as debt collection).
- Using the computer to disrupt or damage the academic, research, administrative, or related pursuits of another.
- Using the computer to invade the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another.

1.1.6.5 Game Playing and Other Personal Use of Institutional Resources

Institutional computing and network services are not to be used for extensive or competitive recreational game playing. Recreational game players occupying a seat in a university computing facility must give up their seat(s) when others who need to use the facility for academic or research purposes are waiting. Game playing, or other personal use of institutional technology resources, that interferes with the operation of the University's technology resources will not be tolerated.

1.1.6.6 Informational Integrity

It is the user's responsibility to be aware of the potential for and possible effects of manipulating information, especially in electronic form, to understand the changeable nature of electronically stored information, and to verify the integrity and completeness of information that is compiled or used. The user should not assume that information or communications are correct when it appears contrary to expectations; it should be verified with the person who originated the message or data.

1.1.6.7 Sharing of Access

Computer accounts, passwords, and other types of authorization are assigned to individual users and must not be shared with others. Each individual is responsible for the use of one's own account, password or authorization codes.

1.1.7 Institution Responsibilities and Limitations

The University provides technology to be used in the course of the educational process. Listed below are some of the responsibilities and limitations with regard to the use of technology.

1.1.7.1 Services

The University has the responsibility to provide, within the overall resource capability of the institution, necessary services to the user, for university-owned resources, through the Information Technology Department. These services include, but are not limited to, access to, assistance with, and maintenance of university-owned technology resources. Problems, questions, and comments on technology resources should be directed to the Information Technology Department.

1.1.7.2 Allocation of Resources

The University has the right and responsibility to allocate its resources in a manner consistent with the achievement of its overall mission.

1.1.7.3 Anti-harassment Procedures

The University has the responsibility to develop, implement, maintain, and enforce the appropriate procedures to prevent harassment through the use of its technology resources, and to impose appropriate penalties when such harassment takes place.

1.1.7.4 System Administration Access

The Director of Information Technology, or his/her designated system administrator(s), may access other's files for the maintenance of the networks, computer and storage systems, such as to create backup copies. In all cases, all individuals' privileges and right to privacy will be preserved to the greatest extent possible in the process.

1.1.7.5 Monitoring of Usage, Inspection of Files

The University may routinely monitor and log usage data such as network session connection times and end-points, computer and disk utilization for each user, security audit trails, network/internet loading, etc. The institution has the right to review data for evidence of violation of law or policy, and other purposes.

1.1.7.6 Imposition of Sanctions

The University may impose sanctions and discipline any person who violates the policies of the University regarding the usage of technology resources. When necessary, the institution has the right to monitor all the activities and inspect the files of specific users on their computers and networks. Any person who believes such monitoring or inspecting is necessary must obtain the authorization of the Director of Information Technology. In all cases, all individuals' privileges and right to privacy will be preserved to the greatest extent possible.

1.1.7.7 Control of Access to Information

The University may control access to its information and the devices on which it is stored, manipulated and transmitted in accordance with state, federal and international law, as well as its own standards and policies.

1.1.7.8 Security

The University has the responsibility to develop, implement, maintain and enforce appropriate security procedures to insure the integrity of individual and institutional information, however stored, and to impose appropriate penalties when privacy is purposefully violated.

1.1.7.9 Suspension of Individual Privileges

The University has the right to suspend access to technology resources for reasons relating to the safety and well being of the campus community or University property. Access will be promptly restored when safety and well being can be assured, unless access is to remain suspended as a result of formal disciplinary action, through appropriate formal process and procedures.

1.1.7.10 Upholding of Copyrights and License Provisions

The University has the responsibility to uphold all copyrights and licensing of technology resources. The University must also follow all laws governing access and use of information, and rules of organizations supplying resources to members of the community.

1.1.7.11 Data Availability

The University will take reasonable precautions to guard against corruption of data or software or damage of data stored on the University resources. The University will take backups on a regular basis of all data residing on servers regulated. In the best interest of

the user it is strongly recommended that the user of critical data should make backups. Under no circumstances does the University assume liability for the loss of information.

1.1.8 University Technology Resources – Examples of Inappropriate Use

All users of the University's technology resources must remember that access is a privilege and that the individual is responsible for their own action(s). The user must adhere to the following guidelines and act in an effective, ethical, moral, and lawful manner. Failure to adhere to these guidelines can lead to an immediate suspension of privileges.

1.1.8.1 Infractions

Listed below are examples of infractions against the University Technology Use Policy. This is not meant to be a comprehensive list but rather a sampling of possible infractions. Common sense and good judgment should always apply to the use of technology.

- Attempt to annoy or inconvenience any user of the system, individual or general:

  Examples:

  - Purposely consuming large enough shares of system resources to affect other users
  - Destructive control codes in files, in file names, or anywhere other users could be affected (virus)
  - Sending control codes to clear another user's screen, lock the keyboard, etc.
  - Stuffing another user's mail file
  - Sending fake "systems messages"
  - Sending obscene mail
- Any unauthorized attempt (hacking) to gain access to any on-campus or worldwide system.
- Posting or mailing obscene or inappropriate material
- Attempting to subvert security systems to gain access to other accounts

  Examples*:*

  - Creating fake login sequences which record the passwords other users enter
  - Having a fake login which gathers the passwords of those attempting to change their own password
- Attempting to circumvent restrictions or resource limits established by Information Services
- Purposely rendering the systems unusable to a significant number of users

  Examples:

  - "Crashing" the system
  - Removing or altering files which are necessary for the proper functioning of generally used programs
- Removing, altering, or reading information belonging to another user of the system without the user's permission
- Logging on as a user other than yourself, and/or falsely representing yourself to be that user in communication to others
- Allowing another user to use your login if that user's own login is removed for disciplinary reasons
- Violating the legal rights of others
- Logging on as a user, other than yourself, if that login name is disabled for disciplinary reasons
- Committing any violation referred to in the Moral and Ethical Standards section of this policy