BELMONT
COLLEGE

INFORMATION TECHNOLOGY APPROPRIATE USE

POLICY 1000.0100.12
Section 10, Information Systems
Responsible College Officer:
Executive Director of Information Systems/CIO
Originally Issued: April 24, 2008
Original Policy: 1000.0100.08
Revised: February 23, 2012

Initiated by:	Matthew Tarbett, Executive Director of Information Systems/CIO	
Reviewed by:	Belinda Porter, Administrative Affairs & Policy Coordinator	
Approved by:	Dr. Joseph E. Bukowski, President	

PURPOSE

To ensure an information technology infrastructure that promotes the basic missions of the College in teaching, learning, and administration. In particular, this policy aims to promote the following goals:

- To ensure the integrity, reliability, availability, and superior performance of IT Systems;
- To ensure that use of IT Systems is consistent with the principles and values that govern use of other College facilities and services;
- To ensure that IT Systems are used for their intended purposes; and
- To establish processes for addressing policy violations.

POLICY STATEMENT

This Appropriate Use Policy provides guidelines for the use of Belmont College's IT resources as well as for the College's access to information and oversight of these resources.

PERSONS AFFECTED

All users of Belmont College's IT Systems.

DEFINITIONS

Incidental Personal Use: Occasional personal use which:

- does not interfere with the College's ability to perform its mission;
- does not interfere with work being performed by another employee or student;
- is not for pay or profit;
- does not consume excessive supplies or system resources.

IT Systems: Computers, terminals, printers, networks, online and offline storage media and related equipment, software, and data files that are owned, managed, or maintained by Belmont College. For example, IT Systems include institutional information systems, desktop computers, and the College's campus network.

Systems Authority: The Executive Director of Information Systems/CIO delegates oversight of all systems. Belmont College retains its right as legal owner or operator of all IT Systems

Systems Administrator: A person assigned to manage a particular system.

User: Any person, whether authorized or not, who makes any use of any IT System from any location.

PROCEDURES

Appropriate Use

IT Systems may be used only for their authorized purposes — that is, to support the educational and administrative functions of Belmont College. The particular purposes of any IT System as well as the nature and scope of authorized, incidental personal use may vary according to the duties and responsibilities of the user.

Proper Authorization

Users are entitled to access only those elements of IT Systems that are consistent with their authorization and function in the College. Any attempt or effort to circumvent security measures is unlawful and a violation of appropriate use.

Proscriptions on Use

Specific Proscriptions on Use. The following categories of use are inappropriate and prohibited:

Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others. Users must not deny or interfere with or attempt to deny or interfere with service to other users in any way, by "resource hogging," misusing mailing lists, propagating "chain letters" or virus hoaxes, "spamming" (spreading email or postings widely and without good purpose), or "bombing" (flooding an individual, group, or system with numerous or large email messages). Knowing or reckless distribution of unwanted mail or other unwanted messages is prohibited. Other behavior that may cause excessive network traffic or computing load is also prohibited.

1. **Use that is inconsistent with Belmont College's non-profit status**. The College is a non-profit, tax-exempt organization and, as such, is subject to specific federal, state, and local laws regarding sources of income, political activities, use of property, and similar matters. As a result, commercial use of IT Systems for non-Belmont College purposes is prohibited. Prohibited commercial use does not include communications and exchange of data that furthers the College's educational and administrative roles, regardless of whether it has an incidental financial or other benefit to an external organization.

   Use of IT Systems in a way that suggests College endorsement of any political candidate or ballot initiative is also prohibited. Users must refrain from using IT Systems for the purpose of lobbying that connotes College involvement, except for authorized lobbying through or in consultation with the Ohio Attorney General's Office.

2. **Harassing or threatening use**. This category includes, for example, display of offensive, sexual material in the workplace and/or repeated unwelcome contacts with another.

3. **Use damaging the integrity of College or other IT Systems**. This category includes, but is not limited to, the following six activities:

   a. **Attempts to defeat system security**. Users must not defeat or attempt to defeat any IT System's security—for example, by "cracking" or guessing and applying the identification or password of another user. (This provision does not prohibit, however, Systems Administrators from using security scan programs within the scope of their systems authority.)

   b. **Unauthorized access or use.** The College recognizes the importance of preserving the privacy of users and data stored in IT systems. Users must honor this principle by neither seeking to obtain unauthorized access to IT Systems, nor permitting or assisting any others in doing the same. Users are prohibited from accessing or attempting to access data on IT Systems that they are not authorized to access. Furthermore, users must not make or attempt to make any deliberate, unauthorized changes to data on an IT System. Users must not intercept or attempt to intercept or access data communications not intended for that user, for example, by "promiscuous" network monitoring, running network sniffers, or otherwise tapping phone or network lines.

   c. **Disguised use.** Users must not conceal their identity when using or accessing IT Systems, except when the option of anonymous access is explicitly authorized. Users are also prohibited from masquerading as or impersonating others or otherwise using a false identity.

   d. **Distributing computer viruses.** Users must not knowingly distribute or launch computer viruses, worms, or other rogue programs.

   e. **Modification or removal of data or equipment.** Without specific authorization, users may not remove or modify any College-owned or administered equipment or data from IT Systems.

   f. **Use of unauthorized devices.** These devices include, but are not limited to, laptops, computer systems, printers, scanners or video systems directly accessing our physical network via network interface cards or our secured protected wireless network, without specific authorization. Users are not permitted to attach wireless access devices to the College network without prior approval.

      Authorized devices include, but are not limited to, flash or thumb drives accessing Belmont computer systems, laptop systems accessing unsecured wireless network.

4. **Use in violation of law.** Illegal use of IT Systems—that is, use in violation of civil or criminal law at the federal, state, or local levels—is prohibited. Examples of such uses are: promoting a pyramid scheme; distributing obscenity; receiving, transmitting, or possessing child pornography; infringing copyrights; and making bomb threats.

With respect to copyright infringement, users should be aware that copyright law governs (among other activities) the copying, display, and use of software and other works in digital form (text, sound, images, and other multimedia). The law permits use of copyrighted material without authorization from the copyright holder for some educational purposes (protecting certain classroom practices and "fair use," for example), but an educational purpose does not automatically mean that the use is permitted without authorization.

5. **Use in violation of College contracts.** All use of IT Systems must be consistent with the College's contractual obligations, including limitations defined in software and other licensing agreements.
6. **Use in violation of College policy.** Use in violation of other College policies also violates this policy. Relevant College policies include, but are not limited to, those regarding sexual harassment and racial and ethnic harassment, as well as College policies and guidelines regarding incidental personal use of IT Systems.
7. **Use in violation of external data network policies.** Users must observe all applicable policies of external data networks when using such networks.

Personal Account Responsibility

Users are responsible for maintaining the security of their own IT Systems accounts and passwords. Any user who changes a password must conform to the published rules. Accounts and passwords are normally assigned to single users and are not to be shared with any other person without authorization by the applicable Systems Administrator. Users are presumed to be responsible for any activity carried out under their IT Systems accounts or posted on their personal web pages.

Responsibility for Content

Official College information may be published in a variety of electronic forms. The Certifying Authority under whose auspices the information is published is responsible for the content of the published material.

A. Belmont College's Internet access is intended to further the business purposes of Belmont College. Belmont College's Internet Access will not be utilized for any commercial activity that is not in support of College business.

B. Incidental personal use of the Internet access is permissible. Excluding incidental personal use, users will not access any electronic material that is not directly relevant to their assigned duties.

C. All electronic information and data generated or gathered by a user, in the course of his/her employment, utilizing College owned computer equipment, shall be for the furtherance of College business. Their contents may be accessed only by authorized personnel for compelling business and/or security reasons.

D. Belmont College reserves the right to monitor, filter, and/or review, at any time, all Internet utilization via Belmont College's Internet access. Belmont College also reserves the right to reveal any Internet access related information to any party that it deems appropriate. The use of encryption, the labeling of a communication as private, the deletion of a communication, or any other such process or action, shall not diminish Belmont College's rights in any manner.

E. Belmont College will disclose Internet access information to any party that it may be required to by federal or state law or regulation. This may include law enforcement search warrants and discovery requests in civil litigation.

F. Users will not post any comments or statements on any web page or send any messages to Internet newsgroups that are not intended to further the business or instructional purposes of Belmont College.

G. Users will not enter any Internet chat rooms or chat channels that are not directly related to the normal business or instructional operations of the College.

H. Users must exercise caution in downloading or sending large files such as OS images over the internet. Large files i.e. 500 megabytes or greater, sent or downloaded over the internet can disrupt internet access to other users in the College. Users may request a time for downloading or sending large files via the internet by emailing the network administrator admin@belmontcollege.edu. Belmont College reserves the right to restrict or limit computer internet access in such cases.

I. Each user is responsible for ensuring that his/her use of Belmont College's Internet access is consistent with this policy, any other applicable College policy, and appropriate business practices. Internet sites containing jokes, pornography, sexist material, racist material, defamatory material, obscene material, pirated software, or any other inappropriate material shall not be accessed. Further, the Internet access system shall not be used for any purpose in violation of any federal or state law or regulation.

J. Users should be mindful that Internet sites they visit collect information about visitors. This information will link the user to Belmont College. Users will not intentionally visit any site that might in any way cause damage to Belmont College's image or reputation.

K. Users should be aware that much of the material available on the Internet is copyrighted or trademarked. Other than viewing publicly available material, users will not use any material found on the Internet in any manner without first establishing that such use would not be in violation of a copyright or trademark.

L. Users will not reveal their passwords to anyone. Excluding members of the Information Systems department, users will not utilize or access Internet accounts belonging to any other user.

Electronic Mail

Employees of Belmont College use electronic mail (e-mail) to communicate within and outside the College. The proper use of this technology saves time and money, reduces administrative costs, enhances communications and improves service. However, unlawful or inappropriate use of these tools reduces the amount of resources available to satisfy the College's missions, and can infringe on the rights of others. The College expects all members of its community to use information technologies in a responsible manner. This policy shall apply to anyone having access to Belmont College's e-mail systems.

A. All e-mail and associated system resources are the property of Belmont College. E-mail is subject to the same restrictions on its use, and the same review process, as are any other College-furnished resources provided for the use of employees.

B. E-mail usage must be able to withstand public scrutiny. Users must comply with all applicable legislation, regulations, policies and standards. This includes complying with copyright and license provisions with respect to both programs and data.

C. The College encourages the use of electronic mail and respects the privacy of users. While a user may delete an e-mail message, copies of the e-mail may still remain on servers and backup tapes. The College does not routinely inspect, monitor, or disclose electronic mail without the holder's consent. Nonetheless, the College may deny access to its electronic mail services and may inspect, monitor, or disclose electronic mail (i) when required by and consistent with law; (ii) when there is substantiated reason to believe that violations of law or of College policies have taken place; or (iii) under time-dependent, critical operational circumstances.

D. All e-mails that are addressed to any person(s) outside of Belmont College will clearly identify the user by full name and official title. The user's telephone number should also be included. (This can be easily accomplished by utilizing the automatic signature feature of the electronic mail system.

E. While e-mail is provided as a business tool to users, its reasonable, incidental personal use is acceptable. This use must not, however, detrimentally affect employee productivity, disrupt the system and/or harm the College's reputation.

F. Users may not:

1. Use e-mail for commercial solicitation or for conducting or pursuing their own business interests or those of another organization;

2. Use e-mail to distribute hoaxes, chain letters, or advertisements; and/or send rude, obscene or harassing messages; or

3. Use e-mail to propagate viruses, knowingly or maliciously; or

4. Use e-mail to subscribe to any e-mail lists or list-serves that are not directly relevant to their assigned duties; or

5. Reveal their e-mail passwords to anyone; or

6. Utilize or access e-mail accounts belonging to any other user.

G. If users must subscribe to list-serve mail services for work-related lists, the users will make every effort to read, store and delete the mail as soon as possible. In addition, users must consider the impact on the network when creating and using large, work-related distribution lists.

H. Due to the potential for virus or Trojan horse attachments, users will exercise extreme caution by utilizing virus protection facilities when downloading and executing any files attached to e-mail. If the attachment is not clearly business related and/or expected from a known source, it should never be opened or executed. Such e-mails and attachments should be immediately deleted.

I. E-mail messages constitute records and management of e-mail must comply with existing record retention legislation, regulations, policies, and standards (e.g., the *Freedom of Information and Protection of Privacy Act*, the *Document Disposal Act*).

J. Any message received which is intended for another person should be returned to the sender. All copies of the misdirected message should be deleted after it has been returned to the sender. An incorrectly addressed message should only be forwarded to the intended recipient if the identity of that recipient is known and certain.

K. E-mail messages should be composed in a professional manner. Users will carefully review all e-mail prior to sending it to ensure that their meaning is clear and not subject to interpretation. Comments, humor and sarcasm that would be inappropriate in memorandums and letters are equally inappropriate in e-mails. Missing body language and tone can cause what was meant as a casual or humorous message to be taken other than intended. If a message generates an emotional response, the recipient should carefully consider an appropriate or professional response. The recipient should consider if a response is needed at all and react accordingly.

The College places a high value on privacy and recognizes its critical importance in an academic setting. Nonetheless, there are circumstances in which, following carefully prescribed processes, the College may determine that certain broad concerns outweigh the value of a user's expectation of privacy and warrant College access to relevant IT Systems without the consent of the user. Those circumstances are discussed below, together with the procedural safeguards established to ensure access is gained only when appropriate.

Conditions of College Access

A. **Conditions.** In accordance with state and federal law, the College may access all aspects of IT Systems, without the consent of the user, in the following circumstances:

1. When necessary to identify or diagnose systems or security vulnerabilities and problems, or otherwise preserve the integrity of the IT Systems; or
2. When required by federal, state, or local law; or
3. When there are reasonable grounds to believe that a violation of law or a significant breach of College policy may have taken place and access and inspection or monitoring may produce evidence related to the misconduct; or
4. When such access to IT Systems is required to carry out essential business functions of the College; or
5. When required to preserve public health and safety.

B. **Process.** Consistent with the privacy interests of users, College access without the consent of the user will occur only with the approval of the designated College official, except when an emergency entry is necessary to preserve the integrity of facilities, to preserve the health of the network. The College, through the Systems Administrators, will log all instances of access without consent. Systems Administrators will also log any emergency entry within their control for subsequent review by the President, Vice President, Dean, or other appropriate College authority. A user will be notified of College access to relevant IT Systems without consent. Depending on the circumstances, such notification will occur before, during, or after the access, at the College's discretion.

C. **User access deactivations.** In addition to accessing the IT Systems, the College, through the appropriate Systems Administrator, may deactivate a user's IT privileges, whether or not the user is suspected of any violation of this policy, when necessary to preserve the integrity of facilities, user services, or data. The Systems Administrator will attempt to notify the user of any such action.

Appropriate Use Agreement

Form 154 – Information Technology Appropriate Use Agreement is an overview of Belmont's Information Technology Appropriate Use Policy. Employees are required to sign off on Form 154 before utilizing any IT System.

The agreement will also be placed on computers at sign-in, in classrooms, and in the *College Catalog and Student Handbook*.

Enforcement Procedures

A. **Complaints of Alleged Violations.** An individual who believes that he or she has been harmed by an alleged violation of this policy may file a complaint in accordance with established College Grievance Procedures (including, where relevant, those procedures for filing complaints of sexual harassment or of racial or ethnic harassment) for students, faculty, and staff. The individual is also encouraged to report the alleged violation to the appropriate administrator overseeing the facility most directly involved, or to the College Administration, which must investigate the allegation and (if appropriate) refer the matter to College disciplinary and/or law enforcement authorities.

B. **Reporting Observed Violations.** If an individual has observed or otherwise is aware of a violation of this policy, but has not been harmed by the alleged violation, he or she may report any evidence to the appropriate administrator overseeing the facility most directly involved, or reporting directly to the College Administration.

C. **Disciplinary Procedures.** Alleged violations of this policy will be pursued in accordance with the appropriate disciplinary procedures for faculty, staff, and students, as outlined in the *Operating Policies Manual*. Any employee or student found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or dismissed from college.
Systems Administrators may participate in the disciplinary proceedings as deemed appropriate by the relevant disciplinary authority. Moreover, at the direction of the appropriate disciplinary authority, Systems Administrators are authorized to investigate alleged violations.

D. **Penalties.** Individuals found to have violated this policy may be subject to penalties provided for in other College policies dealing with the underlying conduct. Violators may also face IT-specific penalties, including temporary or permanent reduction or elimination of some or all IT privileges. The appropriate penalties shall be determined by the applicable disciplinary authority in consultation with the Systems Administrator.

E. **Legal Liability for Unlawful Use**. In addition to College discipline, users may be subject to criminal prosecution, civil liability, or both for unlawful use of any IT System.

F. **Appeals.** Users found in violation of this policy may appeal or request reconsideration of any imposed disciplinary action in accordance with the appeals provisions of the relevant disciplinary procedures.

RELATED DOCUMENTS

- Freedom of Information & Protection of Privacy Act www.justice.gov/oig/FOIA/mis-foipa.htm
- Belmont College Catalog & Student Handbook
- Belmont Operating Policies Manual
- Belmont Operating Policy 740.0330.91, Student Code of Conduct
- Belmont Operating Policy 800.0100.97 , Records Retention
- Belmont Operating Policy 515.0200.10 , Employee Code of Conduct
- Belmont Operating Policy 1000.0400.11, Employee Separation Information Systems
- Belmont Operating Policy 1000.0500.11, Broadcast Email
- Belmont Operating Policy 1100.0220.10, Children on Campus
- Form 154 – Information Technology Appropriate Use Agreement