Memorandum of Understanding

December 3, 2007

General Information

Asbury College provides and maintains the campus data communications networks and information technology services for all employees and students. This system of networks and services includes, but is not limited to e-mail, file servers, administrative systems, web services, and the Internet. This Memorandum of Understanding outlines how employees and students may access the data networks, systems, and services and how they should be used.

The College reserves the right to monitor and limit the use of its computing and network facilities through procedures which are consistent with its mission and the role that computers and data networks are intended to play within that mission. It is our fervent hope that each person who uses the data communications systems will do so in a way that will honor Christ and His Kingdom.

Personal Use of the Internet and Electronic Mail

The Internet and Electronic Mail are available for Faculty, Staff and Students to use for both college and personal activities. The college reserves the right to monitor the network and services in order to manage and maintain those systems. It is also necessary to monitor network use to enforce usage policies. Priority for the limited technology resources will be given to the academic work and business needs of the college.

Excessive use of e-mail or network bandwidth, as defined by disproportionately high use, is not permitted and may result in your network access being limited or cut off for a period of time.

Usage of other Information Systems

With account privileges on Asbury College's Information system, you will have access to many other information systems, through its Internet connection. Be advised that some information systems to which you will have access may contain material which is defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal. The College does not condone the use of such materials and does not permit usage of such materials in the College's own information environment. Employees or students who knowingly bring such materials into the College's information environment will be subject to the same disciplinary policies that apply in other campus situations. Electronic forums do not constitute a separate universe of discourse, governed by a separate ethic, but must be approached under the same set of moral and ethical guidelines that govern other means of discourse at the College.
On-line Conduct

Your account and access to the College's information systems is for employee or student use only. This means that the College does not authorize you to grant others the use of your college-provided accounts. Staff and Faculty must notify the Information Services Help Desk before installing any software on college-owned equipment. Information Services employees maintain Staff and Faculty computer equipment along with all lab computer equipment.

Only public domain software, or software for which the owner has given express consent for on-line distribution, may be transferred to or stored on the College's Information systems. Any software whose purpose is to damage or interfere with use of the system by others is prohibited. The College reserves the right to monitor and terminate the account of anyone found to be in violation of this policy.

Copyrighted material must not be placed on the College's servers or shared on the college network without the author's permission. Only the author(s) or persons they specifically authorize may upload copyrighted material to the College's Information systems.

You may upload public domain programs or information using the College's Information systems. Please verify that your program or other material is in the public domain.

Security on any computer system is a high priority, especially when the system involves many users. If you can identify a security problem on the College's Information systems, you should notify the Information Services department, or send e-mail to helpdesk@asbury.edu. You should not demonstrate the problem to others.

Using or attempting to use software, hardware, or any methods to circumvent or disable any form of security, monitoring, metering, or college measures used to manage, monitor, or control networks, servers, printers, computers, and the Internet (firewall security and content filtering) are not permitted and may result in disciplinary action.

Excessive use of information technology resources, including but not limited to campus network bandwidth, server capacity, Internet bandwidth, and e-mail is not permitted. If any one computer or person causes a disruption to the network or servers then Information Services may disable the network connection to that single computer or the person’s network account so the rest of the campus can continue normal data services. Once the problem has been revolved, the computer connection to the network or person’s account can be restored.

Upon termination of your account with Asbury College’s Information Services, any software legally retained by you shall remain subject to the license agreement under which it was originally obtained from the vendor. You are responsible for the legal and proper use of such software and hereby agree to indemnify and hold Asbury College, its Board of Trustees, officers, employees, and agents harmless from any claim, loss or demand arising from your use of such software.

Computer Accounts and Passwords

You may not allow others to use your account and password. Every student and employee is provided with one or more computer accounts. Those accounts are to be used only by the person they were assigned to and should never be given to or used by anyone else. You are responsible for anything done through the use of your account. Sharing your college-provided account with another person may be grounds for disciplinary action, up to and including dismissal.
Strong passwords should be used. By definition, strong passwords are words use a mix letters and numbers. You should NOT use names or words that can be found in a dictionary for a password.

Do not disclose passwords to anyone including Information Services personnel. If your password must be changed, Information Services staff will assign you a temporary password and require you to change the password the first time you login to the network. Passwords should also be changed periodically to enhance the security of your files.

**SPAM**

SPAM is defined as unsolicited e-mail that is not about the business of the college or about college sponsored events. Any college communication about the work or business of the college and/or college events is not considered spam.

Administrative Departments and Faculty are permitted to send campus messages that contain information that is pertinent to everyone. Advertising non-college events or business and lost and found messages are two specific examples of SPAM that is not permitted. Anyone who SPAMS the campus with an inappropriate message will be contacted and given one warning. Subsequent violations will result in lost e-mail privileges for an appropriate period of time. Public email folders are available to post these announcements. If you have questions about public folders, please call the Help Desk ext. 2177.

**Unlawful Access to a Computer**

Unlawful Access to a Computer is a legal offense, defined in Section 434.840-860 of the Kentucky Code as follows:

1. A person is guilty of unlawful access to a computer when she/he knowingly and willfully, directly or indirectly accesses or attempts to access any computer software, data, computer system or network to defraud or damage another computer system, program or network. (KRS 434.845)

2. A person is guilty of misuse of computer information when she/he receives, conceals, or uses or aids another in doing so, any books, records, documents, property, financial instrument, computer software, computer program, or other material, property, or objects, knowing the same to have been used in or obtained from a violation of KRS 434.845.

Unlawful access to a computer will result in cancellation of privileges as well as other disciplinary action. Specific acts of computer, but are not limited to tampering include changing the network configuration of your computer, uploading or creating computer viruses or password cracking programs, or attempting to use any account without proper authorization.

**Termination of Accounts**

You may terminate your account on the College's Information systems by sending notice to Information Services. Termination will be effective on the day that a system administrator receives the notice or on a future date if so specified in the Notice. Accounts for graduating seniors are normally removed the next working day after graduation.

System administrators reserve the right to suspend or terminate your access to the College's Information systems upon any breach of the Memorandum of Understanding. Prior to a
suspension or termination or as soon after as is practicable, system administrator will inform you of the suspected breach and give you an opportunity to present an explanation. You may request a review hearing within seven (7) days of such suspension or termination if you feel that such action was unjust. After the review, access may be restored if your appeal is upheld.

To appeal the decision of a system administrator, you must file a written request with appropriate information to the Director of Information Services. The director will discuss the appeal with other staff of Information Services during their staff meeting and decide whether to grant the appeal. If you are not satisfied with the Director of Information Services response, you may appeal the Directors decision to a special Vice Presidential committee composed of the VP for Student Development, the VP for Business Affairs and the Provost.

December 2007