TECHNOLOGY HANDBOOK

All Saints Bible College is authorized for operation as a post-secondary education institution by the Tennessee Higher Education Commission.

All Saints Bible College ***holds "Candidate" status with the Association for Biblical Higher Education, 5850 S. T. G. Lee Blvd., Ste. 130, Orlando, FL 32822, 407.207.0808.***

ALL SAINTS BIBLE COLLEGE

TABLE OF CONTENTS

Mission Statement

All Saints Bible College (ASBC) provides Christian-oriented academic programs, to create a stimulating intellectual environment, and to promote spiritual renewal as it equips men and women for Christian ministry and service in church and in society.

I. TECHNOLOGICAL RESOURCES

Statement of Policy:

Computer/Technology Requirements – Students must have access to a personal computer, be connected to the World Wide Web (www) by a reliable Service Provider (ISP). The Academic Computer Lab is available to all ASBC students who pay the general fee. It is also available to ASBC Faculty and Staff as space permits.

Procedures:

A. HOURS

The lab will be available to students Monday through Thursday each week. The specific schedule is posted on the classroom Area bulletin board on the Lower Level of the Church of God in Christ administration building.

When the Lab is closed:

The Lab is ALWAYS closed for Chapel services.
Hours are adjusted to accommodate holidays, school breaks, etc. Check for the specific schedule posted on the classroom Area bulletin board on the Lower Level of the Church of God in Christ administration building.

B. USE OF ASBC COMPUTERS AND INTERNET ACCESS

.01 The purpose of these guidelines is to maintain the integrity of All Saints Bible College's computer network. Understanding of, and abiding by these guidelines, is essential to ensure that the system can be used without impeaching its integrity.

.02 The purpose of All Saints Bible College's network resources, including the Internet, is to support the college in the achievement of their mission and goals, and to improve the Christian community in general. These resources are intended to facilitate day-to-day operations.

.03 If there are any questions regarding the use of college computers or Internet access, it is incumbent upon the employee to seek guidance through the Director of Computer Services.

1. Computer Network Restriction

.01 ASBC computers are to be used for college business. Employees shall not use a ASBC account for any activity that is commercial in nature, not related to work at ASBC, such as consulting services, typing services, developing software for sale, advertising products, website development, and/or other commercial enterprises for personal/financial gain.

.02 Without prior written permission from the Director of Computer Services, the ASBC computer network may not be used to disseminate, view or store commercial or personal advertisements, solicitations, promotions, destructive code (e.g., viruses, Trojan horses, worms, bots, flash programs, self-replicating programs, etc.), political material or activities, pornographic text or images, copyrighted material, or any other unauthorized materials.

.03 Employees may not use the ASBC Internet connection to download games or other entertainment software (including screen savers), or to play games or gamble over the Internet. Additionally, employees may not use the computer network to display, store, or send (using e-mail or any other form of electronic communication such as bulletin boards, chat rooms, user groups, etc.) material that is fraudulent, harassing, discriminatory, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise inappropriate or unlawful.

.04 ASBC Administration, Faculty, Staff and Students shall not attempt to:

- circumvent data protection schemes or uncover security loopholes without prior written consent of the Director of Computer Services. This includes creating and/or running programs that are designed to identify security loopholes and/or intentionally decrypt secure data;

- monitor or tamper with another user's electronic communications or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner;

- facilitate or allow use of a computer account and/or password by an unauthorized person;

- mask the identity of an account or machine which includes sending e-mail that appears to come from someone else; and

- perform an act without authorization that will interfere with the normal operation of computers, terminals, peripherals, networks, or will interfere with others' ability to make use of the resources.

2. Accessing the Internet

.01 The Internet is a worldwide network of computers that contains billions of pages of information. This service is provided to ASBC to facilitate communication, information sharing, information access and enhancement of their job performance. Its use shall be limited to legitimate school business and managed by rules of conduct applicable to any other school owned resource. Users are cautioned that many Internet pages include offensive, sexually explicit, and/or inappropriate material.

.02 As a test to determine if an individual's use of the Internet is necessary or appropriate, the following question shall be asked: *"Is this use of the Internet enabling me to perform my duties more effectively, less expensively, or provide better service to All Saints Bible College?"*

.03 It is acceptable Internet use to perform the following functions as well as those specifically instructed by their supervisors:

- Communications of information exchanges directly relating to the college's Mission;

- Announcements of school, activities and policies and procedures;

- Use for advisory, research, analysis and development activities related to the users duties and responsibilities.

.04 To ensure security and avoid the spread of viruses, users accessing the Internet through a computer attached to the ASBC network must do so through an approved Internet firewall or other security device. Bypassing ASBC computer network security by accessing the Internet directly by modem or other means is strictly prohibited, unless the computer you are using is not connected to the ASBC's network.

3. Frivolous Use

.01 Computer resources are not unlimited. Network bandwidth and memory have finite limits, and all users connected to the network have a responsibility to conserve these resources. Therefore, users must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to: sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-school-related uses of the Internet.

4. Virus Detection

.01 Files obtained from sources outside of ASBC, including disks brought from home, files downloaded from the Internet, newsgroups, bulletin boards, or other online services, files attached to e-mail, and files provided by customers or vendors may contain dangerous computer viruses that may damage the ASBC computer network. Users must not download files from the Internet, open suspicious e-mail attachments from outsiders, or use disks from unknown ASBC sources without first checking for viruses.

.02 Before opening any e-mail attachment, the employee shall first right click on the attachment icon and click "view" to look at attachment without opening it into the ASBC's network or personal computer.

5. Handling a Computer Virus

Outlined below are the recommended steps when a computer virus is detected on their workstation.

.01 ALWAYS, immediately document in writing what is happening including any error messages. To report the problem accurately, it is best not to rely on your memory. Be as specific as possible. Some computer viruses can take time to reveal themselves. Record any unusual messages that are randomly displayed even if they don't seem to affect the performance of your workstation; how you became aware of the problem; what you were doing before the event occurred; and what application was in use at the time of the event. Identify any removable diskettes that may have been used during this period. Any data you have saved could potentially have been infected by the virus. These diskettes shall also be scanned for a virus. Do not use these diskettes until they have been checked for a virus.

.02 Turn off your workstation. To contain the virus, it is best to immediately power-off your workstation. Do not attempt to initiate a normal shutdown. A computer virus can run as a TSR (terminate and stay resident) and as a background process it will continue to cause damage without any indication to the user.

.03 If possible, do not login to the network on another workstation until you receive help. There is a potential risk that your files on the network have been infected. To assist in containing the virus, it is important that you discontinue logging in to the network until anti-virus checks are made there also.

.04 The Director of Computer Services shall be notified immediately and all recorded information shall be forwarded to him.

.05 Resume using your system only after you have received verification that the computer virus has been removed and it has been determined to be virus free.

6. No Expectation of Privacy

.01 Employees are given computers and Internet access to assist them solely in the performance of their duties. Employees shall have no expectation of privacy in anything they create, store, send or receive via the e-mail system using ASBC computer equipment. As stated above, the computer network is the property of ASBC and may be used only for ASBC purposes.

7. Waiver of Privacy Rights

.01 Every user expressly waives any right of privacy in anything he/she creates, stores, sends, or receives via the e-mail system using ASBC's computer equipment or Internet access. The user consents to allow designated ASBC personnel access to and review of all materials created, stored, sent, or received by user through any ASBC network or Internet connection.

8. Blocking Sites with Inappropriate Content

.01 ASBC reserves the right to utilize software that makes it possible to identify and block access to Internet sites containing sexually explicit or other material deemed inappropriate.

9. Security

.01 It is a priority of ASBC to achieve the highest levels of confidentially as possible in the school's computer network. In order to maintain proper security controls, cooperation will be necessary in the following areas:

10. Passwords

.01 User passwords will be issued and controlled by the Director of Computer Services. These passwords are used to identify authorized users on the school system. Therefore, each employee password must be maintained secretly, known only by the employee and the Director of Computer Services. The employee shall not share his or her password or allow anyone else to use it. A password shall consist of a word and/or numbers known to the employee but not easily guessed by others.

11. Use of System

.01 The computer system is to be used only by those with assigned accounts.

12. Logging Off System When Away From Office

.01 If employees are going to be away from their desk for an extended period of time or at the end of the workday, they shall log off the system to prevent unauthorized access under their user name.

.02 Under normal operations at the end of each days work, employees are to log off from all network systems and any file server connections; close all desktop applications; make sure that all file sharing systems are turned off; and then power down their desktop computer.

13. Stand-Alone Computers and Laptops

.01 The guidelines mentioned in this section also relate to stand-alone and laptop computers. There will be no unauthorized use of, or software allowed to be loaded onto a school owned computer. If a computer is connected to a school modem, the employee is permitted to download only to the stand-alone or laptop's hard drive. Under no circumstances shall a download take place to the school network computer system.

14. Donated Computer Equipment and Equipment not Purchased by the College

.01 Computer equipment not procured by the Director of Computer Services will not be maintained or serviced by the school. Every effort is made to maintain system compatibility and standardization to ensure adequate spare parts are in stock and personnel are knowledgeable in maintenance and repair of such equipment. As with any purchase or donation, approval from the President is required before the item is purchased or accepted.

15. Monitoring of Computer and Internet Use

.01 ASBC reserves the right to monitor and log onto any and all aspects of its computer system including, but not limited to, monitoring Internet sites visited by users, monitoring chat and newsgroups, monitoring file downloads, and all communications sent and received by users.

.02 Each users will be required to sign a Use of School Computer and Internet stating that they have read, understand and will comply with the standards set forth in this policy.

16. Requests for Removal of Access to On-Line Systems

.01 For users who have terminated their relationship with ASBC, removal of access will be done.

C. USE OF SCHOOL SOFTWARE

.01 ASBC licenses the use of computer software from a variety of third parties. The software developer usually copyrights software. Unless expressly authorized to do so, ASBC users may not make copies of software except for back-up or archival purposes. The purpose of this procedure is to prevent copyright infringement and to protect the integrity of the ASBC computer environment from viruses. For additional information on copyright infringement, refer to the Computer Software sub-section of the Copyright Infringement policy as found in the General Administration Section of this Policies and Procedures Manual.

.02 It is the policy of ASBC to respect all computer software copyrights and to adhere to the terms of all software licenses to which they are a party. The Director of Computer Services is responsible for enforcing these guidelines.

.03 ASBC users may not duplicate any licensed software or related documentation for use either on school premises or elsewhere unless if is expressly authorized to do so by an agreement with the licenser. Unauthorized duplication of software may subject users to both civil and criminal penalties under the United States Copyright Act.

.04 Employees may not give ASBC-owned/registered computer software to any other users or any registered software to non-employees including: spouses, parents, contractors, students, and others. Users may use owned/registered software on the college's local area network or on multiple machines only in accordance with applicable license agreements.

.05 For a complete description of ASBC computer services policies and procedures, please refer to the Computer Services section found in the General Administration Section of this Policies and Procedures Manual.

1. Personal Software

.01 The use of personal software will not be allowed. Loading personal software is the number one means of introducing viruses into a computer network. Valid software licenses are required for all software loaded onto the school computer network. If there is a software package an employee desires to have available on the network, the employee shall notify the Director of Computer Services, and if approved, it will be purchased and installed by the Director of Computer Services.