Bishop State

A Member of the Alabama Community College System

Information Technology
Acceptable Use Policies for Students

1.0 Overview

The college's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to the college's established culture of openness, trust and integrity. Bishop State Community College is committed to protecting the college's employees, partners and students from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and BORIS access, and are the property of Bishop State Community College. These systems are intended to be used for school purposes in order to enhance student learning, not for personal use.

Effective security is a team effort involving the participation and support of every person who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Bishop State Community College. These rules are in place to protect the student and the college. Inappropriate use exposes Bishop State Community College to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies specifically to students and potential students of Bishop State Community College. This policy applies to all equipment that is owned or leased by Bishop State Community College that is available for student use. A separate document exists for employee policy.

4.0 Policy

4.1 General Use and Ownership

1. While Bishop State Community College's computer services desires to provide a reasonable level of privacy, students should be aware that the data they create on the corporate systems remains the property of Bishop State Community College. Because of the need to protect Bishop State Community College's network, management cannot guarantee the confidentiality of information stored on any network device belonging to Bishop State Community College.
2. The college recommends that any information that students consider sensitive or vulnerable be secured in an appropriate manner and not be stored on any Bishop State Community College computer or network device.
3. For security and network maintenance purposes, authorized individuals within the college may monitor equipment, systems and network traffic at any time.
4. Bishop State Community College reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by the college. Examples of confidential information include but are not limited to: Social Security numbers, student numbers, PINs, etc. Students should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. E-mail passwords should be changed at regular intervals.
3. Students must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.6 Unacceptable Use

The following activities are, in general, prohibited. Under no circumstances is a student of Bishop State Community College authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Bishop State Community College owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities, which fall into the category of unacceptable use.

4.6.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Using Bishop State Community College owned computing equipment for personal or non-school related activities.
2. Violating the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Bishop State Community College (see **illegal file-sharing** below).
3. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Bishop State Community College does not have an active license is strictly prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Revealing your account password to others or allowing use of your Bishop State e-mail, BORIS, or Blackboard accounts by others. This includes family and other household members.
7. Using a Bishop State Community College computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any Bishop State Community College account.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the student is not an intended recipient or logging into a server or account that the student is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet

spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to Computer Services is made.
11. Executing any form of network monitoring.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, Bishop State Community College employees to parties outside Bishop State Community College without proper authorization.

4.6.2 Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Bishop State Community College's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Bishop State Community College or connected via the college's network.
7. Sending mass mailings to all students. This activity is limited to Bishop State employees only, and only with the approval of Computer Services.

4.6.3 Illegal File-sharing and Downloading (P2P)

1. Illegal downloading and sharing of copyrighted materials on the Bishop State Community College network is strictly forbidden, in accordance with HEOA regulations issued October 29, 2009. These materials include copyrighted music (.mp3/.mp4, etc. files), bit torrents, and other illegal movie and video downloads.
2. The College uses content filtering to reduce and block file sharing activity, as well as traffic monitoring.
3. Anyone who engages in this type of unauthorized distribution of copyrighted materials, including peer-to-peer (P2P) file sharing, may be subject to civil

and criminal liabilities, as well as any disciplinary action that deemed appropriate by the College.

4. The College will review this policy yearly and make modifications where necessary.
5. Below is a list of resources that may be helpful in further understanding this process, and any legal alternatives:

http://www.educause.edu/HEOA

http://www.educause.edu/Resources/Browse/LegalDownloading/33381

http://www.educause.edu/blog/sworona/189008

5.0 Enforcement

Any student found to have violated this policy may be subject to disciplinary action, up to and including suspension.

6.0 Definitions

Term	**Definition**
Spam	Unauthorized and/or unsolicited electronic mass mailings.
VPN	Virtual Private Network – software and hardware that creates a secure Internet "tunnel" allowing remote access to a local network through that network's firewall.
Ponzi	A fraudulent investment operation that pays returns to investors from their own money or money paid by subsequent investors rather than from any actual profit earned.
FTP	File Transfer Protocol – a network protocol used to store and exchange files over a computer network, and usually over the Internet.
Blog	An abbreviation for "web log", usually maintained by an individual with regular entries of commentary, descriptions of events, or other material such as graphics or video, posted in reverse chronological order.
P2P	An abbreviation for "peer-to-peer" file sharing. This refers to a type of file-sharing where computers or other Internet-ready devices are used to share music, video, and other materials with other users via the Internet, and there is usually no centralized server involved.