

Computer and Information Systems Policy of The Baptist College of Florida

I. Overview

The Baptist College of Florida's intentions for publishing a *Computer and Information Systems Policy* are not to impose restrictions that are contrary to the spirit of The Baptist College of Florida (BCF), but to enhance the protection of its constituents against illegal or damaging actions by individuals, either knowingly or unknowingly, while promoting a culture of openness, trust, and integrity.

Information systems owned and operated by The Baptist College of Florida, are to be used for institutional purposes in serving the interests of BCF, and of our constituents in the course of normal operations.

Effective security is a team effort involving the participation and support of every BCF constituent who deals with information and/or information systems. It is the responsibility of every constituent to know these guidelines, and to conduct his or her activities accordingly.

BCF reserves the right to amend this *Computer and Information Systems Policy* at any time and from time to time.

II. Purpose

The Baptist College of Florida relies heavily upon information systems to meet operational, financial, educational, and informational needs. It is essential that these systems be protected from misuse and unauthorized access. It is also essential that BCF's computers, computer systems, and computer networks, as well as the data they store and process, be operated and maintained in a secure environment and in a responsible manner. Computing resources are valuable, and their abuse can have a far-reaching negative impact. Computer abuse affects everyone who uses computing facilities. The BCF community should exercise high moral and ethical behavior in the computing environment.

III. Scope

This policy applies to ALL information systems and refers to ALL hardware, data, software, and communications networks associated with these systems whether these systems are owned or leased by BCF or connected to BCF networks. This policy applies to all constituents of The Baptist College of Florida. In addition to this policy, all constituents are subject to applicable federal, state and local laws.

IV. Definition of Terms used in this document

Computer Systems: Computer systems include but are not limited to stand-alone or networked microprocessor devices, workstations or mainframe resources including the peripheral devices that connect to these resources.

Computer Networks: Computer networks are a collection of connected communicating computers, local or wide area, wired or wireless, and the hardware and software that connects the networks and individual terminals, microcomputers, or workstations to other devices.

Constituents: Constituents are users; constituents include employees, students, alumni, contractors, consultants, temporary workers, visitors, volunteers and all personnel affiliated with third parties who use or access Information Systems.

Custodian: Individual who has been assigned responsibility for or is accountable for the files and the data contained in the files.

Email: The electronic transmission of information through a mail protocol.

Host: Individual computer system . This may include, but is not limited to servers, desktop computers, notebook computers, tablet computers, or PDA type devices

Information Systems: Information Systems include Internet/intranet/Extranet-related systems, including but not limited to computer equipment, computer networks (wired and wireless), software, databases, file services, operating systems, storage media, network accounts providing electronic mail or network access, WWW browsing, and FTP (File Transfer Protocol).

Public Listings: Sites that are accessible by the public using computer resources. This may include, but is not limited to newsgroups, blogs, or chat rooms.

Sensitive Information: Information is considered sensitive if it can be damaging to BCF or its customers' dollar value, reputation, or market standing.

Spam: Unauthorized and/or unsolicited electronic mass mailings.

Unauthorized Disclosure: The intentional or unintentional revealing of restricted information to people who do not have a need to know that information.

Users: Users are constituents; users include employees, students, alumni, contractors, consultants, temporary workers, visitors, volunteers and all personnel affiliated with third parties who use or access Information Systems.

V. Computer Usage Guidelines

A. Authorization and Security

Each constituent must have a valid, authorized account in areas where required; may only use his/her account in accordance with its authorized purpose; may not allow other persons to use his/her account unless authorized by BCF's Management Information Systems (MIS) for a specific purpose; is responsible for safeguarding his/her own computer accounts, specifically user names, passwords and/or personal identification numbers (PIN).

Each constituent must have specific authorization from MIS to use information systems. Constituents may not connect unauthorized or unsupported devices to BCF information systems.

Postings by constituents from a BCF email address to public listings are prohibited, unless posting is in the course of business duties.

All hosts used by constituents and connected to The Baptist College of Florida computer systems and computer networks, whether owned by the constituent or The Baptist College of Florida must be continually executing virus-scanning software with a current virus database and definitions.

Constituents must exercise extreme caution when opening email attachments which may contain viruses, email bombs, or Trojan code.

B. Auditing and Monitoring Policy

While The Baptist College of Florida desires to respect the privacy of its constituents, constituents should be aware that the data created or stored on BCF information systems is the property of The Baptist College of Florida and is subject to access by BCF as provided below. Because of the need to protect BCF information systems, BCF cannot guarantee the confidentiality of information stored on any network device belonging to The Baptist College of Florida.

For security and network maintenance purposes, MIS may monitor equipment, systems, network traffic and logs at any time. BCF designates certain personnel to investigate suspected information systems abuse or violations of other BCF policies. The College reserves the right to examine any and all files, including email, and logs.

Audits may be conducted to: Ensure integrity, confidentiality and availability of information and resources; Ensure conformance to BCF *Computer and Information Systems Policy*; Monitor user or system activity where appropriate; and Investigate possible security incidents or violations of BCF policies.

When requested, or for the purpose of performing an audit, any access needed will be provided to authorized members of the BCF staff. This access may include: User level and/or system level access to any computing or communications device; Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on BCF equipment or premises.

C. Access to BCF Information Systems

Constituents may not change, copy, delete, read, or otherwise access files or software without permission of the custodian of the files or MIS. Constituents may not: bypass accounting or security mechanisms to circumvent data protection schemes; attempt to modify software except when intended to be user customized; prevent others from accessing the system by software modification.

Constituents must exercise caution to prevent the unauthorized or inadvertent disclosure or transmission of sensitive information.

D. Software Acquisition and/or Distribution

Constituents may not distribute copyrighted proprietary material without the written consent of the copyright holder; violate copyright, information property or patent laws concerning computer software, documentation, or other tangible assets; load any copyrighted software onto any device (except software lawfully loaded onto personally-owned devices) without specific prior permission from MIS.

Constituents are strictly prohibited from the unauthorized copying or use of unlicensed software; such action is not considered to be taken in the course of employment. As a result, BCF will not provide legal defense for individuals who may be accused of making unauthorized copies of software even if these individuals maintain that such action was taken in the course of their employment. If BCF is sued or fined because of unauthorized copying or use by constituents, it may seek payment from the individuals as well as subject them to appropriate disciplinary or legal action.

E. Decency/Community Values

Constituents must not use BCF computer systems or BCF computer networks to violate any rules in the BCF Faculty/Staff/Student handbooks or policy manuals or any local, state, or federal laws.

A constituent shall disclose to the appropriate BCF authorities misuses of computing resources or potential loopholes in computer systems security and cooperate with appropriate BCF or other authorities in the investigation of abuses.

BCF provides access to various resources, such as the Internet, through its network. BCF does not tolerate the use of information systems for pornographic or other uses that are inappropriate in an academic or Christian setting and violate the values set forth in the BCF Faculty/Staff/Student handbooks. Values violations include **computer misconduct, harassment, disorderly conduct, disrespect for others, insubordination, lewd and indecent conduct, misrepresentation or forgery, slander, and other conduct that is not consistent with BCF's moral and Christian values.** In addition to the termination of computer use privileges, employees or students found guilty of values violations are subject to disciplinary action as set forth in the BCF Faculty/Staff/Student handbooks, and may include dismissal.

F. Email Usage

Constituents must exercise utmost caution when sending any email from inside BCF to an outside network.

G. BCF Wireless Net Policy

BCF Wireless Net operates on the 2.4 GHz band. Usage of low cost wireless 2.4 GHz devices has grown rapidly and this has created obstacles to the proper operation and performance of this wireless technology. We all must be aware of the potential interference of 2.4GHz wireless devices within our wireless network coverage area.

Devices that interfere or conflict with the operation of BCF Wireless Net should not be operated on the BCF campus. Devices that can interfere with BCF Wireless Net include, but are not limited to:

- 2.4 GHz spectrum cordless phones
- 2.4 GHz consumer short distance wireless video links
- wireless Ethernet access points/routers
- A computer operating in IEEE 802.11b/g Ad-Hoc (peer-to-peer) mode.
- Apple Airport Base Station and the Macintosh computer operating as a software base station

Please note that Xbox 360 and Media Center PCs have been reported to cause problems with 2.4GHz wireless networks.

VI. Unacceptable Use of Information Systems

The following activities are prohibited. However, under appropriate circumstances employees may be exempted from these restrictions during the course of executing their job responsibilities. Such authorization will come from the Senior Vice President and will be in writing. (For example, MIS staff may disable the network access of a host if that host is disrupting production services).

The lists below are not intended to be an exhaustive list of unacceptable conduct, but rather provide examples of types of activities which violate BCF's rules. BCF reserves the right to take appropriate disciplinary action against any constituent who violates the letter or spirit of these rules and policies. Sanctions imposed by BCF in response to academic or disciplinary violations shall be in addition to fines or penalties that may be imposed by law enforcement authorities for illegal acts.

A. Privacy Violations

- Attempting to access another user's computer files or data without permission
- Supplying or attempting to supply false or misleading identification information to

- access another user's account
- The unauthorized "borrowing" or examination of another user's data or output
- Deliberate, unauthorized attempts to access or use BCF's resources, computer facilities, networks, programs, data, or any system files other than those designated for public access
- Unauthorized capturing of data from computer systems or computer networks
- 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.

B. Theft

- Using any method to avoid normal charges for the use of computer resources
- Abuse of specific computer resources, such as the Internet or BCF computer networks
- Attempting unauthorized or illegal access to computers outside the Institution using BCF's computers or computer networks
- Removing or moving BCF owned computer equipment or audio/visual equipment without proper authorization
- Executing any form of network monitoring which may intercept data not intended for the constituent's host
- Providing information about or a list of BCF employees, students, alumni or former students to parties outside The Baptist College of Florida
- Unauthorized use or forging of email header information

C. Vandalism

- Alteration, or attempted alteration, of user system software, data, or other files, as well as resource or equipment destruction or disruption
- Intentional introduction or spreading of computer viruses, Trojans, email bombs or other software which causes harm to information systems or to another users account
- Tampering with or obstructing BCF's information systems
- Inspecting, modifying, or distributing data or software without proper authorization, or attempting to do so
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the constituent is not an intended recipient or logging into a server or account that the constituent 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, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes
- Damaging computer network related hardware, computer hardware or software

D. Copyright Issues

BCF owns licenses to a number of proprietary programs. Constituents who redistribute software from the computing systems break agreements with BCF software suppliers, as well as applicable copyright, patent, and trade secret laws. Therefore, the redistribution of any software from computing systems is strictly prohibited except in the case of software that is clearly marked as being in the public domain. Violations include, but are not limited to:

- Copying, transmitting, disclosing data, software or documentation without proper authorization, or attempting to do so.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws

E. Harassment

- Repeated sending of unwanted messages or files
- Generating or storage of spam on, or sending of spam from BCF Information Systems
- Interfering with the legitimate use of computer resources of another user
- Sending of abusive or obscene messages via information systems
- Use of information systems to engage in abuse of constituents

F. Unethical or Illegal Use, Games, Chain Letters, Miscellaneous

- Sending chain letters, unauthorized mass mailings, "Ponzi" or other "pyramid" schemes of any type.
- Using BCF computer systems for non-professional, non-academic, unethical, or illegal purposes
- Excessive use of BCF computer networks for personal entertainment (e.g.; radio, television broadcasts, music, games, competitions, file downloads, etc.) that hinders the legitimate work of other constituents
- Using BCF owned computers for recreational purposes
- Personal advertisements or commercial activity
- Port scanning or security scanning
- Posting the same or similar non-business-related messages to large numbers of public listings including newsgroups

VII. Penalties and Enforcement

Misuse or abuse of BCF's computers, computer systems, computer networks, and data is forbidden. Misuse or abuse of information systems is not simply unethical; it can be a violation of user responsibility and federal laws. Therefore, BCF will take appropriate action in response to user misuse, unethical use, or abuse of information systems. Action may include, but is not limited to the following:

- Referral to the appropriate office for disciplinary action
- Referral to appropriate law enforcement authorities outside of BCF
- Access to all computing facilities and system may be suspended temporarily or removed permanently.
- Legal action may be taken to recover damages.

Alleged computer abuse or misuse of Information Systems by students will be referred to the Director of Student Services. If evidence of a violation is found, it will be treated as an academic violation or a disciplinary rule violation as appropriate. Violations may result in the suspension or loss of computer and/or network privileges. Violations that could result in misdemeanor or felony charges may be referred to the appropriate authorities for prosecution to the fullest extent of the law.

Alleged computer abuse or misuse of computing services by faculty or staff will be referred to the appropriate supervisor. If evidence of a violation is found, appropriate disciplinary action will be taken. Violations which could result in misdemeanor or felony charges may be referred to the appropriate authorities for prosecution to the fullest extent of the law.

VIII. Distribution of This Policy

The Baptist College of Florida will ensure that all constituents are aware of the policy by publishing and distributing it in appropriate media designed to reach all constituents. Each user (constituent) will be required to agree to abide by this *BCF Computer and Information Systems Policy*.

Acceptance Signature: _____ Date: _____