

Christian Fellowship Center and Academy Information Systems Acceptable Use Policy

1.0 Overview

Christian Fellowship Center and Academy Leadership's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Christian Fellowship Center and Academy's established culture of openness, trust and integrity. Christian Fellowship Center and Academy Leadership is committed to protecting Christian Fellowship Center and Academy employees, member's, students and the community 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, WWW browsing, and FTP, are the property of Christian Fellowship Center and Academy. These systems are to be used for church/school purposes in serving the interests of the church/school, and of our members, students and visitors in the course of normal operations.

Effective security is a team effort involving the participation and support of every Christian Fellowship Center and Academy's computer user 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 Christian Fellowship Center. These rules are in place to protect the computer user and Christian Fellowship Center and Academy. Inappropriate use exposes Christian Fellowship Center and Academy to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other computer users at Christian Fellowship Center and Academy, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Christian Fellowship Center and Academy.

4.0 Policy

4.1 General Use and Ownership

1. While Christian Fellowship Center and Academy network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the organization's systems remains the property of Christian Fellowship Center and Academy. Because of the need to protect Christian Fellowship Center and Academy's network, the leadership cannot guarantee the confidentiality of information stored on any network device belonging to Christian Fellowship Center and Academy.
2. Users are responsible for exercising good judgment regarding the reasonableness of personal use. In the absence of such policies, users should be guided by departmental policies on personal use, and if there is any uncertainty, users should consult their supervisor or leader.
3. For security and network maintenance purposes, authorized individuals within Christian Fellowship Center and Academy may monitor equipment, systems and network traffic at any time. Christian Fellowship Center and Academy 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. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly; user level passwords should be changed every three months.

2. All hosts used by the employee that are connected to the Christian Fellowship Center and Academy Internet/Intranet/Extranet, whether owned by the user or Christian Fellowship Center and Academy, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.
3. Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Users may be exempted from these restrictions during the course of their legitimate job responsibilities

Under no circumstances is a user of Christian Fellowship Center and Academy equipment authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Christian Fellowship Center and Academy -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.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of 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 Christian Fellowship Center.
2. 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 Christian Fellowship Center and Academy or the end user does not have an active license is strictly prohibited.
3. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
4. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
5. Using a Christian Fellowship Center and Academy 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.
6. Making fraudulent offers of products, items, or services originating from any Christian Fellowship Center and Academy account.
7. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user 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.
8. Port scanning or security scanning is expressly prohibited unless prior notification to Christian Fellowship Center and Academy's Network Administrator is made.
9. Executing any form of network monitoring which will intercept data not intended for the user's host, unless this activity is a part of the Network Administrator's normal job/duty.
10. Circumventing user authentication or security of any host, network or account.
11. Interfering with or denying service to any user other than the users' host (for example, denial of service attack).
12. 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.
13. Providing information about, or lists of, Christian Fellowship Center and Academy members, students to parties outside Christian Fellowship Center and Academy.

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 Christian Fellowship Center and Academy's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Christian Fellowship Center and Academy or connected via Christian Fellowship Center and Academy's network.
7. Posting the same or similar non-church/school-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.4. Social Networking (Blogging, Facebook, Twitter, and MySpace)

1. Social media activities should be kept to a minimum and should not interfere with work commitments.
2. Your online presence reflects the Christian Fellowship Center and Academy. Be aware that your actions captured via images, posts, or comments can reflect that of Christian Fellowship Center and Academy.
3. Social networking, which includes (but not limited to) blogging, Facebook, Twitter, and MySpace by users, whether using Christian Fellowship Center and Academy's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Christian Fellowship Center and Academy's systems to engage in social networking is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Christian Fellowship Center and Academy's policy, and is not detrimental to Christian Fellowship Center and Academy's best interests. All forms of social networking from Christian Fellowship Center and Academy's systems are also subject to monitoring.
4. Users shall not engage in any social networking that may harm or tarnish the image, reputation and/or goodwill of Christian Fellowship Center and Academy and/or any of its members.

5.0 Enforcement

Any user/member found to have violated this policy may be subject to disciplinary action

6.0 Definitions

Term	Definition
<i>Blogging</i>	Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.
<i>Spam</i>	Unauthorized and/or unsolicited electronic mass mailings.
<i>Host</i>	Desktop Computer, Laptop, or electronic device connected to the network.

7.0 Revision History

Name	Revision	Notes	Date
Info-Systems-Acceptable-Use- Rev-pa.doc	Rev. PA	Author: Ben Diehl Supervisor of Technology	March 17, 2008
Info-Systems-Acceptable-Use- Rev-A.doc	Rev A	Final Revision: Sharon Herbster Administrator	June 15, 2010

Final Draft