TRINITYFELLOWSHIP

INFORMATION TECHNOLOGY POLICY

This document sets forth Trinity Fellowship (the "Company") policies with regard to computer, e-mail, and Internet usage, including access to, review or disclosure of e-mail messages sent or received by Company employees, and Internet access and usage. Trinity Fellowship reserves the right to modify or update these policies at any time. **Use of the computer system, e-mail system, or the Internet in violation of these policies or other Company policies can result in disciplinary action, including termination of employment.**

Trinity Fellowship's computer systems, network, iPads, phone system, cell phone, e-mail system, Internet access, and any other device (collectively called the "Computer System" in this document) are provided to employees at the expense of Trinity Fellowship to assist them in carrying out Company business and performing their job responsibilities and duties.

Trinity Fellowship owns, maintains, and is responsible for the Computer System. In the course of their jobs, employees may use the Computer System to communicate internally with co-workers or externally with clients, consultants, vendors, and other business acquaintances. Trinity Fellowship provides its employees with the Computer System to facilitate business communications and to enhance employee productivity. As with the telephone, there may be occasion to use the Computer System for personal purposes. Personal use is permitted if it does not interfere with job performance, consume significant resources, give rise to more than nominal additional costs, or interfere with the activities of other employees. Under no circumstances shall the Computer System be used for personal financial gain, to solicit others for activities unrelated to Trinity Fellowship's business, or in connection with political campaigns or lobbying.

1. Access and Review of E-Mail Communications and Internet Usage

Trinity Fellowship treats all messages sent, received, or stored in the e-mail system as business messages.

Trinity Fellowship has the ability to access, review, copy, and delete any messages sent, received, or stored on the e-mail system. Trinity Fellowship also has the ability to access deleted messages in certain circumstances. Trinity Fellowship also has the capability to monitor employees' Internet usage, including the time spent on-line and the sites accessed.

Trinity Fellowship reserves the right to access, review, copy, or delete all e-mail messages of any kind for any purpose and to disclose them to any party (inside or outside of Trinity Fellowship). Trinity Fellowship reserves the right to review all

computer files and communications, and to monitor its employees' use of the Internet, to maintain system integrity and ensure that users are using the system appropriately, responsibly, and in accordance with Company policies and procedures.

If Company employees use the e-mail system to transmit personal messages, those messages will be treated in the same way as business-related messages. In other words, Trinity Fellowship reserves the right to access, review, copy, delete, or disclose personal messages for any purpose. Accordingly, employees should not use the e-mail system to send, receive, or store any messages that they wish to keep private. Employees should treat the e-mail system like a shared file system, and expect that any messages sent, received, or stored in the system (or on hard drives) will be available for review by any authorized representative of Trinity Fellowship for any purpose.

WHEN USING THE COMPUTER SYSTEM, WHETHER FOR BUSINESS PURPOSES OR PERSONAL USE, EMPLOYEES AND OTHERS SHOULD HAVE NO EXPECTATION THAT ANY COMMUNICATION OR INFORMATION TRANSMITTED OVER COMPANY FACILITIES OR STORED ON COMPANY-OWNED COMPUTERS IS OR WILL REMAIN PRIVATE.

2. E-Mail Etiquette

Please bear in mind that your e-mail messages may be read by someone other than the person to whom you send them, and may someday have to be disclosed to outside parties or a court in connection with litigation. Accordingly, please ensure that your messages are courteous, professional, and businesslike. Remember that e-mail messages, once sent, are usually irretrievable. Be sensitive to the fact that, in the absence of an explanation, e-mail messages may be ambiguous and convey the wrong impression. This is of particular concern when a message is forwarded to multiple recipients. Instead of sending messages quickly without adequate review, consider printing the messages and reading them before distribution to ensure the content is appropriate.

3. Storing and Deleting E-Mail Messages

Trinity Fellowship strongly discourages the storage of a large quantity of e-mail messages for a number of reasons. First, because e-mail messages frequently contain confidential information, limiting the number, distribution, and availability of such messages is desirable. Second, retention of messages consumes storage space on the network server and personal computer hard disks, and can slow the performance of both the network and individual personal computers. Finally, if Trinity Fellowship needs to search the network server, back-up tapes, or individual hard disks for genuinely important documents, the search will be more efficient if there are fewer files to search.

Accordingly, employees should promptly delete any e-mail messages they send or receive that no longer require action or are not necessary to an ongoing project. Employees should audit their stored e-mail messages periodically to identify messages that are no longer needed and should delete those messages.

Because e-mail transmissions will not be stored permanently on the Computer System, it is important that employees make and file hard (paper) copies of those incoming and outgoing e-mail messages they want to keep, much as they would ordinarily keep and file copies of correspondence. These messages may also be archived on the employee's own computer, where they will be stored off of the network. Note, however, that these messages are not backed up as part of the network.

4. Subscriptions to Mailing Lists and Discussion Groups

No employee shall subscribe to any e-mail mailing list or discussion group, unless the subject and purpose of the list or group is directly related to the employee's job duties. Any person subscribing to such a list or group must advise the Information Technology Department or other appropriate personnel of the name of the list, and must provide a copy of the subscription confirmation received from the list or group.

5. Permitted and Prohibited Uses

a. Use Primarily for Business Purposes

The computer system, e-mail system, and Internet access may be used to support and promote Trinity Fellowship business objectives. The use of computers and Internet access through the Trinity Fellowship system is a privilege, not a right, and may be revoked.

Therefore, for example, employees may not:

- play games on the computers;
- intentionally waste limited computer resources;
- engage in activities that disrupt the workplace business environment;
- engage in actions that damage computers, computer systems, or computer networks;
- use the Computer System for commercial purposes, for personal gain or profit, or to engage in illegal activity;
- use the e-mail system to copy and/or transmit any documents, software, or other information protected by copyright laws; or
- use the Computer System in violation of Company policies, including the computer, e-mail and internet usage policies described in this Agreement.

Use of the computer system, e-mail system, or the Internet in violation of these or other Company policies can result in disciplinary action, including termination of employment.

b. E-Mail Use

E-mail messages, whether created inside Trinity Fellowship, or outside Trinity Fellowship and transmitted within Trinity Fellowship, or from Trinity Fellowship to

other sites, can generate claims of defamation, harassment, and discrimination. Therefore, employees may not:

- Use the e-mail system to engage in any communications that are in violation of any policy, including Trinity Fellowship's equal employment opportunity or sexual harassment policies; or
- Use the e-mail system to transmit or display:
    - defamatory, sexually explicit, obscene, offensive or harassing messages, images, cartoons, jokes, or pictures;
    - messages that disclose personal information without authorization;
    - unwelcome propositions, requests for dates, or love letters;
    - profanity, obscenity, slander, or libel;
    - ethnic, religious, or racial slurs; or
    - any other message that could be construed as harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, disability, or religious or political beliefs.

c. Internet Use

An employee accessing the Internet from a Company site is responsible for all online activities that take place through the use of his or her log-in and password. When using another organization's networks or computing resources, employees must comply with the rules appropriate for that network.

Those with Internet access privileges may not:

- access inappropriate websites (including those involving gambling, pornography, or obscene materials, or those that display defamatory, sexually explicit, obscene, offensive, or harassing messages, images, cartoons, jokes, or pictures, display profanity, obscenity, slander, libel, or ethnic, religious, or racial slurs);
- obligate Trinity Fellowship financially to any commercial websites;
- use the Internet from a Company site to engage in the practice of moonlighting or for any commercial purposes, advertising, or other similar activities.

d. Reporting Violations of Policy

Any employee who becomes aware that the use of the Computer System has resulted in a violation of these policies or other Company policies should promptly report such violations to the Information Technology Department or other appropriate personnel. **The failure of any employee to report a violation of these or other Company policies relating to a breach of system security or confidentiality may result in disciplinary action, including termination of employment.**

6. Computer System Security

a. Importance of System Security

Trinity Fellowship has an obligation to maintain the confidentiality of its own and its customer information. As a consequence, all users of the Computer System must take steps to ensure the security of the system and to maintain the confidentiality of all information on the system or communicated through the use of the system. Each employee is responsible for what happens under his or her log-in name. **Violations of security policies are considered serious violations of company policy, and can result in disciplinary action, including termination of employment.**

b. System Access

Password and user log-on IDs are unique to each authorized user and will be assigned by the Information Technology Department. Passwords must be kept private. They should not be shared, coded into programs, or written down.

In order to protect against dissemination of confidential information, employees should not access their e-mail messages for the first time in the presence of others. E-mail windows should not be left open on the screen when the computer is unattended. E-mail passwords (and other computer passwords) should be changed regularly.

Computers should not be left on if you will be away from your desk, and should never be left on overnight. You should always log out of the system if you will be away from your computer.

c. Computer Viruses

Computer viruses can be injected into the system through the receipt of e-mails, e-mail attachments, or files from other systems. Use particular care when opening files attached to e-mails from unknown senders. Employees must pay attention to and strictly comply with all warnings and instructions of the Information Technology Department relating to viruses. Employees must immediately inform the Information Technology Department of the presence of any virus on any Company computer. Any computer that is infected or suspected of being infected must immediately be disconnected from the network to reduce the risk of spreading a virus. Employees are prohibited from disabling or interfering with any virus-scanning software installed on their system.

d. Installing or Downloading Software

The Information Technology Department must approve and install all software on any Company computer system. No employee may download software without the approval of the Information Technology Department. If authorized to download software, employees must comply with all restrictions and procedures for downloading software, including mandatory virus scanning and detection procedures. Employees must inform the Information Technology Department of any virus, configuration change, or different behavior of a computer or application, especially after the addition of new software to the environment.

All employees must obey and follow all licensing agreements and procedures with regard to the use and installation of all software. The Information Technology Department staff will inspect computers periodically to verify that all software has been approved and licensed properly.

7. Confidentiality of Communications

a. Importance of Confidentiality

Employees must exercise a greater degree of caution in transmitting information through e-mail than they take with other means of communicating information (e.g., written memoranda, letters, or phone calls) because of both the reduced human effort required to redistribute such information and security considerations on the Internet. Confidential information of Trinity Fellowship or its customers should never be transmitted or forwarded to outside individuals or companies not authorized to receive that information.

Always use care in addressing e-mail messages to make sure that messages are not inadvertently sent to outsiders or to the wrong person inside Trinity Fellowship. In particular, employees should exercise care when using distribution lists to make sure that all addressees are appropriate recipients of the information. Lists are not always kept current and individuals using lists should take measures to ensure that the lists are up to date. Do not routinely forward messages containing confidential information to multiple parties unless there is a clear business need to do so.

TRINITYFELLOWSHIP

ACKNOWLEDGMENT

INFORMATION TECHNOLOGY POLICY

I acknowledge that I have read and will abide by Trinity Fellowship policies regarding computer systems, network, iPads, phone system, cell phones, e-mail system, Internet access, and any other device (collectively called the "Computer System" in this document). In particular, I understand:

1. That Trinity Fellowship has the complete authorization to monitor my computer usage, e-mail communications, and Internet usage;
2. That Trinity Fellowship may monitor on a routine and/or special case basis;
3. That Trinity Fellowship may elect not to monitor and may not strictly enforce its computer policies, but that any such election or determination not to enforce any policy strictly will not be construed as a waiver of Trinity Fellowship's right to enforce its policies in any particular situation; and
4. That any violation by me of the Trinity Fellowship information technology policy may result in a loss of access, disciplinary action (including termination), or other legal action.

_____

Employee's Signature

_____

Employee's Name

_____

Date