INTERNET-COMPUTER USAGE POLICY

COMPUTER NETWORK AND INTERNET ACCESS POLICY

Disclaimer

The Internet is a constantly growing worldwide network of computers and servers that contain millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. Users are further cautioned that it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. Additionally, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive content. Employees and users (herein referred to as "Users," or "User") accessing the Internet do so at their own risk and understand and agree that Harvest City Church, (herein referred to as "Organization," or "The Organization") is not responsible for material viewed or downloaded by users from the Internet. To minimize these risks, your use of the Internet at The Organization is governed by the following policy:

Permitted Use of Internet and Organization computer network

The computer network is the property of The Organization and is to be used for legitimate corporate purposes. Users are provided access to the computer network to assist them in the performance of their jobs. Additionally, certain Users may also be provided with access to the Internet through the computer network. All Users have a responsibility to use The Organization's computer resources and the Internet in a professional, lawful and ethical manner. Abuse of the computer network or the Internet may result in disciplinary action, including possible termination and civil and/or criminal liability.

Computer Network Use Limitations

PROHIBITED ACTIVITIES. Without prior written permission from The Organization, The Organization's computer network may not be used to disseminate, view or store commercial or personal advertisements, solicitations, promotions, destructive code (e.g., viruses, Trojan horse programs, etc.) or any other unauthorized materials. Occasional limited appropriate personal use of the computer is permitted if such use does not:

a. Interfere with the User's or any other employee's job performance;

b. Have an undue effect on the computer or Organization network's performance;

c. Violate any other policies, provisions, guidelines or standards of this agreement or any other of the Organization;

d. Use The Organization's Computer Systems to access, transmit, store or publish information about The Organization's employees, members, vendors, partners, etc. or The Organization's specific business information that is not in the public domain to any party outside The Organization without proper authorization.

Further, at all times users are responsible for the professional, ethical and lawful use of the computer system. Personal use of the computer is a privilege that may be revoked at any time.

ILLEGAL COPYING. Users may not illegally copy material protected under copyright law or make that material available to others for copying. You are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material you wish to download or copy. You may not agree to a license or download any material for which a registration fee is charged without first obtaining the permission of the Organization's IT department.

COMMUNICATION OF TRADE SECRETS. Unless expressly authorized to do so, Users are prohibited from sending, transmitting, or otherwise distributing proprietary information, data, trade secrets or other confidential information belonging to The Organization. Unauthorized dissemination of such material may result in severe disciplinary action as well as substantial civil and criminal penalties under Provincial and Federal laws.

Duty not to Waste or Damage Computer Resources

ACCESSING THE INTERNET. To ensure security, avoid the spread of viruses and malware, and to maintain The Organization's Internet Usage Policies or Acceptable Use Policies, employees may only access the Internet through a computer attached to The Organization's network and approved Internet firewall or other security device(s). Bypassing The Organization's computer network security by accessing the Internet directly, without prior authorization from the Organization's IT Department, by personal connections such as (but not limited to) Cellular Networks, Internet Protocol (IP) Addresses other than IP addresses assigned by The Organization, Wimax, modems, or proxy avoidance techniques or by any other means is strictly prohibited.

FRIVOLOUS USE. Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all Users connected to the network have a responsibility to conserve these resources. As such, 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 or other social media, uploading or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the Internet.

VIRUS DETECTION. Files obtained from sources outside The Organization (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 Organization's computer network. Users should never download files from the Internet, accept e-mail attachments from outsiders, or use disks from non-Organization sources without first scanning the material with Organization-approved virus checking software. If you suspect that a virus has been introduced into The Organization's network, notify The Organization immediately.

WAIVER OF PRIVACY RIGHTS. User expressly waives any right of privacy in anything they create, store, post, send or receive using the Organization's computer equipment or Internet access. User consents to allow Organization personnel access to and review of all materials created, stored, sent or received by User through any Organization network or Internet connection.

MONITORING OF COMPUTER AND INTERNET USAGE. Employees are given computers and Internet access to assist them in the performance of their jobs. Employees should have no expectation of privacy in anything they create, store, post, send or receive using The Organization's computer equipment. The computers and computer network are the property of The Organization and may be used only for Organization purposes, although occasional limited appropriate personal use of the computer is permitted.

The Organization has the right to monitor, log and archive 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 via Email, IM & Chat & Social Networking. These monitoring actions will not be engaged without the express joint authorization of the Organization's Business Manager and Manager of the Organization's IT Services Department. The Organization will not use Key-logging software on employees' Organization-owned computers, or any software to read employee e-mail correspondence, gain access to an employee's Organization-owned computer or gain access to an employee's files located on The Organization's server/network unless suspicious activity is detected/reported which would warrant a search. The monitoring of activities will be used in a proactive manner to detect and act upon unauthorized access and illegal or unethical use of The Organization's Computer Systems.

Sharing of Passwords

Each User is given access to The Organization's application systems and network infrastructure based on the requirements of their specific roles and responsibilities. Because of this, access to specific information differs between each User. In a computing environment, the primary control for access to information and approval authorization limits are managed by the User's access name (Username) and password. The User is fully accountable for all activity within their own account and must never share their password(s) with anyone for any reason. If there is a perceived reason to justify the sharing of passwords, the User must contact the IT department and an acceptable solution will be determined and authorized.

Blocking Sites With Inappropriate Content

The Organization has the right to utilize hardware and software that makes it possible to identify and block access to Internet sites containing sexually explicit or other material deemed inappropriate in the workplace.

Blocking Sites With Non-productive Content

The Organization, if it deems necessary under certain circumstances, has the right to utilize hardware and software that makes it possible to identify and block access to Internet sites containing non-work-related content such as (but not limited to) Drug Abuse; Hacking; Illegal or Unethical Material; Discrimination; Violence; Proxy Avoidance; Plagiarism; Child Abuse; Alternative Beliefs; Adult Materials; Advocacy Organizations; Gambling; Extremist Groups; Nudity and Risqué Photos; Pornography; Tasteless Material; Weapons; Sexual Content; Sex Education; Alcohol; Tobacco; Lingerie and Swimsuit; Sports; Hunting; War Games; Online Gaming; Freeware and Software Downloads; File Sharing and Offsite Storage; Streaming Media; Peer-to-peer File Sharing; Internet

Radio or TV; Internet Telephone; Online Shopping; Malicious Websites; Phishing; SPAM; Advertising; Brokerage and Trading; Web-Based Personal Email; Entertainment; Arts and Culture; Education; Health and Wellness; Job Search; Medicine; News and Media; Social Networking; Political Organizations; Reference; Religion; Travel; Personal Vehicles; Dynamic Content; Folklore; Web Chat; Instant Messaging or IM; Newsgroups and Message Boards; Digital Postcards; Education; Restaurant or Dining; Personal Websites or Blogs; Content Servers; Domain Parking; Personal Privacy; Finance and Banking; Search Engines and Portals; Government and Legal Organizations; Web Hosting; Secure Sites; or Web-based Applications.

Acknowledgement of Understanding

I have read and agree to comply with the terms of this policy governing the use of The Organization's computer network. I understand that violation of this policy may result in disciplinary action, including possible termination and civil and criminal penalties.

Printed Name: _____

Signature: _____

Date: _____