Next Level Church Acceptable Use Policy of IT Equipment

Computer and Technology Resource Usage Policy NEXT LEVEL CHURCH provides a variety of electronic communications systems for use in carrying out its business. All communication and information transmitted by, received from or stored in these systems are the property of NEXT LEVEL CHURCH and, as such, are intended to be used for job-related purposes only.

The following summary guidelines regarding access to and disclosure of data on any NEXT LEVEL CHURCH electronic communication system will help you better determine how to use these systems in light of your own and the company's privacy and security concerns. The following are only summary guidelines; employees should contact the Information Technology (IT) department for more detailed information.

The IT department maintains the Computer and Technology Resource Usage Policy on behalf of NEXT LEVEL CHURCH. However, other departments may develop supplemental policies and controls to accommodate specific requirement so long as these policies do not compromise corporate policies and controls.

Monitoring: NEXT LEVEL CHURCH provides the network, personal computers, electronic mail and other communications devices for your use on company business. NEXT LEVEL CHURCH may access and disclose all data or messages stored on its systems or sent over its electronic mail system. NEXT LEVEL CHURCH reserves the right to monitor communication and data at any time, with or without notice, to ensure that company property is being used only for business purposes. The company also reserves the right to disclose the contents of messages for any purpose at its sole discretion. No monitoring or disclosure will occur without the direction of either the human resources department, or executive leadership, unless otherwise noted.

Retrieval: Notwithstanding the company's right to retrieve and read any e-mail messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorized to retrieve or read any e-mail messages that are not sent to them and cannot use a password, access a file, or retrieve any stored information unless authorized to do so.

Passwords: Initial passwords are assigned by the IT department and should not be given to other staff or persons outside the organization. Employees should change the provided passwords as soon as possible using the instructions provided by the IT staff. NEXT LEVEL CHURCH reserves the right to override any employee-selected passwords and/or codes. Employees are required to provide the company with any such codes or passwords to facilitate access as needed. Periodically, staff may be required to change their passwords. At no time should an NEXT LEVEL CHURCH employee allow a temporary, contractor or another employee use of their login. In the case where an employee does provide another person access to their account, they will be responsible for the actions of the individual using their account. Passwords should not be stored in computer data files, on the network, or be displayed openly at any workstation.

Message Content: The e-mail system is not to be used to solicit or proselytize for commercial ventures, outside organizations or other non-job-related solicitations. The system is not to be used to create any offensive or disruptive messages. Among those which are considered offensive are any messages which contain sexual implications, racial slurs, gender-specific comments or any other comment that offensively addresses someone's age, sexual orientation, national origin or disability. The organization’s overall employee manual or code of conduct shall be considered the prevailing authority in the event of possible misconduct.

Employees should note that any data and information on the system will not be deemed personal or private. In addition, the e-mail system may not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior authorization.

Legal Proceedings: Information sent by employees via the electronic mail system may be used in legal proceedings. Electronic mail messages are considered written communications and are potentially the subject of subpoena in

litigation. NEXT LEVEL CHURCH may inspect the contents of electronic mail messages in the course of an investigation, will respond to the legal process and will fulfill any legal obligations to third parties.

Physical Security: Access to computer rooms will be limited to staff who require access for the normal performance of their jobs. Computers with sensitive information installed on the local disk drive should be secured in a locked room or office during non-business hours. Equipment which is to be removed from NEXT LEVEL CHURCH property must be approved in advance with the IT department and an inventory of this equipment maintained by IT. All equipment removal from the premises by an individual must be documented, including the makes, manufacturers and serial numbers on an IT supplied system. If the employee leaves the organization, he or she must return the equipment to NEXT LEVEL CHURCH prior to the last day of employment.

Network Security: IT will monitor network security on a regular basis. Adequate information concerning network traffic and activity will be logged to ensure that breaches in network security can be detected. IT will also implement and maintain procedures to provide adequate protection from intrusion into NEXT LEVEL CHURCH's computer systems from external sources. No computer that is connected to the network can have stored, on its disk(s) or in its memory, information that would permit access to other parts of the network. Staff should not store personal, business, member or other credit card/account information, or passwords within word processing or other data documents.

Personal Computer Security: Only legally licensed software will be installed on NEXT LEVEL CHURCH computers. Users are expected to read, understand and conform to the license requirements of any software product(s) they use or install. Software cannot be copied or installed without the permission or involvement of the IT department. IT will configure all workstations with virus protection software, which should not be removed or disabled. Each employee is responsible for protecting their computer against virus attack by following IT guidelines for scanning all incoming communications and media, and by not disabling the anti-virus application installed on their workstation. All data disks and files entering or leaving NEXT LEVEL CHURCH should be scanned for viruses. All staff will log out of the network and turn their computers off before leaving the office at night. Staff should log off of the network when they will be away from their desk for an extended period.

Backup Procedures: All network resources are backed up nightly. Nightly backups are stored for one week, and a weekly tape will be stored for no more than five weeks. Data stored on the local PC drives is not routinely backed up. Staff working on especially crucial information are encouraged to backup these projects to disks which can be supplied by the IT department. Computer users will be responsible for ensuring that the data stored on their local machines is backed up as required by the owner.

Access to NEXT LEVEL CHURCH Computers: NEXT LEVEL CHURCH will provide computer accounts to all NEXT LEVEL CHURCH staff. External people who are determined to be strategically important to NEXT LEVEL CHURCH, such as temporary staff, volunteers, or contractors, will also be provided accounts as appropriate, on a case-by-case basis. The employee managing the temporary or contract staff assumes responsibility for the identification of access requirements and use of the account. Accounts will be revoked on request of the user or manager or when the employee terminates employment at NEXT LEVEL CHURCH.

Internet Use: The Internet is to be used for business purposes only. Employees with Internet access are expressly prohibited from accessing, viewing, downloading, or printing pornographic or other sexually explicit materials. In addition, employees should be mindful that there is no assurance that e-mail texts and attachments sent within the company and on the Internet will not be seen, accessed or intercepted by unauthorized parties.

Failure to comply with all components of the Computer and Technology Resource Usage Policy may result in disciplinary action up to and including termination of employment. If you do not understand any part of the policy, it is your responsibility to obtain clarification from your manager or the IT department.

Next Level Church Acceptable Use Policy of IT Equipment

Software Usage: Employees are expected to use the standard software provided by IT, or identify applications they need in the course of their work. Staff members are not permitted to download applications, demos or upgrades without the involvement of IT. Employees will use the standard e-mail system provided by NEXT LEVEL CHURCH for official e-mail communications, and should not install their own e-mail systems.

Failure to comply with all components of the Computer and Technology Resource Usage Policy may result in disciplinary action up to and including termination of employment. Any employee who does not understand any part of the policy is responsible for obtaining clarification from his or her manager or the IT department.

Unauthorized access to this computer system and software is prohibited by Title 18, United States Code, Section 1030, Fraud and Related Activity in Connection with Computers. , This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. , In the course of monitoring individuals improperly using this system, or in the case of system maintenance, the activities of authorized users may also be monitored. , Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

_____ _____

Signature of Employee Printed Name of Employee

_____ _____

Date Title