

Information Systems Policy

XYZChurch is striving to take advantage of various technologies designed to enhance productivity, promote sharing of information and facilitate both internal and external communications. As these technologies are implemented and made accessible, it is important to establish procedures regarding use. These are not intended as barriers to getting things done, but as boundaries to keep users and the organization from encountering various problems.

This policy applies to all XYZChurch church staff and all other authorized users of the global electronic mail and messaging infrastructure made available by XYZChurch, including Internet, Intranet and on-line access provider systems. Users are responsible for complying fully with this policy as stated, but XYZChurch reserves the right to modify this policy at any time, with or without prior notification. Violations could be the basis for staff member discipline or discharge.

Computers & Software

Ownership

The computer an employee is assigned for work is the property of XYZChurch. The unit, monitor, and related peripherals may not be removed from the premises unless the user is expressly authorized to do so by the Information Systems group. Alterations to computer hardware or the installation of additional peripheral items is not allowed unless approved by IS. Computer equipment assigned to you must be used for XYZChurch related purposes only. Upon separation, you must return all equipment in good working order that was provided to you during the course of your employment.

Non-XYZChurch Systems

For information security purposes, devices which are not the property of XYZChurch should never be connected to the XYZChurch network or any XYZChurch computers without the written permission of the Director of Information Systems. This includes all Firewire, USB, and DVI enabled devices which are not the property of XYZChurch. Support for hardware and software will be provided by the IS group for church-owned computers only.

Maintenance

All maintenance and repair work will be performed by the person authorized by XYZChurch's IS group. No outside vendor or any other third party is to be contacted for maintenance or repair work without the consent and prior notification of the Director of Information Systems.

Negligence

Staff will be required to replace or pay for the repair of any computer provided to them in the event the computer is stolen, misplaced or damaged, if it is determined that the loss or damage was caused by negligence. For the purpose of this policy, negligence is defined as knowingly causing or allowing to be caused the loss or damage of the computer or its peripherals. Please immediately report a loss or damage to any computer or equipment to IS.

Purchasing

It is the desire of the IS department to provide each staff member and department with the technological resources and tools needed based on job function. Since the IS group is accountable for the IS budget and provides strategic direction of the technology footprint, the choice of hardware and software (including suppliers and models) is at the sole discretion of Information Systems. All purchases and purchasing decisions of and for network connected devices are made by or in collaboration with the IS Department. This includes all hardware, software, and peripherals. Purchases not planned for in the annual budget planning process will be considered on a case by case basis by the Director of Information Systems.

Special Note on Laptops:

Any exception to the below eligibility criteria for laptops, any upgrades or replacement of lost, damaged, or stolen laptops must be approved in writing by the Director of Information Systems. The following criteria will determine the eligibility of a laptop:

- Annual budget approval
- Staff member's Director or Department Head (either core or campus specific)
- Required mobility as determined by the job description
- Network access required during daily meetings as determined by job description

Software

Additional software programs may not be installed by the user without the prior knowledge and approval of the IS group. Making copies of installed software for personal or home use is prohibited by almost all software licensing agreements. Under the Federal Copyright Law, software that is loaded on your computer hard disk may not be duplicated for use on any other computer unless you are granted that right from the software maker. Many products are serial numbered, and in most cases no two computers may have software with the same serial number. No software may be installed on XYZChurch computers by any staff member that is not licensed to XYZChurch by the manufacturer of the software.

Copyrights & Software Use

XYZChurch computer users must abide by applicable laws regarding duplication of

software and other electronic files including text, photography, video, music, and any file sharing.

Many computers have iTunes software installed on them. Staff who use iTunes or other music sharing platforms are expected to know and observe copyright laws regarding music sharing. Because staff computers are an asset of XYZChurch, music and other media residing on a XYZChurch computer is the property of XYZChurch. XYZChurch is under no obligation to return said music or de-authorize any content, regardless of nature, residing on a XYZChurch computer.

Lastly, the content residing on all computers must be in good taste, inoffensive to others, and most importantly, a reflection of our core values.

Security and Privacy

Access

Information Systems assigns each user a password in order to access the network and any relevant software. Passwords are intended to prevent unauthorized access to XYZChurch systems and thereby prevent loss or damage to the organization. Authorized users will be given a username consisting (in most cases) of your first name followed by the first initial of your last name, e.g. JohnS. Passwords must be at least 6 characters long. Other recommendations are using letter and number combinations as well as complex characters, e.g. *, /, \ etc. Users will be required to change their passwords every 90 days.

Please provide security for your computer through a password protected screen saver, and by locking your door when you are not in your office.

Users should not share password information with, or provide computer or network access to other staff, volunteers, or outside parties.

Additionally, you may not access files, data or directories that are not related to the performance of your assigned duties. The improper use (including the unauthorized review, dissemination, removal, installation, or alteration) of files, passwords, computer systems or programs owned by or licensed to XYZChurch is prohibited and could bring legal and disciplinary action.

Vandalism or Sabotage

Any activity by an individual that poses a threat (potential or real) to network operations, causes physical damage to any computer or to the network infrastructure, or results in the damage or loss of electronic information could bring legal and disciplinary action. Such

activity includes but is not limited to:

- Unauthorized deletion of files from the file server
- Unauthorized changes or deletions of all or part of any operating system software
- Unauthorized changes to any hardware or software network configuration
- Disruption of electrical power to any network device, computer, printer, or any other computer related item with the perceived intent of causing harm
- Alteration, theft, or damage of network servers, computers, printers, network hubs, network cabling, wiring closets, cameras, or any other network network devices or peripherals
- Alteration, theft, or damage of tapes, disks, memory sticks, or any other electronic or digital media with the perceived intent of causing harm
- Unauthorized entrance into the XYZChurch data center

Privacy

Each user is assigned a folder area on the file server for storing information created or used while engaged in normal work activity. Although network security settings are in place to prevent access by other staff into a user's folder area, any information a user considers to be of a personal, confidential nature should not be created on XYZChurch computers, transmitted over the XYZChurch network, or stored on the file system.

XYZChurch is not responsible for any access, disclosure or loss of such information. In situations where there is a legitimate work need to access information residing in a user's folder area, Information Systems is authorized, but not obligated, to provide access to the users department supervisor or a staff member designated by the users department supervisor. Network storage directories established for the storage of files that need to be accessed by other staff within the department or other departments have the same requirements as outlined above.

Church Data Management Systems

Users must take particular care not to disseminate confidential church information to unauthorized users. Use of the system for the communication of personal, private or confidential information is not appropriate. If incidental or occasional personal use of the system is made, such use is still subject to the same policies and procedures set out in this policy.

Internet & Email

Representing XYZChurch

Please remember, you are an ambassador of Christ and XYZChurch when blogging, posting comments of any type, or when participating in interactive conversations like instant messaging and chat conferences. Due to the fluidity of the Internet, it is important to

consider the potential impact of connecting XYZChurch's name with any personal information you choose to put on the Internet. Inappropriate use could damage XYZChurch's reputation, and may lead to disciplinary action.

Monitoring

Web browsing, Instant Messaging, FTP, interactive conversations online, email, and other types of network use should be limited to church related activities. All Internet use and content browsing will be monitored by Information Systems for inappropriate content, use, and interaction using both tools on the network and placed on your computer.

Notifications will be sent to Human Resources by the IS team within 24 hours of discovery of questionable activity. Any activity which could prove to be illegal will be reported to the FBI within 24 hours of discovery. The use of XYZChurch systems for the transmissions of offensive comments, discriminatory language, vulgarities and/or obscenities is strictly prohibited. Discovery of these activities could bring legal and disciplinary action.

Email

Email has the very positive attribute of affording quick and efficient communication. On the other hand its "faceless" nature tends to foster an attitude of anonymity and informality that could lead to improper use. While it is our intention to treat communications via email as confidential to the greatest extent possible, it may be necessary for IS and authorized supervisors to access your communications during the normal course of business in cases not necessarily warranted by questionable activities outlined above. Accordingly, you do not have any right to privacy in communications via Electronic Media at XYZChurch. The following are intended to promote good e-mail habits and define the appropriate use of both internal and Internet e-mail.

- Staff Emails – Before you address an e-mail to all of the staff, or a large number of staff, it must have approval from a DLT member, the Director of Information Systems, or the Director of Human Resources. The subject matter should reflect a matter of importance to all staff on all campuses.
- Reasonable Use – email should primarily be used to communicate work related information e-mail may also be used to convey information that is not strictly work related yet has a bearing upon the staff and staff related functions.
- Security – Each staff member must ensure that internal messages meant only for staff are sent to the appropriate recipients. System users should not leave the system on and available to unauthorized users.

Remember

- Email messages can be misdirected by the sender or by an error in the message routing process.
- Internet and Intranet e-mails rely on public networks that are outside company

control. Service levels and confidentiality cannot be guaranteed.

- Once sent, e-mail messages cannot be retrieved or removed from a recipient's mailbox.

Prohibited Uses of E-mail

- Sensitive or proprietary information communicated by electronic message to internal employees may not be retransmitted externally without the permission of the department director and/or a member of the executive team.
- Revealing any confidential internal e-mail names and passwords of church e-mail users to anyone outside the church, including people who request such information over the telephone and seem to have a legitimate reason for asking. All such requests must be referred to the IT Network Administrator for a response.
- Requests for access to the contents of e-mail in order to respond to legal process, such as subpoenas, or for purposes of representing the church in connection with any actual or threatened litigation, investigation or claim must be brought to the attention of a member of the Executive team. Unauthorized access of e-mail messages is a serious violation of church policy and may be grounds for staff member discipline or dismissal.
- Content (text and/or graphics) that may constitute harassment, or be considered discriminatory, obscene, derogatory or excessively personal, whether intended to be serious or humorous. Failure to adhere to this policy may result in disciplinary action.
- Sending files and/or attachments in violation of copyright laws or licensing agreements.
- Sending messages prohibited or restricted by government security laws or regulations.
- Sending chain letters.
- Personal commercial activities
- Promotion of political positions or actions
- Solicitation of any type, except for church-sanctioned activities

Personal Use of Phone & Mail

Please use discretion in using XYZChurch telephones when making local personal calls. Personal use of telephones for long-distance and toll calls is not permitted. You will be required to reimburse XYZChurch for any charges that may result from personal use of the telephone.