CONTINUING RESOLUTION

CR12.05.N10. COMPUTER AND ELECTRONIC MEDIA USAGE GUIDELINES

WHEREAS, this congregation is committed to the ministry of Jesus Christ through all possible means, including electronic technologies; and

WHEREAS, computer technologies and information management systems are a tool for churches that wish to grow their ministries; and

WHEREAS, to better serve our members and provide our employees and volunteers with the best tools to do their jobs, this congregation has already made substantial investments in computer, church management, and electronic communication systems; and

WHEREAS, this congregation makes available to our workforce access to one or more forms of electronic media and services, including, but not limited to, computers, e-mail, telephones, voicemail, fax machines, external electronic bulletin boards, wire services, online services, intranet, internet, and the world wide web; and

WHEREAS, this congregation encourages the use of the above media and associated services to facilitate and support church ministry/business because they can make communications more efficient and effective and because they are valuable sources of information about members and attendees, vendors, technology, and new products and services; and

WHEREAS, the electronic media and services provided by this congregation are church property and users of such equipment and services have the responsibility to use these resources in a professional, ethical, and lawful manner;

THEREFORE, BE IT RESOLVED that Trinity Evangelical Lutheran Church, Latrobe, PA (hereafter church) allow our employees, volunteers and staff the use of our church computers and electronic communications media. The use of these church resources and facilities is governed by the Congregation Council (C12.05.) which sets forth the following guidelines and policies for users of these services. No guideline or policy can lay down rules to cover every possible situation. Instead, these guidelines and policies express this congregation's philosophy and set forth general principles when using electronic media and services provided by the church.

1. PROHIBITED COMMUNICATIONS

Electronic media can not be used for knowingly transmitting, retrieving, or storing any communication that is:

a. Discriminatory or Harassing
b. Derogatory to an individual or group
c. Obscene, sexually explicit or pornographic
d. Defamatory or threatening
e. In violation of any license governing the use of software
f. Illegal or unethical
g. Contrary to church's ministry/business interests

2. PERSONAL OR COMMERCIAL USE

The computers, electronic media and services provided by the church are primarily for ministry/business use to assist employees and volunteers in the performance of their jobs. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal, non-business/non-ministry purposes is understandable and acceptable, and all such use should be done in a manner that does not negatively affect the systems' use for their ministry/business purposes. However, employees and volunteers are expected to demonstrate a sense of responsibility and not abuse this privilege.

Likewise, it is understood that many consider their private businesses as a ministry, providing products and services to Christians and the community at-large. However, it is inappropriate and prohibited by this congregation to abuse resources or information (e.g., e-mail lists, web sites, online forums, e-mail addresses, phone numbers, and personal addresses) provided by the church for promoting private businesses.

3. ACCESS TO COMMUNICATIONS

Generally, electronic information created and/or communicated by an employee or volunteer using e-mail, word processing, utility programs, spreadsheets, voicemail, telephones, internet, and bulletin board system access, and similar electronic media is not reviewed by the church. However, the following conditions should be noted.

a. The church may routinely gather logs for electronic activities or monitor employee communications directly, e.g., telephone numbers dialed, sites accessed, call length, and time at which calls are made, for the purposes of:
   i) Cost analysis
   ii) Resource allocation
   iii) Optimum technical management of information resources
   iv) Detecting patterns of use that indicate employees or volunteers are violating church guidelines or engaging in illegal activity.

b. The church reserves the right, at its discretion, to review any user's electronic files and messages stored on or sent from church computers and servers to the extent necessary to ensure electronic media and services are being used in compliance with the law, this continuing resolution, and other governance documents of this congregation.

c. Employees and volunteers should not assume electronic communications are completely private. Accordingly, if they have sensitive information to transmit, they should use other means.

4. SOFTWARE

To prevent computer viruses from being transmitted through the church's computer system, downloading of any unauthorized software to church computers or servers is strictly prohibited. Only software registered or licensed through the church may be downloaded. Employees and volunteers should contact the church's System Administrator (ref. most recent continuing resolution C12.04.B.) if they have any questions.

5. SECURITY/APPROPRIATE USE

a. Employees and volunteers must respect the confidentiality of other individuals' electronic communications. Except in cases in which explicit authorization has been granted by an Officer (ref. Constitution article C11.01.) or called ministry staff of this congregation, employees and volunteers are prohibited from engaging in, or attempting to engage in:
   i) Monitoring or intercepting the files or electronic communications of other employees and volunteers to third parties
   ii) Hacking or obtaining access to systems or accounts they are not authorized to use
   iii) Using other people's log-ins or passwords
   iv) Breaching, testing, or monitoring computer or network security measures

b. No e-mail or other electronic communications can be sent that attempt to hide the identity of the sender or represent the sender as someone else.

c. Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.

d. Anyone obtaining electronic access to other companies' or individuals' materials must respect all copyrights and can not copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.

e. To prevent computer viruses from being transmitted through the church's computer system, users should not open e-mails sent from unfamiliar or suspect sources. It is best practice to view the content of all e-mails using view windows before opening or to delete without opening.

6. ENCRYPTION

Password protected documents or administrative access controls are preferred methods of protecting sensitive information. However, employees can use encryption software supplied by the church's System Administrator for purposes of safeguarding sensitive or confidential ministry/business information. Employees who use encryption on files stored on a church computer must provide the church's System Administrator with a sealed hard copy record (to be retained in a secure location) of all the passwords and/or encryption keys necessary to access the encrypted files.

7. PARTICIPATION IN ONLINE FOURMS

The church recognizes that participation in some forums might be important to the performance of an employee's or volunteer's ministry or job. (For instance, an employee or volunteer might find the answer to a technical problem by consulting members of a group devoted to the technical issue.) However, users should remember that any messages or information sent on a church-provided system to one or more individuals via an electronic network (e.g., internet mailing lists, bulletin boards, and online services) are statements identifiable and attributable to this church.

8. VIOLATIONS

Any user of church computers or services who abuses the privilege of their access in violation of this continuing resolution will be subject to corrective action, including possible termination of employment, legal action, and criminal liability.

9. MISCELLANEA

a. Usage of this congregation's computers or services automatically implies acceptance of the guidelines and policies established in this continuing resolution.

b. This continuing resolution is subject to change by the Congregation Council in accordance with ***C18.02.** of the Constitution of this Congregation. In the event of any revision to this continuing resolution, reasonable means to communicate the revised guidelines to our users, including posting of the revised continuing resolution on the congregation's website, will be employed.