INTERNET USAGE POLICY

The Internet has transformed our way of connecting with others—and has escalated communication problems within congregations. Check with your local school district or companies for samples of how they deal with Internet use by their staff and volunteers.

SAMPLE POLICY TEXT BELOW

⇓

Internet Use

The ability to communicate electronically has led to increasingly complex issues regarding privacy, security of confidential information, boundary violations, and the potential for harassment (based on gender, race and other categories).

1.   The congregation is responsible for the content of messages sent and received on church employees' computing devices, including cell phones, computers, laptops, or tablets. That responsibility includes all messages and attachments, written on equipment owned by the congregation and/or processed using the congregation's computer network. Every computing device owned by the congregation or established for its use shall have a protective login code that is carefully protected.

2.   The congregation is also responsible for the websites visited on its computing devices and/or processed using the congregation's computer network. If necessary, protective measures should be in place to block inappropriate internet sites.

3.   Since internet access and use are intended for the congregation's business, employees and volunteers shall have no right or expectation of privacy in any internet activity or e-mail messages using the church equipment or networks. The church reserves the right to review any internet activity of any employee or volunteer at any time for any reason and to monitor, audit, delete and read e-mail or social media messages received or sent on congregational computing devices or through the congregation's network. Staff and volunteers should be especially cautious about any personal information revealed in social media, even if they think their privacy settings on Facebook or other accounts are sufficient.

4.   E-mail users should treat all unsolicited e-mail with suspicion, particularly e-mail received from the Internet. If the user is unsure of the authenticity and integrity of an e-mail, it should be deleted immediately. Anonymous e-mails shall be ignored and deleted.

5.   Since electronic messages are subject are subject to the same level of review as paper documents regarding legal retention periods, the congregation should establish standards, procedures and techniques to ensure proper retention and disposal of e-mail.