INTERNET SECURITY AND SOCIAL MEDIA BOUNDARIES

by: **TERRACE CRAWFORD**

GENERAL NETWORK & INTERNET SAFETY

Church computers can greatly enhance the efficiency of administration, and the Internet creates exciting ways ways to communicate and advance your ministry. But the digital age also presents a variety of risks that churches need to consider and address.

Keep Your Network Safe

Threats to your computer network range from computer viruses, security breaches, lightning damage, and hardware failure, to power outages and unintentional harm from inexperienced users. To minimize such risks, take the following precautions.

Install three types of security software, including a firewall to prevent unauthorized Internet users from accessing your computer network. Use an anti-spyware program to identify and combat "spyware." Spyware is a category of malicious software designed to watch what users do with their computers and to send this information to a hacker over the Internet. Also run antivirus software to protect against computer viruses and worms. Update the virus definition files frequently, and run a scan of the hard drive after each update.

Finally, educate all computer users to never open attachments from unknown sources and to virus-scan all files that are opened or downloaded, even from a trusted source.

Additional security measures include using passwords to protect against unauthorized access to your computer network and to secure documents containing sensitive information.

Good passwords should be at least eight characters in length and contain both letters and numbers in random order.

If your organization uses Windows, keep Windows software up to date. For former employees and volunteers, discontinue computer network access. And be sure to install surge-protection devices in your facility to guard against sudden electrical surges that can damage computer equipment.

Maintaining Data Backup

Despite the best precautions, your church may still experience a loss of data. That's why consistent data backup is so crucial. For instance, regularly back up computer files to another media such as magnetic tapes, "zip" disks, CD-ROMs, or flash drives. Be especially careful to back up database files such as membership files, spreadsheet and financial reporting files, and large documents generated by staff or volunteers. Remind staff members to regularly back up their work. Store a copy of the backed-up data off-site, and keep installation CDs for software programs stored in a secure location.

Operating a Safe Website and Safe Searching

Church websites have become exciting communication tools with dynamic capabilities such as streaming media broadcasts or podcasts, online event registration, and online financial transactions. When operating a website, churches should consider the following:

•**Maintain the name.** Consider reserving all variations of your church domain name (.org, .com, .net) to avoid confusion and to keep others with ill intent from establishing alternative websites at those addresses. Have all domains point to your church's main website address.

•**Protect privacy.** Develop a privacy notice that addresses whether and how your church collects information from the website. Become familiar with the Children's Online Privacy Protection Act (COPPA). Even if COPPA does not apply to your organization, many churches voluntarily comply with COPPA to protect the personal information of children under age 13.

•**Obtain permission to publish.** Photographs or videos of individuals should not be posted on the church website without their permission. Express written permission should be obtained for any photos accompanied by identifying information such as name and residence. Even with parental permission, photos of minors should not be accompanied by any personally identifying information.

•**Comply with copyrights.** The church may be held liable for any unauthorized use of copyrighted or trademarked works, photos, images, music, logos, and other material housed on its website. Copyright and trademark laws must be followed. Likewise, to protect the church's works from unauthorized duplication or use, the church should consider including a copyright notice on its website.

•**Maintain control.** Consider appointing a person or team to oversee the website's content and style. All pages on the site should be known and approved by the team. Guidelines should be in place before considering pages such as discussion boards, newsgroups, and file or photo sharing.

•**Monitor.** Appoint a designated staff or lay person to regularly view the website looking for functionality problems, broken links, irregularities, inappropriate postings, unauthorized pages, and vandalism or hacking. That individual (and a backup) should have the authority and know-how to take down the website or individual pages, if the need arises.

•**Conducting commerce.** Financial transactions over the Internet warrant special security consideration such as the Secure Sockets Layer (SSL) protocol that provides a secure encrypted connection between an individual's web browser and the church's web server. In addition, before selling items over the Internet, consult with the church's accountant regarding any sales tax and Unrelated Business Income Tax (UBIT) implications in your state.

Internet and E-Mail Usage

Internet and e-mail programs can be highly effective in furthering the mission of the church. However, abuses of the Internet and e-mail can lessen productivity or, in the worst cases, have a devastating impact on the church's ministry. To help head off problems with Internet and email usage, do the following:

•Establish an electronic communications policy that clearly sets out the church's expectations on such issues as the following:

•Distinguish business versus personal use of the Internet, e-mail, and phones
•Determine church ownership of computers, programs, and other computer-related items
the church's not providing a right or expectation of privacy in the use of the
Internet, e-mail, or voice mail the church's right to monitor or inspect computers, equipment, and messages guidance on downloading files and/or software programs, the specifying of prohibited conduct, proper and improper use of mass communication techniques such as e-mail blasts or phone tree messaging.
•All users of church computers should be made aware of the electronic communications policy and adhere to it.
•Use filtering and/or accountability software. Filtering software can prevent access to certain websites that contain objectionable content, while accountability programs track Internet usage activity.
•Assign responsibility to a designated person to periodically review the usage logs for church Internet activity.

SOCIAL MEDIA BOUNDARIES

OPPORTUNITIES AND EXPECTATIONS FOR MINISTRY

Social media is a form of communication, used for connection, relationship, conversation, advocacy, evangelism, debate, news, and information, and a means of seeking and offering support. It may not be everyone's preferred form of communication, but it is an important method, and we have an expectation that most ministers can, should and will utilize social media in their ministries in ways that enhance ministry, enrich lives, and reflect individual and organizational values.

At the same time, the 24/7 "always on" nature of social media creates expectations related to the accessibility of leaders and ministers, what news and information ministers see on social media, and confidential spaces. Some of those expectations may be reasonable; many, however, are implicit and will need to be named in order to evaluate their appropriateness for any particular ministry setting.

Questions of liability also must not be ignored. In many states, ministers are mandatory reporters and are bound by law to report certain actions or behaviors to secular authorities. Social media is not considered a private space, and nothing revealed on social media can be construed as confidential information.

BOUNDARY CONSIDERATIONS

In all social media activities basic boundary considerations must be made. Who controls the information shared on social media? Whose story is it to tell? Who else may need to know this information? Are there additional concerns, such as mandatory reporting obligations? Do policies regarding transparency include provisions for periodic review of an authorized minister's social media interactions to ensure both confidentiality and appropriate behaviors?

RECOMMENDATIONS –

GENERAL GUIDELINES FOR SAFE SEARCH& USAGE

1. A synonym for "pastor" is "parson," which comes from the same root as "person." Authorized ministers should see themselves as embodying whole, authentic and integrated personhood, and should strive to be the same person online that they are in other spaces. Guidelines for social media consumption and participation should mirror any minister's personal rule for life, and should be in cooperation with this denomination.

2. At the same time, ministers are professionals by virtue of their authorization (regardless of their particular employment), so they should strive to balance this authenticity with appropriateness, and maintain appropriate boundaries around one's personal and professional

spheres. An authorized user should exercise great care in sharing and speaking on social media, even on personal accounts.

3. Users must remember that social media is not confidential space. Even in "closed" groups or private communications, it's possible for information to be copied and shared in other spaces. Ministers should assume that anything they share on social media may be shared by others, even if the minister maintains strong privacy settings.

4. At the same time, users should not assume that personal information they have read about or from others on social media is public because it is online or that it may be freely shared with others.

5. Before posting, authorized user should consider whether social media is an appropriate medium for the message. In communicating with individuals over social media, ministers should also consider whether they would convey this same message in the same way in face-to-face conversation with the parishioner. Ministers should also avoid posting vague messages that invite rumor or speculation, particularly (though not exclusively) on the part of those they serve.

6. A minister's voice is often considered the voice of the church, and social media content from the minister may be viewed as church policy or as representing a church position.

7. Authorized ministers should maintain a current list of pages, groups and accounts associated with the church or ministry setting, along with any relevant passwords and the names of all administrators. This list should always be accessible to another member of the ministry setting staff or governing board.

RECOMMENDATIONS –

SAFE SEARCH& USAGE (MINOR TO ADULT RELATIONSHIPS)

1. With regard to a congregation's Safe Conduct policies, digital space should be regulated in similar ways to other church space: there must be more than one adult who administrates church-related sites, closed groups, list serves, etc.; adults should not be in private, one-on-one conversations with youth; the congregation should periodically monitor the social media interactions of the adult leaders (authorized ministers, employed or volunteer youth workers, etc.).

2. Adults, including leaders/ministers, should not submit "friend" requests to minors or youth. Youth may request friendships with adults, and adults should discern the level of contact they should maintain with youth prior to responding to these requests.

3. If an authorized minister or other youth worker (employed or volunteer) chooses to accept friend requests from minors or youth who are associated with their community of faith, we recommend that other adults within the same community of faith have access to that adult's profile and correspondence.

4. When and where available, authorized users and other youth workers may choose to create separate personal and professional profiles on networking sites to create a line of privacy. Authorized users are still held accountable for what is shared in their personal and professional accounts.

5. Authorized users and other youth workers (employed or volunteer) who choose to accept friend requests from minors or youth should use all applicable privacy settings to shield youth from any age-inappropriate content that may exist within the authorized minister or youth worker's profile.

6. All youth and adults should be informed that any communication sent via digital methods (email, social networking site notes or posts, etc.) is not confidential and may be reported or shared with others.

7. Authorized ministers who work directly with youth are encouraged to establish church-sponsored digital communication groups to maintain contact with youth members. These groups should include other adult leaders (employed, volunteer, or parents).

8. We strongly recommend "closed" but not "hidden" groups be used for youth groups. These groups should have both youth and adult administrators, and only those known to the group should be permitted access to the groups.

9. Covenants should be created to govern what is appropriate and inappropriate content to be placed and displayed in the online group for a youth group.

10. Youth groups should decide within their covenant whether or not their social networking site groups are open to parents of current members. Additionally, former youth members and adult leaders of youth groups, due to departure, removal or loss of eligibility (aged out of program) should be removed from digital communication youth groups (Facebook groups, list serves, etc.).

11. Any inappropriate material that is not covered by mandatory reporting laws should be deleted from the social networking group or site. Any material that is covered by mandatory reporting laws should be reported to the authorized minister (within your community of faith), documented for church records, and then deleted from the social networking group or site.

12. Any content that details inappropriate behavior (outside of the bounds of the established covenant) during a church sponsored event or activity should be addressed by authorized ministers, other youth workers and parents.

13. Parents should be informed that content appearing on youth pages or in groups that are NOT sponsored by the church are not within the purview of authorized ministers or other youth workers. Authorized ministers and youth workers should not participate in any youth page or group that is not sponsored by the church.

14. Adults should refrain from initiating video chats with youth, and if initiated by youth, should include another person, preferably an adult.

15. All transcripts of online text chats, video chats, blogs or video blogs should be saved when possible.

16. All authorized ministers and youth workers should consider the content and nature of any post that will be read by or visible to youth. Authorized ministers and youth workers' (including employed and volunteer) voices are often considered the voice of the church, and all such content may be viewed as church policy or as a church opinion.

17. Authorized ministers and youth workers may only post non-identifying pictures of minor children on church-related social media with written permission of the family. Authorized ministers and youth workers may not post identifying images of minor children on their personal social media pages.

18. Additionally, pictures or video may only be shared with the express permission of the owner of the image (the copyright holder) to use the image.

RECOMMENDATIONS FOR TRANSITIONS –

PRIOR TO A DEPARTURE FROM A MINISTRY SETTING

Prior to departure from a ministry setting, authorized ministers should create and share a social media transition plan as part of overall ministry transition, and commit to following through on that plan as part of their departure from the ministry setting. This plan should take into account the following recommendations:

1. Prior to departure, the authorized minister should pass along administrator duties, remove their own administrator status, and share password information to someone else in the ministry setting for all ministry-related pages, groups and accounts.

2. Authorized ministers should discern carefully whether they will unfriend/unfollow parishioners and others with whom they've had a pastoral relationship or move them to a more restricted list.

3. Ministers should prioritize the needs of the ministry setting and whoever will follow in ministerial leadership over their own desires to maintain relationship (or the desires of parishioners to stay in contact). Ministers should also be consistent: the practice should be to either unfriend/unfollow everyone from that setting, or move them all to a restricted list. Authorized ministers should communicate this policy to their ministry setting so that there is no confusion.

4. Authorized ministers must refrain from providing pastoral care through digital communication after the end date of their contract/call/covenant with their community of faith. Continuing to provide pastoral care through social media interferes with the ministry of one's successor and is typically a violation of the Minister's Code of Ethics.

5. Following a period of 1-3 years, authorized ministers should discern whether they will change their privacy settings and/or begin to accept friend requests of former parishioners. Ministers

should not initiate friend/follow requests, and they must continue to refrain from providing pastoral care through digital communication to former parishioners.

Release Form

I, the undersigned, do hereby consent and agree that the [Photographer's Name] Audio/Visual & Social Media Ministry has the right to take photographs of me to use these in any and all media, now or hereafter known, and exclusively for [church name here] I further consent that my name and identity may be revealed therein or by descriptive text or commentary if agreed consensually.

I do hereby release to [Photographer's Name], has all rights to exhibit this work in print and electronic form publicly or privately and to market and sell copies. I waive any rights, claims, or interest I may have to control the use of my identity or likeness in whatever media used.

I understand that there will be no financial or other remuneration for recording me, either for initial or subsequent re-posts.

I also understand that [Photographer's Name] is not responsible for any expense or liability incurred as a result of my participation in this recording, including medical expenses due to any sickness or injury incurred as a result.

I represent that I am at least 18 years of age, have read and understand the foregoing statement, and am competent to execute this agreement.

Name/Person(s)

Witness for the undersigned

Signature Date