10 Things
Every Church Administrator Should Know About...

Cyber Liability

Brotherhood Mutual®
Insurance Company

6400 Brotherhood Way, P.O. Box 2227, Fort Wayne, IN 46801-2227 ■ 800.333.3735 ■ brotherhoodmutual.com

1. Website Privacy Policy

Visitors to your ministry's website trust you to protect their personal information. A website privacy policy is essential for explaining why you collect personal information and how you use it. It is important to make clear that your online privacy applies only to your ministry's website, not to websites that you may link to from your site. Your website privacy policy should address the following six core topics:

- **List the types of information you collect.** Does your website ask users for their name, address, phone number, and email address? What about debit and credit card numbers? Your privacy policy should specifically state the types of information you collect and why.
- **Describe your methods of collecting information.** Is information collected automatically when users visit your website (e.g., via "cookies"), or do you collect information through fillable forms?
- **State your purpose for collecting information.** Why does your ministry collect personal information from users? Your answer may be "to further the purpose of the ministry by facilitating communication between the user and others who attend." If you are collecting financial information, your policy should state specifically how the data will be used.
- **Specify if and how you share information.** Beware of well-intentioned but inaccurate policy statements, such as "we will not share your information with any third party." Does your ministry share information with a related organization, such as a school or camp? Do you use cloud data backup or a vendor for processing electronic tithes? If so, you are sharing data, and your ministry's privacy policy should reflect this.
- **Describe the ways you secure information.** Do you work with networking and website programming professionals to ensure that your ministry's website uses industry-standard security protocols, firewalls, and encryption programs? Ensuring that these safeguards are in place is important, especially if your ministry handles financial information.
- **If your website targets young users, ensure legal compliance.** If your ministry's website, or even a portion of it, is directed at children under the age of 13, the Child Online Privacy Protection Act (COPPA) likely applies to your website. COPPA protects the personal information of children under age 13 by requiring website owners to post a compliant privacy policy and obtain parental consent before collecting information. Consult the Federal Trade Commission's resource, "Children's Online Privacy Protection Rule: A Six-Step Compliance Plan" and your local attorney.

Need a form?

See this sample *Online Privacy Form* and this free article entitled *"Does Your Website Need a Privacy Policy?"* from BrotherhoodMutual.com.

2. Network Security: Wi-Fi

Free wireless Internet offered in a church context might be appreciated by members and guests who want to look up Scripture on their smart phones or tweet quotes from the sermon. However, an unfiltered wireless Internet connection can be used to download copyrighted or inappropriate materials or even to steal information from computers on your church's network. If your wireless Internet is not protected by a password, those near your building might be able to access or exploit it at any time. To protect your ministry, consider the following:

- **Install a content filter.** Your church could be held responsible for certain illegal activities done on its network by guests. To protect your church, members, and visitors, employ a content filter to block inappropriate websites from use.
- **Protect your network with passwords.** Create complex Wi-Fi passwords and administrative passwords. Change your administrative computer password at least every six months, and consider changing your Wi-Fi password every week.
- **Establish terms of use.** Another way to help regulate Internet usage is to require all visitors to agree to an Internet usage policy before using your church's Wi-Fi. Consider asking visitors to sign a paper release form, or provide a digital consent form as users sign on to your network. Key policy features might include:
  - o Prohibiting any actions inconsistent with your ministry's beliefs. These might include online gambling, online bullying or harassment, accessing obscene content, or downloading pirated content.
  - o Requiring all who access your network to be at least 18 years old or else supervised by an adult. An agreement signed by someone under the age of 18 is generally not enforceable.
  - o Requiring visitors to use up-to-date antivirus software.
  - o Advising visitors to avoid sharing sensitive information over your network.
  - o Posting a "hold-harmless" clause, notifying users that your church is not responsible for damage to electronic devices or software, or the loss or theft of personal information. Users should be advised to browse the Internet at their own risk.

Strive to create a cyber-safe culture that encourages your staff, members, and guests to click and browse carefully, whether at church or at home.

Need a form?

Download the *Sample Wi-Fi Terms and Conditions* from Brotherhood Mutual's website to help you get a start on your own. Also, see this related article, *Protect Computer Networks When Offering Free Wi-Fi*.

3. Network Security: Connected Devices

Offering free Wi-Fi can open the door to data thieves. Here are some simple measures your church can implement to protect your ministry staff's connected devices.

- **Establish two distinct networks.** As a first step, make sure your church provides two networks, one public and one private. Share your church's public Wi-Fi password as freely as your policy allows, but take precautions to ensure that your private network password is never divulged outside of staff circles.
- **Connect staff devices to your private network, only.** Your staff should never connect computers, phones, tablets, or other devices containing sensitive information (e.g., financial information, sensitive communications with members, notes from counseling sessions) to your church's public network.
- **Secure office and personal devices.** The increased number of connected devices in modern church offices poses new security risks. Not only should these devices be kept on a private network, but access to these devices also must be closely regulated. Keep church offices locked when they are not in use to prevent unauthorized access.
- **Dispose of office devices safely.** When your ministry retires an old copier, fax machine, computer, or external hard drive—whether by recycling it, returning it at the end of its lease, trading it in for a newer model or selling the device secondhand—make sure the data on the device is not left intact. A manufacturer, dealer, or service provider typically gives options for safe data recovery, overwriting, or disposal.

Need more information?

For a related resource, see *"Include Copiers in Data Security Plans,"* an article from Brotherhood Mutual's Safety Library.

4. Data Protection Measures

Help your ministry avert many common cyber liability risks by implementing these security features.

- **Encrypt data.** When encryption is activated on a device, data is scrambled before it is stored in the machine's memory. Without a decryption key, encrypted data can only be recovered with high-level expertise and extensive computational resources.
- **Overwrite data.** Some office equipment, such as copy machines, offer overwriting as a scheduled cleanup task. The U.S. Bureau of Consumer Protection recommends overwriting the entire hard drive on a copy machine at least once a month. The more frequently this is done, the lower the likelihood of information being compromised.
- **Secure data with passwords, passcode locks, and traditional locks.** Many data thefts are low-tech crimes of opportunity. Installing passwords and passcodes on all of your devices is a great way to avert these threats. Keep computers and devices behind locked doors when not in use.
- **Install firewalls.** Hardware and software firewalls are another excellent way to safeguard against unauthorized access to your computer network.
- **Back up data.** One solid backup option is to save your computer's files to an external hard drive each month and store the hard drive in a safe deposit box or other secure, off-site location. As an alternative, your church might subscribe to a cloud backup service. In this case, choosing a reputable vendor that will maintain the security of your data is of utmost importance.

Taking these measures will greatly improve the security of your ministry's data.

Need a checklist?
Download the *Cyber Security Checklist* from BrotherhoodMutual.com.

5. Cyber Threat Management and Best Practices

By implementing a few best practices, your church office staff can do its part to monitor and maintain network security.

- **Closely monitor pulse indicators.** Staff should be vigilant in watching for the following signs, which may indicate that your network has been compromised.
  - o Computers and devices "freeze up" or "crash" more frequently than usual.
  - o Computers and devices suddenly take longer than normal to process basic commands.
  - o Pop-up advertisements frequently and randomly appear on users' screens, even when they are not surfing the Internet.
  - o The initial search page on users' Internet browsers changes, or users suddenly notice new toolbars in their browser windows.
- **Implement preventative measures.** Consider implementing the following precautions.
  - o Equip computers and other devices with software to block spyware, viruses, and ads.
  - o Scan computers weekly for malicious software.
  - o Set your ministry's Internet browsers on a high security setting.
  - o Update your ministry devices' operating systems, antivirus software, and Internet browsers in a timely manner.
  - o Monitor financial accounts closely.
  - o Warn computer users in your office to guard against phishing attempts, which occur when someone masquerading as a trustworthy entity requests sensitive information via email. Avoid sending personal information or login credentials by email as a general rule. Take particular caution when a sender, claiming to be a familiar company or service, requests information they should already have on file.
  - o Advise users to only enter login information online when they see a padlock in their address bar indicating Secure Socket Layer (SSL) encryption.
- **Prepare data breach response measures.** If your church's sensitive data is ever stolen, your ministry should have a plan in place for how it will respond.
  - o Find an experienced, trustworthy IT professional to serve as a security consultant and to investigate any cyber attack that may occur.
  - o Prepare a sample notification letter, which would be used in the event of a data breach to notify individuals that their personal information was stolen.
  - o Make a list of state agencies to contact if your ministry encounters a suspected scam or believes its data was stolen.
  - o Familiarize yourself with the cyber breach coverages that your insurance company offers, and keep your agent's contact information accessible at all times.

Want more information?

See this related resource, *"Protect Ministry Data and Computers,"* from Brotherhood Mutual's Safety Library.

6. Electronic Tithes, Financial Data Security

Electronic tithing offers a convenient, confidential way to donate money. If your church is contemplating this option, consider these tips.

- **Find a reputable vendor.** Many churches that accept electronic tithes choose to work with a reputable vendor to avoid hassle. Here are some tips to consider when looking for a vendor to process your tithes:
  - o Check the Better Business Bureau website, which features helpful business reviews and ratings.
  - o Ask for referrals from churches that work with the vendor.
  - o Ensure that the vendor uses Secure Socket Layer (SSL) encryption, which protects information from online thieves. When a site has an SSL Certificate, a padlock appears on the donor's Internet browser bar, indicating the transaction is secure.
  - o Check into the company's data security measures.
  - o Verify that your vendor complies with Payment Card Industry (PCI) Date Security Standards. PCI standards are guidelines that help keep financial information secure on the Internet.
  - o Ask your ministry's attorney to review any vendor agreement before church leaders sign it.
- **Take precautions with in-house processing and local data storage.** For churches that process tithes in-house, one key issue to consider is the storage of financial information. For example, any time a church maintains a record of its donors' credit card numbers or bank information, your ministry becomes responsible for guarding that information. If someone were to steal credit card information and run up fraudulent charges, your church could be legally obligated to pay for the damages. Even if no fraudulent charges were made, your church might be required to notify all of its donors, which costs time and money and might compromise trust levels among your members.
- **Establish a tithing policy.** Adopt a policy that lays out basic guidelines for donations. For example, determine which forms of payment your church will accept. Some churches choose not to accept donations via credit card, opting instead for e-checks and bank drafts.

Want more information?

See page 5 of *The Deacon's Bench, Winter 2013* for an article on electronic tithing.

7. Treatment of Prayer Requests and Personal Data

Here are some suggestions for communicating church news digitally and maintaining your church's prayer ministry without offending prayer recipients or breaking the law:

- **Secure consent.** Individuals have the right to share virtually anything regarding their own health. However, your church's social media administrator or the organizer of your email prayer chain may be restricted from disclosing an individual's medical status without the individual's express permission. The solution is to ask permission. Keep in mind that information shared on the Web tends leave a permanent record, even after deletion.
- **Acquire permission in writing, when possible.** Verbal permission is often easiest to secure, yet written permission provides stronger legal protection. Consider creating a template email or paper form for members to return to you confirming their permission to share information.
- **Keep it simple.** Even with a prayer recipient's consent, it's best to keep health-related information general. A notice that says "Sue Smith has been admitted to the hospital, and we pray for a speedy recovery" is better than "Sue Smith suffers from debilitating panic attacks and has been hospitalized. Please pray for her."
- **Defer to a spokesperson.** Some churches avoid both the problem of obtaining consent and that of determining how much detail to share by designating a relative or close friend who has agreed to serve as spokesperson. The spokesperson can decide how much detail to release and to whom. This person is often in a better position than the church to know how much information to share.
- **Consideration for employees.** Churches should be particularly cautious about disclosing employees' health-related information. The failing health or absence of a church staff member tends to be widely noticed, and can lead to well-intentioned questions. These questions are typically directed at church staff members, who may know confidential details of their co-worker's medical status from internal announcements or even the church's healthcare plan. Health-related information should only be disclosed in non-specific terms and with express permission from the staff member.

Need more information?

Read *"Prayer Lists: How to Protect Privacy,"* an article from Brotherhood Mutual's Safety Library.

8. Social Media

Many churches find social media useful in staying connected with those who participate in their ministries and in reaching out to the broader community. If your ministry has a social media presence, here are some tips to help guide your efforts:

- **Designate a team.** Task a small group of page administrators with posting entries on your ministry's social media pages. Team members should take shifts monitoring these pages and respond quickly when comments or questions are posted to show concern and responsiveness. Train team members how to handle sensitive issues, such as negative feedback, emergency situations, and obscene content.
- **Handle sensitive responses offline.** Some conversations should be handled in a private, offline setting. If someone posts regarding a negative experience or situation that involves sensitive information, offer to resolve the issue in a private meeting or phone call. If a comment includes an allegation of improper conduct, follow your ministry's normal procedure for investigating, reporting, and dealing with the issue. Also, train team members to recognize types of content that must be reported to law enforcement if discovered.
- **Address acceptable (and unacceptable) content.** Establish expectations by posting a social media policy for your page.
    - o Define types of content that will not be tolerated, such as advertisements, spam, and obscene material. Instruct page administrators to delete content that violates your policy.
    - o Have your social media policy approved by a locally licensed attorney. This helps ensure that your policy follows all applicable laws.
    - o Include a disclaimer on your ministry's social media page outlining your ministry's expectations for interactions and terms for removing content. The disclaimer can also tell visitors that your ministry assumes no liability for damages related to your ministry's social media page.
    - o Reserve the right to use content posted by visitors, such as compliments about a pastor's sermon, in other church publications.
- **Decide what to post.** Content should support your organization's overall goals. Examples include sharing inspiring Bible verses, photos, or videos to help your audience walk closer with God; giving the public a sneak peek at your worship services through audio and video clips of recent sermons; posting invitations to ministry events; and updating your audience on the progress of outreach projects. However, avoid sharing sensitive information such as a member's medical details or other personal matters.
- **Get permission.** Even in the social media world of "shares" and "retweets," copyright infringement can cost thousands of dollars in fines. Get permission from the original source before posting photos or videos that aren't your ministry's original work.
- **Put your best foot forward.** Ensure that each of your ministry's posts is worded in a way that is clear and relatable to a wide audience. Use original, high-quality photos. To protect individuals' privacy, obtain a signed photo release form from each person who appears in a picture on your ministry's social media page. Children under the age of 18 should have release forms signed by parents or guardians. You also might consider disabling photo tagging on your ministry's page. Further, photos taken by smart phones may contain location information. Turning this feature off or removing location information can protect the privacy of those photographed. Grow your social media audience by encouraging congregants to engage with your page.

Need a form?

Visit BrotherhoodMutual.com for a free social media sample policy and disclaimer.

9. Digital Communications with Youth

Text-messaging may be students' preferred method of communication, but it's not always best. If your church uses text messages, email, and/or social media to connect with youth, take the following steps to keep everyone safe.

- **Print and distribute a general policy, specifying electronic communications parameters.** This policy should spell out your ministry's expectations for youth, staff members, and volunteers when it comes to texting, social media, and other forms of communication. Have the policy approved by a local attorney, and train your staff and volunteers to follow the policy. The training should outline the recommended practices, limitations, and legal parameters for texting and other forms of electronic communication within youth ministry.

- **Specify when young people can and cannot use their devices.** In your church's policy, consider restricting the use of cell phones and other personal devices during official youth activities. This not only will avoid distractions that often come with cell phones, but also will help protect your church against charges of negligent supervision, should a student communicate inappropriately—or even illegally—during a ministry activity.

- **Develop a youth communication policy.** Establish parameters for which platforms your youth are permitted to use. Determine what measures your staff members will take to ensure user privacy and safety, and how they will communicate openly with parents.

  - Require consent forms to be signed prior to allowing youth to participate in your ministry's electronic communications.

  - Make it clear that youth who violate your ministry's communication policy may lose communications privileges or be removed from your youth ministry program. Ministry leaders also should notify parents about policy violations.

  - Encourage youth leaders to send texts, emails, and other messages to a group (including parents) rather than to individuals. If one-to-one messaging occurs, ministry personnel should immediately report it to a supervisor or other adult leader. Youth workers and other adult leaders also may want to avoid friending or following students on social media.

  - Train youth workers who become aware of possible child abuse through electronic media to notify their supervisor so that the ministry can consult with its attorney and report abuse as the law requires.

  - Some ministries have found Facebook groups to be a useful forum for communication between meetings. To maximize privacy, it may be best to designate the group's privacy setting as "secret," so that only those invited to join are able to view its message board and member list. Parents can be added to the group for an extra layer of transparency.

- **Inform staff, volunteers, and youth group members about the dangers of sexting.** Explicit messages are not only emotionally damaging, but under some state laws, young people also can be charged with a sex crime for transmitting sexually explicit photos. Inform your staff of any legal duties they may have if they become aware of such activity, including the need to report it to law enforcement or child protective agencies.

- **Stay abreast of new technologies and social media platforms**. New social apps and personal tech devices pop up frequently. In this ever-changing digital environment, it is critical that youth leaders be aware of how students are communicating and address new risks as they appear.

Need a form?

See this *Youth Ministry Communication Policy* template from BrotherhoodMutual.com.

10. Copyright Issues

In light of today's penchant for quick, open communication, copyright issues have never been more complex, nor more important to understand. Use the following list as a starting point for understanding how to treat photos, music, videos, and streaming media content.

- **Understand the purpose of copyright laws.** Copyright laws are designed to protect intellectual property, such as photos, music, and videos, from being used without the express permission of the author or artist.
- **Understand what copyright protects.** The original author of a copyrighted work has the exclusive legal right to:
  - o Copy, print, or reprint their work.
  - o Record it or perform it publicly.
  - o Sell or distribute it.
  - o Revise, arrange, or transform it.
- **Know your legal options for using copyrighted works.** If your church wants to use creative works belong ing to someone else, there are several approaches your ministry can take to reduce the risk of copyright infringement.
  - o Obtain permission from the copyright owner. If you can't determine who owns the content, it's best not to use it.
  - o Purchase a blanket license. Blanket licenses allow churches to use thousands of copyrighted songs and motion pictures, but licenses have limits. Learn what a license includes before purchasing it.
  - o Understand fair use. A narrow exception to the copyright law is known as "fair use," the definition of which is very limited and subjective. Determining whether the fair use exception applies is difficult and should not be used as a common practice.

    Generally, courts have noted that use of copyrighted material is typically permitted for the purposes of scholarship, commentary, criticism, parody, news reporting, and research. However, copyright infringement can still occur, even when used for those purposes. According to the U.S. Copyright Office, courts generally will consider the use of a work as "fair use" when:

    - A small portion of the total work is used (no specific amount of a work is always permitted).
    - The work is used for a nonprofit cause.
    - The work comes from a factual rather than an artistic source (e.g., a map rather than music)
    - The original author suffers no financial loss as a result of the use.

    Typically, courts also will examine whether the original author was credited for producing the copyrighted material. However, simply crediting the original author alone will not protect you against infringement claims.

- Learn about the religious services exemption. The copyright act also entitles churches to a special exemption. It allows the "performance of a nondramatic literary or musical work or of a dramatic musical work of a religious nature, or display of a work, in the course of services at a place of worship or other religious assembly." This is a very limited exemption, and while this protection might be more predict able than "fair use," it still is much less reliable than using works purchased under a license.

- **Consider linking to content, rather than hosting it on your site.**
  - If you want to share a song, a video, or another piece of multimedia, consider linking to it rather than hosting it.
  - If you want to share the text of a poem, a passage from a commentary, or lyrics to a song that will be used in your Sunday service, consider providing a link to the desired text instead of posting it on your website.

- **Understand how copyright affects different media.**
  - Videos and pictures. Generally, you have the right to use photo and video material recorded in public places, as opposed to privately owned locations, but it's best to get permission.
  - Music. The religious services exemption provides protection for churches using certain copyrighted musical works in the context of a traditional, indoor worship service. It doesn't apply in other contexts (e.g., weddings, funerals, choral performances, retreats, outdoor events, telephone hold music, audio featured on your website). To be safe, it is wise to always purchase a license, or to create your own original music compositions and audio soundbites.
  - Text message. Depending on the terms and conditions of an individual's cellular carrier, message content may actually be owned by the carrier. However, if the individual who wrote the text message grants permission for use, the likelihood of litigation may be reduced.

- **Consult your attorney.** Seek legal counsel when making decisions regarding the use of copyrighted works.

Need more information?

Read *"Complying with Copyright Laws"* and *"Copyright Laws and Fair Use,"* articles from Brotherhood Mutual's Safety Library. Also refer to this sample Photo Use Agreement.

A commitment to meeting the needs of others with compassion is the call of every ministry. It's the passion that drives everything you do, and we understand why, because it's a passion we share. For us, protecting your ministry is more than a job—it's a commitment.

Ministry is your passion...
...We understand why.®

Brotherhood Mutual®
Insurance Company

Insuring America's churches and related ministries®

6400 Brotherhood Way, P.O. Box 2227, Fort Wayne, IN 46801-2227 ■ 800.333.3735 ■ brotherhoodmutual.com