Brotherhood Mutual®

10 Things

EVERY CHURCH ADMINISTRATOR
SHOULD KNOW ABOUT...

CYBER LIABILITY

Brotherhood Mutual®

10 Things EVERY CHURCH ADMINISTRATOR SHOULD KNOW ABOUT **CYBER LIABILITY**

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 from them, and how you use it. Your website privacy policy should address the following six core issues:

- **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.

Remember to clarify that your online privacy policy applies only to your ministry's website, not to websites that you may link to from your site. Be sure to have your policy reviewed and approved by a locally licensed attorney.

NEED A FORM?

See the sample *Online Privacy Form* on 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 help protect your ministry, consider taking the following steps:

- **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 administrative computer passwords at least every six months, and consider changing Wi-Fi passwords 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:
  - Prohibiting any actions inconsistent with your ministry's beliefs. These might include online gambling, online bullying and harassment, accessing obscene content, or downloading pirated content.
  - Requiring all who access your network to be at least 18 years old, or supervised by an adult. An agreement signed by someone under the age of 18 is generally not enforceable.
  - Requiring visitors to use up-to-date antivirus software.
  - Advise visitors to avoid sharing sensitive information over your network.
  - 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.

NEED A FORM?

Download the *Sample Wi-Fi Terms and Conditions* from Brotherhood Mutual's website to help you get started writing your own policy.

3. NETWORK SECURITY: CONNECTED DEVICES

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

- **ESTABLISH TWO DISTINCT NETWORKS.** As a first step, make sure your ministry provides two networks: one public and one private. Share your ministry'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 ministry's public network.

- **SECURE OFFICE AND PERSONAL DEVICES.** The multiplying number of connected devices in the modern ministry office poses new security risks. Not only should these devices be kept on a private network, but access to these devices also should be closely regulated. Keep offices locked when they are not in use to help prevent unauthorized access and theft.

- **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?

See *Include Copiers in Data Security Plans*, an article from BrotherhoodMutual.com.

4. DATA PROTECTION MEASURES

Help your ministry minimize 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 AND TRADITIONAL LOCKS.** Many data thefts are low-tech crimes of opportunity. Installing passwords 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 help safeguard against unauthorized access to your computer network.
- **BACK UP DATA.** One 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 ministry 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.

NEED A CHECKLIST?

Download the *Cyber Security Checklist* from BrotherhoodMutual.com.

5. CYBER THREAT MANAGEMENT AND BEST PRACTICES

When it comes to cyber security, one wrong click can put your ministry's data at risk. By implementing a few best practices, your ministry staff can do its part to monitor and maintain network security.

- **WATCH FOR SIGNS OF TROUBLE.** Staff members should be vigilant in watching for the following signs, which may indicate that your network has been compromised.
  - Computers and devices "freeze up" or "crash" more frequently than usual.
  - Computers and devices suddenly take longer than normal to process basic commands.
  - Pop-up advertisements frequently and randomly appear on users' screens, even when they are not surfing the Internet.
  - 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:
  - Equip computers and other devices with software to block spyware, viruses, and ads.
  - Scan computers weekly for malicious software.
  - Set your ministry's Internet browsers on a high security setting.
  - Update your ministry devices' operating systems, antivirus software, and Internet browsers in a timely manner.
  - Monitor financial accounts closely.
  - 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.
  - Users should 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.** Your ministry should have a plan in place for how it will respond if a data breach occurs.
  - Find an experienced, trustworthy IT professional to serve as a security consultant and to investigate a breach.
  - Prepare a sample notification letter, which would be used in the event of a data breach to notify individuals that their personal information was compromised.
  - Make a list of state agencies to contact if your ministry encounters a suspected scam or believes its data was stolen.
  - Ask your insurance agent to evaluate your insurance policy, looking specifically to make sure your ministry has adequate computer-related coverage.

WANT MORE INFORMATION?

See the article *Protect Ministry Data and Computers,* from BrotherhoodMutual.com.

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 process donations. Here are some tips to consider when looking for a vendor:
  - Check the Better Business Bureau website, which features helpful business reviews and ratings.
  - Ask for referrals from churches that work with the vendor.
  - Check into the company's data security measures. 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. Also, verify that the vendor complies with Payment Card Industry (PCI) Data Security Standards. PCI standards are guidelines that help keep financial information secure on the Internet.
  - Ask your ministry's attorney to review any agreement before signing it.
- **PROTECT SENSITIVE DATA.** For churches that process electronic tithes in-house, one key issue to consider is the storage of financial information. For example, any time a ministry maintains a record of its donors' credit card numbers or bank information, the ministry becomes responsible for guarding that information. If someone were to steal credit card information and run up fraudulent charges, the ministry could be legally obligated to pay for the damages. Even if no fraudulent charges are made, your church might be legally required to notify all of its donors about the data breach, which costs time and money and might diminish trust 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* safety newsletter, *Financial Controls* edition 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 while protecting privacy:

- **SECURE CONSENT.** Individuals have the right to share virtually anything regarding their own health. However, your ministry'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 ministries 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.** Ministries should be particularly cautious about disclosing employees' health-related information. The failing health or absence of a staff member tends to be widely noticed, and can lead to well-intentioned questions. These questions are typically directed at ministry 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.

WANT 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 on your ministry's social media pages. This team should take shifts monitoring the pages and respond quickly when comments or questions are posted. Train team members on how to handle such issues 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.

- **ADDRESS ACCEPTABLE (AND UNACCEPTABLE) CONTENT.** Establish expectations by posting a social media policy for your page. When drafting your policy, be sure to:
  - Define the types of content that will not be tolerated, such as advertisements, spam, and obscene material. Instruct page administrators to delete content that violates the policy.
  - 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.
  - Reserve the right to use content posted by visitors, such as compliments about a pastor's sermon, in other church publications.
  - Have your social media policy approved by a locally-licensed attorney. This helps ensure that the policy follows all applicable laws.

- **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 post 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?

Download the sample *Social Media Policy* from BrotherhoodMutual.com.

9. DIGITAL COMMUNICATIONS WITH YOUTH

Electronic messaging may be students' preferred method of communication, but there are serious risks involved. If your ministry uses text messages, email, or social media to connect with youth, create and follow an electronic communications policy to help keep everyone safe. Consider taking the following steps when creating your policy:

- **ESTABLISH GENERAL GUIDELINES.** Spell out the ministry's expectations for youth, staff members, and volunteers when it comes to texting, social media, and other forms of communication. Also, 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 young people to participate in your ministry's electronic communications.
  - Make it clear that students who violate your ministry's communication policy may lose communication privileges or be removed from your youth ministry program. Ministry leaders should notify parents about policy violations.
  - Create parameters for which platforms your youth are permitted to use while participating in ministry activities.
  - 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 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.
- **SPECIFY WHEN YOUNG PEOPLE CAN AND CANNOT USE THEIR DEVICES.** In your ministry'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.
- **EDUCATE ON THE DANGERS.** Inform staff members, 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.
- **UPDATE THE POLICY TO ADDRESS NEW TECHNOLOGIES.** 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.

Remember to have your youth communication policy approved by a locally licensed attorney. Train (and re-train) your staff and volunteers to follow the policy.

NEED A FORM?

See the sample *Youth Ministry Communication Policy* on BrotherhoodMutual.com.

10. COPYRIGHT ISSUES

In today's digital culture, sharing information is quick and easy. This convenience comes with an increased risk of copyright infringement, making copyright issues 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. The original author of a copyrighted work has the exclusive legal right to:
  - Copy, print, or reprint their work.
  - Record it or perform it publicly.
  - Sell or distribute it.
  - Revise, arrange, or transform it.
- **KNOW YOUR LEGAL OPTIONS.** If your church wants to use copyrighted material that belongs to someone else, there are several approaches that can help your ministry reduce the risk of copyright infringement.
  - **Obtain permission from the copyright owner.** If you can't determine who owns the content, it's best not to use it.
  - **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 making a purchase.
  - **Understand fair use.** "Fair use" is a narrow and complicated exception to copyright law. Claiming "fair use" of copyrighted material should not be a common practice.
  - **Use links instead of hosting on your site.** You may want to share a song, video, book passage, song lyrics, or another piece of multimedia on your website. If the content belongs to someone else, provide a link to the original content instead of posting it directly on your website.
- **UNDERSTAND HOW COPYRIGHT AFFECTS DIFFERENT MEDIA.**
  - **Music.** The "religious services exemption" provides protection for churches using copyrighted musical works in the context of a traditional, indoor worship service. In any other setting (e.g., weddings, funerals, choral performances, outdoor events, audio or streaming content featured on your website), purchase a license, or consider creating your own original music compositions and audio.
  - **Videos and photos.** Whether or not a copyright is indicated on a piece of visual art, it may be protected. Even photos and video on "public" social sites like Facebook, Flickr, and YouTube belong to the person who created the art. Get permission from the copyright holder, or opt for art that is in the public domain. If streaming or broadcasting church services online, remember that another license is often required to play, perform, or otherwise use any copyrighted video or photos in a recording or broadcast. Some churches choose to limit their broadcasts to sermons and other non-copyrighted content. Others receive permission or purchase licenses to use copyrighted material.
  - **Written works.** Avoid printing or otherwise displaying copyrighted written works in a group setting, such as a church newsletter or website, unless the ministry has permission from the author to do so. Poems that are credited to "anonymous" may be copyrighted, as well; an Internet search may help you find the original source of the work to ask for permission to use it.
- **CONSULT YOUR ATTORNEY.** Seek legal counsel when making major decisions regarding the use of copyrighted works.

NEED MORE INFORMATION?

Read *Copyright Laws and Fair Use,* an article from BrotherhoodMutual.com.