



Alabama Baptist  
STATE BOARD OF MISSIONS

## ***Helping Churches to Be Safer Places***

# **Preventing Adult Sexual Misconduct in Your Church**

(Revised 9/3/2019)

**This piece focuses on protecting the church against adult with adult sexual misconduct, especially as it could involve ministerial staff.**

There is a companion piece, *Protecting Children and Youth from Sexual Misconduct in Your Church*, which is available at [www.alsbom.org/safe](http://www.alsbom.org/safe) or 1.800.264.1225 , ext. 241 or 283.

**This resource is provided by the gifts of Alabama Baptists through the Cooperative Program.**

Prevent Sexual Misconduct: Pre-employment .....	3
Check background .....	3
Prevent Sexual Misconduct: Supervision .....	4
Set rules for counseling. ....	4
Counseling Guidelines .....	4
Churches should consider establishing guidelines of proper ethics and conduct. ....	4
Such guidelines could include: .....	4
Reported Adult Sexual Misconduct: Response .....	5
The Victim(s) .....	5
The Congregation .....	5
The Perpetrator .....	5
Appendix A .....	7
Background Checks .....	7
Appendix B.....	8
A Covenant of Ministerial Ethics .....	8
Appendix C.....	9
Set Rules for Youth and Children’s Ministers .....	9
Appendix D .....	10
Sample Sexual Harassment Policy .....	10
Appendix E.....	12
Church Computer Use Policy .....	12
Duty not to waste computer resources.....	12
Accessing the Internet .....	12
Frivolous use .....	12
Virus detection.....	12
No expectation of privacy.....	12
Waiver of privacy rights .....	12
Monitoring of computer and Internet usage .....	13
Church has the right to utilize blocking software.....	13
Acknowledgement of understanding .....	13
Appendix F.....	14
Sample Church Computer Network and Internet Access Sexual Misconduct Policy.....	14
Disclaimer .....	14
Permitted use of Internet and church computer network .....	14
Access .....	14
Computer network use limitations.....	14
Prohibited uses.....	14
Illegal copying.....	15
Communication of confidential and/or personal member information .....	15
Appendix G .....	16
Sample Church Internet Usage Policy.....	16
The two key tenants to this usage policy are: .....	16
Appendix H .....	19
Sample Social Media Policy .....	19
Use of Social Media .....	19
Social Media Guidelines .....	19
Appendix I.....	21
Social Media Practices for Ministers.....	21
Concerning adults .....	21
Concerning minors.....	21
Appendix J .....	22
Appropriate and Inappropriate Forms of Affection .....	22

*Employment and other laws are constantly evolving, and nothing contained herein should be considered legal advice. The reader should consult the church's attorney before carrying out any of the suggestions or adopting any of the policies contained herein.*

*This information is designed to help autonomous Baptist churches think through vital issues and formulate their own internal policies. This resource, like all past and present resources from the State Board of Missions, is not binding on local congregations which are entirely self-governing. Consult a qualified attorney when drafting your own policies.*

---

## Prevent Sexual Misconduct: **Pre-employment**

---

### **Check background**

1. Check references.
  - a) Carefully check at least five references when considering calling a minister. It is wise to check at least two that are not listed on the resume.
  - b) Excellent reference sources include associational missionaries in associations where the minister has served, former staff members who have worked with the prospective minister, and church and community leaders from a former church. While it is wise to contact the current employer, do not do so without agreement with the prospective minister.
2. Look for gaps in ministry service.
3. Conduct an interview.
  - a) Include the spouse in the interview.
  - b) Some questions to ask in the interview are:
    - Share your salvation experience.
    - Share your call-to-ministry experience.
    - The church requires a criminal background check. Do you have a problem with that? Is there anything that might be discovered in the background check that could affect the potential employment decision?
    - Do you have any faults of character or behavior that should be known by this committee?
  - c) During the interview, secure permission for conducting a criminal background check and credit check.

Conduct a criminal background check and a credit check. (See : Background Checks, on page 7.)

Churches should consider creating a covenant of ministerial ethics to provide accountability and prevent factual disclosure of misconduct. (See: "A Covenant of Ministerial Ethics" on page 8.)

---

## Prevent Sexual Misconduct: **Supervision**

---

### ***Set rules for counseling.***

#### ***Counseling Guidelines***

1. Put in writing and present to potential ministerial staff during pre-employment.
2. Offer only short-term counseling unless the church has a professional counselor on the staff. One or two sessions should suffice to assess the need for referral to a professional counselor. The minister(s) should develop a network of professional counselors to which referrals can be made. (Pathways Counseling, which is a part of the ministry of the Alabama Baptist Children's Homes and Family Ministries should be a primary referral).
3. Counseling sessions should be conducted only on church premises and when others are close by in the building.
4. The ministers should refrain from any speech or action that could be construed as sexual or romantic.
5. All information notes and records from counseling sessions should be secured and kept confidential.
6. Any violation of these procedures could result in discipline which, if warranted, could include termination.

### **Churches should consider establishing guidelines of proper ethics and conduct.**

#### ***Such guidelines could include:***

- 1) Rules for youth and children's ministers (See "Set Rules for Your Youth and Children's Ministers," Appendix C on page 9.)
- 2) A Sexual Harassment Policy (This is required by Federal Law, see "Sample Sexual Harassment Policy," Appendix D on page 10.)
- 3) A computer and Internet use policy (See "Church Computer Use Policy," Appendix E on page 12 and also see "Sample Baptist Church Computer Network and Internet Access Sexual Misconduct Policy," Appendix F on page 14.)
- 4) An appropriate amount of leave time for ministers and family.  
One contributing factor in ministerial misconduct is a high level of stress. Stress does not excuse misconduct, but it can explain why misbehavior occurs.
  - a) Give appropriate vacation time.
  - b) Have guidelines as to how vacation is to be used. Example: Vacation time is not to be used for revivals.
  - c) Require a minister to take one weekday off. The higher priority a minister places on spouse and family, the less likely there will be involvement in sexual misconduct.
- 5) Consider adopting guidelines for texting and social media use (See "Sample Social Media Policy," Appendix E on page 17.)

Social Media Practices for Ministers (See “Sample Social Media Policy,” Appendix H on page 19 and “Social Media Practices for Ministers,” Appendix I on page 21.)

A code of conduct on appropriate and inappropriate forms of affection. (See “Appropriate and Inappropriate Forms of Affection,” Appendix J on page 22.)

---

## **Reported Adult Sexual Misconduct: Response**

---

There are three areas of responsibility: the victim(s), the congregation, and the reported perpetrator.

### ***The Victim(s)***

- 1) Provide immediate attention to the victims(s).
- 2) There should be immediate contact from the pastor to provide pastoral care and to inform the victim(s) and their families of the planned process the church is taking.
- 3) Assign church members who are close to the victim(s) to provide immediate and long-term ministry.
- 4) Provide professional counseling support.
  - a) The church should pay the cost.
  - b) The counselor should be one acceptable to the victim(s).

Note: If the victim is a minor the immediate reporting is mandatory.

### ***The Congregation***

- 1) The pastor should not try to handle the situation alone. He should immediately involve a key lay leader such as the deacon chairman. The key lay leader should become a part of devising a strategy of response. If the pastor is the one accused, the lay leader should lead in the response process. Even if the church is a pastor/staff-led church, key lay leadership must be involved in dealing with this kind of crisis.
- 2) Contact outside sources for advice and counsel:
  - a) Associational Missionary.
  - b) State Board of Missions: Office of LeaderCare and Church Health. (See Contact us: page 22.)
  - c) Legal Counsel.
- 3) Contact the church’s insurance company.
- 4) A group of mature lay leaders—such as the deacons—should be fully informed and given permission to share correct information.
- 5) Inform the congregation when deemed necessary.

Tell the truth. That does not necessarily mean divulging all the details. The church should never be able to accuse its leadership of misinforming them. It is better to share nothing with the congregation than to tell them something misleading.

### ***The Perpetrator***

- 1) Inform the accused person of the allegations.
- 2) Inform the accused person of the process to be followed.

- a) During the time of the investigation, the accused should step down from the position held.
  - b) If the accused is a church employee, there should be compensation during the time of investigation.
  - c) If there is a confession or credible evidence of wrongdoing, the perpetrator should be given the option of a confession, preferably in a resignation letter. Caution: A public confession may be risky. The one confessing may stray from the agreed upon statement and make an emotional appeal for forgiveness and restoration to the employed position.
  - d) If there is a confession or credible evidence and the person refuses to resign, he/she should be told of the process for dismissal. Check the church's bylaws to see if there is a prescribed procedure.
- 3) Severance pay should be considered for the sake of the family. The spouse and children are secondary victims.

---

## Appendix A

---

### **Background Checks**

#### **Conducting a Criminal Background Check**

Why is it necessary to conduct a background check on church workers, employed and volunteer? Simply answered, “What you don’t know can hurt you!” Certainly, churches need to protect themselves from lawsuits (negligent hiring, negligent retention, negligent referral), but much more importantly churches must protect their members and guests, especially children and minors. The general assumption is that the church should know about previous behavior before hiring employees and enlisting volunteers. Background checks are an important tool for meeting this assumption. Churches are encouraged to conduct a background check before putting people – even volunteers – to work in sensitive areas, such as with preschoolers, children and youth.

What should be done?

**1) Receive written permission granting authorization to conduct a background check from the person to be screened.**

You should be supplied with the proper authorization form from the background check service. If they do not provide one, a simple authorization form is available from the State Board of Missions’ Office of LeaderCare & Church Health. (See Contact us: page 22.)

**Select a background reporting agency to run the check.** Listed on page 77 are several companies that provide such a service. Discuss with the selected company costs, coverage and application forms [See “Background Checks,” on page 7].

**Upon receiving the report,** handle the information provided with extreme confidentiality. Only the personnel committee and those requesting the background check should be allowed to see the information. Retain this information permanently in a secure location other than the individual personnel file (just as you would HIPAA information).

#### **Sources for Background Checks**

- Bradley Personnel Consultants [www.bradley-personnel.com/background-checks.html](http://www.bradley-personnel.com/background-checks.html)
- Employment Screening Services (screening including drugs and alcohol use)  
<http://www.es2.com>
- LifeWay <https://www.lifeway.com/en/shop/services/church-administration/background-checks>
- MinistrySafe [www.MinistrySafe.com](http://www.MinistrySafe.com)
- Protect My Ministry [www.protectmyministry.com](http://www.protectmyministry.com)
- Shepherd’s Watch Background Checks (formerly “Church Volunteer Central”)  
<https://www.group.com/category/ministry-resources/volunteer-management/shepherds-watch-background-checks.do>
- Single Source Services [www.singlesourceservices.com](http://www.singlesourceservices.com)

---

## **Appendix B**

---

### ***A Covenant of Ministerial Ethics***

As a minister called of God to serve this church, I commit myself to these ethical practices:

I will continuously cultivate my relationship with the Lord that I may grow more and more into the image of Jesus, my Savior and Lord.

I will conduct myself in a way that exemplifies the gospel I preach, demonstrating what it means to be a Christian.

I will nurture strong relationships with my family.

I will develop relationships with friends and colleagues that will help hold me accountable for proper behavior.

I will demonstrate sexual integrity in ministry by observing these forbidden boundaries:

- Sexual relations outside marriage.
- Unwanted or inappropriate physical contact.
- Improper behaviors such as suggestive speech, either verbal or written.
- The use of pornography.

I will submit to the church-adopted policies and procedures for responding to an allegation of sexual misconduct. If I am guilty of such misbehavior, I will confess and resign. If there is credible evidence of misconduct, I will resign. I will permit full disclosure of information to be made to the deacons or a comparable authoritative body which could include the congregation. Further, I will accept that factual information will be revealed to inquiring churches considering me as their minister.

Signed: \_\_\_\_\_

Dated: \_\_\_\_\_



---

## Appendix C

---

### ***Set Rules for Your Youth and Children's Ministers***

Youth ministries are at high risk for sexual misconduct allegations. Youth workers are often closer in age to the teens they work with, they're often unmarried and they spend a lot of time with youth — sometimes off-premises or at overnight activities. Establish rigid guidelines for youth ministers and youth activities.

- 1) Plan youth activities in advance of an event.
  - a) Establish a youth ministry team or youth committee.
  - b) No spontaneous “Let’s all go to...”
- 2) Ensure that adequate adult supervision is present.
  - c) Two-person rule: Reasonable effort will be made to have two adult workers present or nearby with minors (preschoolers, children and students) during church activities. Reasonable effort will be made to assure that one adult is not left alone with one minor. A husband and wife working the same room will typically be considered as one adult for purposes of this policy.
  - d) Six-month rule: Only adults who have been members of their current church for six months or more may serve as supervisors/chaperones.
  - e) Adults-only rule: Only allow adults age 21 and older as supervisors/chaperones of minors.
  - f) If possible, other than the youth minister, enlist only people age 25 or older as chaperones of minors.
- 3) No dating of minors by youth ministers or other paid or volunteer youth workers.

---

## Appendix D

---

### **Sample Sexual Harassment Policy**

Definition (EEOC 29 Code of Federal Regulations 1604.11)

- 1) Sexual Harassment Policy  
Unwelcome sexual advances, requests for sexual favors and other verbal or physical conduct of a sexual nature constitute sexual harassment when:
  - a) Submission to such conduct is made either explicitly or implicitly a term or condition of an individual's employment,
  - b) Submission to or rejection of such conduct by an individual is used as the basis for employment decisions affecting such individual, or
  - c) Such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile or offensive working environment.
- 2) Purpose  
To define the policy of the Sample Baptist Church that all employees have the right to a work environment free from all forms of discrimination and conduct which can be considered harassing, coercive or disruptive, including sexual harassment.
- 3) Policy  
The church's position is that sexual harassment is a form of misconduct that undermines the integrity of the employment relationship. No employee -- either male or female -- shall be subject to unsolicited and unwelcome sexual overtures or conduct, either verbal or physical.
- 4) Sexual harassment does not refer to occasional compliments of a socially acceptable nature. It refers to behavior that is not welcome, that is personally offensive, that debilitates morale, and that, therefore, interferes with work effectiveness. Such behavior may result in disciplinary action up to and including termination.
- 5) Policy Implementation  
It is the responsibility of the senior pastor, ministers and supervisors to make sure the organizational component for which each is responsible is in full compliance with this policy. Employees who have complaints should report such conduct to their supervisors. If this is not appropriate, employees are urged to report and ask the assistance of the senior pastor. If the act was criminal in nature, call law enforcement to investigate. Otherwise it is the responsibility of the senior pastor to provide guidance, investigate charges of impropriety, and recommend appropriate action. All claims must be thoroughly investigated.
- 6) Complaints Procedure
  - a) Employee  
Complaints of sexual harassment should be brought to the attention of the supervisor unless the alleged harasser is the employee's supervisor. In such cases, the employee should feel free to bypass the supervisor and take the complaint directly to the senior pastor. If the senior pastor is the offender, the employee should take the complaint directly to the chairman of deacons.

b) Supervisor

After notification of any employee's complaint, the supervisor will immediately contact the senior pastor. If the senior pastor is the offender, the supervisor will immediately contact the chairman of deacons.

c) Process

i) After notification of the employee's complaint, a confidential investigation will immediately be initiated to gather all facts about the complaint. The senior pastor will have the primary responsibility for investigations. If the senior pastor is the offender, the deacons will have the primary responsibility for investigations.

ii) After the investigation has been completed, a determination will be made regarding the resolution of the case by the senior pastor. If the senior pastor is the offender, the deacons shall decide regarding the resolution of the case. If warranted, disciplinary action, up to and including termination, will be taken. If no action is warranted, then both parties will be informed that the facts did not substantiate the allegations. In this situation, steps must be taken to facilitate both parties continuing to work with each other.

iii) Non-Retaliation - This policy prohibits retaliation against employees who bring sexual harassment charges or assist in investigating charges. Any such employee will not be adversely affected in terms and conditions of employment, nor discriminated against or discharged because of the complaint.

7) Non-Employees

In addition to the above, any complaints of sexual harassment by an employee against vendors or any other non-employees who do business with the Sample Baptist Church should be reported and investigated in the same manner as stated in section 6).

---

## **Appendix E**

---

### ***Church Computer Use Policy***

#### ***Duty not to waste computer resources***

##### ***Accessing the Internet***

To ensure security and avoid the spread of viruses, users accessing the Internet through a computer attached to the church's network must do so through an approved Internet firewall or other security device. Bypassing Church's computer network security by accessing the Internet directly by other means is strictly prohibited unless the computer you are using is not connected to the church's network.

##### ***Frivolous use***

Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all users connected to the network have a responsibility to conserve these resources. As such, the User must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending unauthorized mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online social media, uploading or downloading large files, accessing unauthorized streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the Internet.

##### ***Virus detection***

Files obtained from sources outside the church, including disks brought from home; files downloaded from the Internet, newsgroups, bulletin boards or other online services; files attached to e-mail; and files provided by customers or vendors may contain dangerous computer viruses which may damage the Church's computer network. Users should never download files from the Internet, open or accept e-mail attachments from outsiders, or use disks or other storage media from non-church sources without first scanning the material with church-approved virus checking software. If you suspect that a virus has been introduced into Church's network, notify the network administrator immediately.

##### ***No expectation of privacy***

Employees are given access to computers and Internet access to assist them in the performance of their jobs. Employees should have no expectation of privacy in anything they create, store, send or receive using the church's computer equipment. Church computers and the network are the property of church and may be used only for church purposes.

##### ***Waiver of privacy rights***

User expressly waives any right of privacy in anything he creates stores, sends or receives using Church's computer equipment or Internet access. User consents to allow any Church personnel access to and review of all materials created, stored, sent or received by User through any Church network or Church Internet connection.

***Monitoring of computer and Internet usage***

Church has the right to monitor and log any and all aspects of its computer system including, but not limited to, monitoring Internet sites visited by Users, monitoring chat and newsgroups, and monitoring file downloads and all communications sent and received by all users.

Blocking sites with inappropriate content.

***Church has the right to utilize blocking software***

Church has the right to utilize blocking software that makes it possible to identify and block access to Internet sites containing sexually explicit or other material deemed inappropriate in the workplace.

Site-blocking software is installed and maintained on church computers.<sup>1</sup>

***Acknowledgement of understanding***

I have read and agree to comply with the terms of this policy governing the use of Sample Baptist Church's computer network. I understand that violation of this policy may result in disciplinary action, including possible termination and civil and criminal penalties.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_

---

<sup>1</sup> Internet Safety also offers a \$19.99 application for the iPhone, iPod Touch, and iPad.

Covenant Eyes also offers filtering and accountability software for personal computers. The accountability software, priced at \$7.99 per month for the first user and \$2 for each additional user, monitors a person's internet use and emails a report of all websites visited for accountability partners to view.

---

## Appendix F

---

### ***Sample Church Computer Network and Internet Access Sexual Misconduct Policy***

#### *Disclaimer*

The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. Additionally, having an e-mail address listed on a website or social media may lead to receipt of unsolicited e-mail containing offensive content. Users accessing the Internet do so at their own risk, and Sample Baptist Church is not responsible for material viewed or downloaded by users from the Internet. To minimize these risks, your use of the Internet at Sample Baptist Church is governed by the following policy:

#### *Permitted use of Internet and church computer network*

Church computers and the network are the property of Sample Baptist Church ("Church") and may only be used for legitimate business and ministry purposes. Users are provided access to Church computers and the network to assist them in the performance of their jobs. Additionally, certain employees ("Users") may also be provided with access to the Internet through the computer network. All Users have a responsibility to use Church's computer resources and the Internet in a professional, lawful and ethical manner. Abuse of Church computers and the network or the Internet may result in disciplinary action, including possible termination, and civil and/or criminal liability.

#### *Access*

1. Passwords are required to access a computer.<sup>2</sup>
2. Church computers may only be used by those with a church-related need.
3. Church computers may be used for personal tasks by those authorized to use them for church-related purposes, but only on personal time, to a small degree, and never in a way that costs the church money or efficiency.<sup>3</sup>

#### *Computer network use limitations*

##### *Prohibited uses*

Church's computer network may not be used to disseminate, view or store pornographic text or images, or any other unauthorized materials. Employees may not use Church's Internet connection to download games or other entertainment software (including screen savers) or to play games over the Internet. Additionally, you may not use Church computers or the network to display, store or send (by e-mail or any other form of electronic communication such as bulletin

---

<sup>2</sup> Having a password for each person who has access to a computer at a church eliminates a lot of problems with users who might want to use church-owned computers to view pornography and other inappropriate websites.

<sup>3</sup> This approach is like one commonly used for the personal use of church phones.

boards, chat rooms, Usenet groups, etc.) material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory or otherwise inappropriate or unlawful. Furthermore, anyone receiving such materials should notify their supervisor immediately.

### *Illegal copying*

Never copy material you find on the Internet without the owner's permission. Copyright laws say that copyright holders must consent to the use of their works with very few exceptions. The fact that we are a church is not one of the exceptions. Nothing may be used without the prior express written permission of the copyright holder. This does not apply to works created by Church staff (unless there is a special written agreement in place) because those are considered works made for hire and the church owns the copyright.

You may not illegally copy material protected under copyright law or make that material available to others for copying. You are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages and other material you wish to download or copy. You may not agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of Church leaders.

### *Communication of confidential and/or personal member information*

The information on the church system is an asset. Information must be protected by everyone who has access to it in the same way they would protect any other church asset.

Never give anyone copies of mailing lists or directories without the written permission of the pastor or church administrator. Even then, these should only go to members of the congregation and should include a statement that they may only be used for fostering the fellowship and ministry of the church (never for commercial purposes).

Some data must be guarded to protect people's privacy. Consider, for instance, the harm that could be done to someone if their Social Security number, checking account routing information, credit card information, or counseling notes were made public.

Unless expressly authorized to do so, you are prohibited from sending, transmitting or otherwise distributing confidential and/or personal member information, data or other confidential information belonging to Church. Unauthorized dissemination of such material may result in severe disciplinary action as well as substantial civil and criminal penalties under state and federal laws.

---

## Appendix G

---

### ***Sample Church Internet Usage Policy***

The following is a sample policy your church can use to develop guidelines for Internet usage on church computers. Replace [Church Name] with your church name and make other adjustments to the policy language as needed.

#### 1) Policy Guidelines

[Church Name] provides certain employees access to the vast information resources of the Internet with the intention of increasing productivity and enhancing church-related communication. While this access has the potential for employees to do their jobs faster or smarter, there is justifiable concern that it can also be misused. Such misuse can waste time, potentially violate laws, ordinances or other [Church Name] policies, garner negative publicity for the church and potentially expose it to significant legal liabilities.

This Internet Usage Policy, which applies to all employees, is designed to facilitate understanding of the expectations for the use of these resources. The underlying philosophy of this policy is that Internet access from [Church Name] is primarily for church-related purposes including communicating with congregation members and colleagues, researching relevant topics and obtaining useful business information. In addition, all existing laws and [Church Name] policies apply to an employee's conduct on the Internet, especially those that deal with intellectual property protection, privacy, misuse of [Church Name] resources, sexual harassment, information and data security, and confidentiality.

The best way to determine if use of the Internet is appropriate is to ask, "If I were doing this same activity in some other way (e.g., telephone, library, in person, by hand) would this activity be appropriate?"

#### *The two key tenants to this usage policy are:*

- Do not do anything with [Church Name] Internet access resources that would otherwise be considered illegal, grossly inappropriate or offensive to the established value system expressed by [Church Name] as a Christian, nonprofit organization. Viewing or downloading erotica, playing games, sending non-[Church Name] related mass mailings, and running a private business are obvious examples.
- Do not waste [Church Name] time. There are plenty of fascinating site to explore, but [Church Name] time should be spent conducting [Church Name] business. Church employees may use their Internet facilities for nonbusiness research or browsing during lunch and outside of work hours, provided that all other usage policies are adhered to.

#### 2) B. Detailed Internet Policy Provisions

- a) [Church Name] domain name will appear with every Internet post made by a church computer user. Any user may thus be viewed as a representative of [Church Name] while conducting business on the Internet. During any Internet use, users are required to refrain from any activity or communication that would have a negative impact on [Church Name] or the reputation of [Church Name].



- b) User IDs and passwords help maintain individual accountability for Internet resource usage. Any user who obtains a password or ID for an Internet resource must keep that password confidential. [Church Name] policy prohibits the sharing of user IDs or passwords obtained for access to Internet sites.
- c) Each user using [Church Name] Internet facility shall identify himself or herself honestly, accurately and completely when corresponding or participating in interactive activities and shall not send unsolicited mass electronic mail.
- d) Only those persons who are duly authorized to speak to the media or public gatherings on behalf of [Church Name] on a subject may speak/write in the name of [Church Name] to any blog, newsgroup or chat room. Other users may participate in blogs, newsgroups or chats in the course of business when relevant to their duties, but they do so as individuals speaking only for themselves and should make that clear in their communication. Only those persons who are authorized to speak to the media or public gatherings on behalf of [Church Name] on a subject may grant such authority to blog, newsgroup or chat participants.
- e) Employees are reminded that the Internet is not a secure method of communication. Neither proprietary information nor any information received in confidence by [Church Name], or the user, may be sent on the Internet unless prior approval is received from the senior pastor or the administrator.
- f) The display of any kind of obscene image or document of any [Church Name] computing resource may be a violation of existing [Church Name] policy on sexual harassment and is prohibited. In addition, obscene material may not be archived, stored, distributed, edited, or recorded using [Church Name] network, printing or computing resources. A user, who accidentally connects to a site that contains sexually explicit or offensive material must disconnect from that site immediately and report the accidental connection to the church computer system administrator or computer committee.
- g) Freeware, shareware and commercial software from the Internet may be subject to computer viruses, may not work properly, or may be subject to copyright infringement laws. Users may download only software with direct business use with permission of the church computer system administrator or committee and must arrange to have such software properly licensed and registered. Users may not use [Church Name] Internet facilities to download entertainment software or games, or to play games against opponents over the Internet. No user may use [Church Name] facilities knowingly to download or distribute pirated software or data. Any software or files downloaded via the Internet may be used only in ways that are consistent with their licenses or copyrights.
- h) No user may use [Church Name] facilities to deliberately propagate any virus, worm, Trojan horse, trapdoor, or backdoor program code; or knowingly disable or overload any computer system, network, or to circumvent any system intended to protect the privacy or security of another user.
- i) [Church Name] Internet facilities and computing resources must not be used to knowingly violate the laws and regulations of the United States or any other nation or the laws and regulations of any state, city, province or local jurisdiction in any way.
- j) Users should not have any expectation of privacy as to his or her Internet usage. It is possible to monitor Internet usage patterns and [Church Name] will regularly inspect any

and all files stored on [Church Name] resources to the extent necessary to ensure compliance with this Internet Usage Policy.

- k) Infractions of these policies constitute a misuse of [Church Name] assets and therefore is considered a violation of [Church Name] Personnel Policy. Any such infraction may result in termination or other disciplinary actions.

I HEREBY CERTIFY THAT I HAVE READ, AND THAT I AGREE TO, THIS INTERNET USE POLICY. (FOR YOUTH, MUST BE SIGNED BY A LEGAL PARENT OR GUARDIAN.)

Signature \_\_\_\_\_ Dated: \_\_\_\_\_

Printed name \_\_\_\_\_

Parent/Guardian Signature \_\_\_\_\_

(if youth under age 18) Name \_\_\_\_\_

---

## Appendix H

---

### ***Sample Social Media Policy<sup>4</sup>***

This sample agreement should be reviewed and approved by your attorney prior to use.

This policy provides guidelines for employees and volunteers to follow when they use social media tools on behalf of (name of ministry) or when (name of ministry) becomes part of a social media dialogue.

New social media tools emerge regularly. This policy applies to all forms of social media: those currently in use and those that (name of ministry) may adopt at any time.

#### ***Use of Social Media***

- All (name of ministry) policies (including harassment, confidentiality and software use policies) apply to the use of social media.
- (Name of ministry)'s official social media participation is managed by the (social media team, an individual, a ministry committee, etc.). This (team, individual, committee) is responsible for regularly posting information on the ministry's behalf and for monitoring and responding to posts on these pages.
- Ministry employees who misuse the ministry's social media resources in ways that violate the law or ministry policies are subject to disciplinary action.

#### ***Social Media Guidelines***

1. Employees and volunteers interested in representing (name of ministry) on social media must first sign a consent and application form and attend a social media training class. The class will outline the recommended practices, limitations and legal parameters for administering the ministry's social media accounts.
2. Social media postings should not disclose sensitive or confidential information, unless the person that the information concerns has given written consent to share such information. This may include medical information or other personal matters.
3. Social media representatives should refrain from posting photos of individuals—or identifying the individuals—on the ministry's official social media pages without their prior written consent which may be given by email or text. Social media representatives are responsible for disabling the "tagging" of individuals in photos posted on the ministry's page. If the photos include location information, this information is to be removed as well.
4. Social media representatives will respect copyright and fair use laws, making sure that they have permission or authority to use content before posting it. Simply giving credit to the author will not protect the ministry from a possible copyright infringement claim.
5. Social media representatives will monitor the page at least once per (measure of time), removing content that is obscene, embarrassing, abusive or otherwise objectionable. If any

---

<sup>4</sup> Brotherhood Mutual Insurance. Used by Permission. Social Media Policy This sample agreement should be reviewed and approved by your attorney prior to use. M288 (3/14)

posted material appears to be illegal (e.g., child or elder abuse, etc.), social media representatives should contact their supervisor and other appropriate authorities.

6. When communicating with youth via social media, employees and volunteers should follow the ministry's youth communication policy.  
In addition, ministry workers and volunteers who serve in children and youth ministries should keep their professional image in mind. Online conduct and behavior affect this image. (Name of ministry) discourages staff members and volunteers from accepting invitations to "friend" youth members within personal social networking sites. Contacting youth members outside the ministry's youth group page may create risks for ministry workers and alter the dynamic between a youth leader and youth.
7. Employees and volunteers are personally responsible for the content they publish online, including content they publish through their own social media pages. Employees should be sure to identify themselves as part of the ministry staff, including their role at (name of ministry) and make it clear that they are speaking for themselves, not officially for the ministry.
8. As an employee or volunteer of (name of ministry), remember that your online posts have the potential to affect the ministry, even those you make on a personal level. For this reason, we ask that you conduct your online interactions in accordance with the Employee/Volunteer Handbook, the ministry's statement of faith, and code of conduct.
9. In the event of a crisis, contact the social media leader, church leadership and the church attorney before responding to any posting or comments related to the crisis.

**Note: This is a sample document only. Your organization is responsible for compliance with all applicable laws. Accordingly, this sample should not be used or adopted by your organization without first being reviewed and approved by an attorney. Brotherhood Mutual Insurance Company assumes no liability in connection with the use or distribution of this sample document.**

---

## Appendix I

---

### ***Social Media Practices for Ministers***

Texting and Social Media can be dangerous concerning privacy and concerning the possibility of sexual misconduct. Ministers and church leaders may consider some of the following suggestions to make their online experiences safer.

#### ***Concerning adults***

Attorney James Sexton writing for *Time*<sup>5</sup> magazine said, “Facebook is the single greatest breeding ground ever for infidelity.” Other dangers exist such as adults in a married relationship using dating apps such as Tinder resulting in cheating. Ministers and church leaders should learn about the dangers of social media.

Conversations should be kept professional and not be flirtatious.

#### ***Concerning minors***

Group texts are best. If a minor sends a text to a church leader one on one, the leader should not reply to the sender without including his spouse or a trusted youth worker in the reply.

To address privacy concerns, social media can also include a private group page for the church youth group for example.

The church should be aware of privacy concerns over photographing and posting images of minors. A photo release should be signed by parents for events such as camps. A church could consider using purchased stock photos for publication and a private social media page for church members.

Based on McGreror, T. (2017, September 1). Selfie: A Parent's Guide to Social Media. Retrieved from <https://www.tommymcgregor.com/selfie-a-parents-guide-to-social-media>

---

<sup>5</sup> Sexton, J. J. (2018, March 26). Divorce Lawyer: Facebook is a Cheating Machine. Retrieved from <https://time.com/5208108/facebook-cheating-infidelity-divorce/>.

---

## Appendix J

---

### ***Appropriate and Inappropriate Forms of Affection***

Church leaders should develop standards of behavior concerning proper and improper forms of conduct. Some examples of proper forms of affection include:

- Brief hugs side to side or “A frame.”
- Pats on arms or shoulders, etc.

Examples of inappropriate forms of behavior include:

- Kisses on the lips and lengthy embraces.
- Tickling, wrestling and “wedgies” would be examples of improper touch as these are often used by predators as a part of the victim “grooming process.”
- Church leaders should avoid being alone with a child including in a car or at church.
- Church leaders should avoid being alone with the opposite sex.
- Having children on one’s lap over age 5 may be inappropriate.

Guidelines should be established for bathroom procedures concerning preschoolers and children.

Staff should carefully consider overnight activities concerning sleeping arrangements, observing the “two-adult” rule. The two-adult rule means that reasonable effort will be made to assure that two or more unrelated adults are present or nearby at church and at other activities. Concerning the sleeping arrangements for overnight activities, adults should not be in bed with a minor.

**Contact us:**

[www.alsbom.org/safe](http://www.alsbom.org/safe)

or

Cooperative Program and Stewardship Development

1.800.264.1225, 283.

or

LeaderCare and Church Health

1.800.264.1225, ext. 241 or 210.