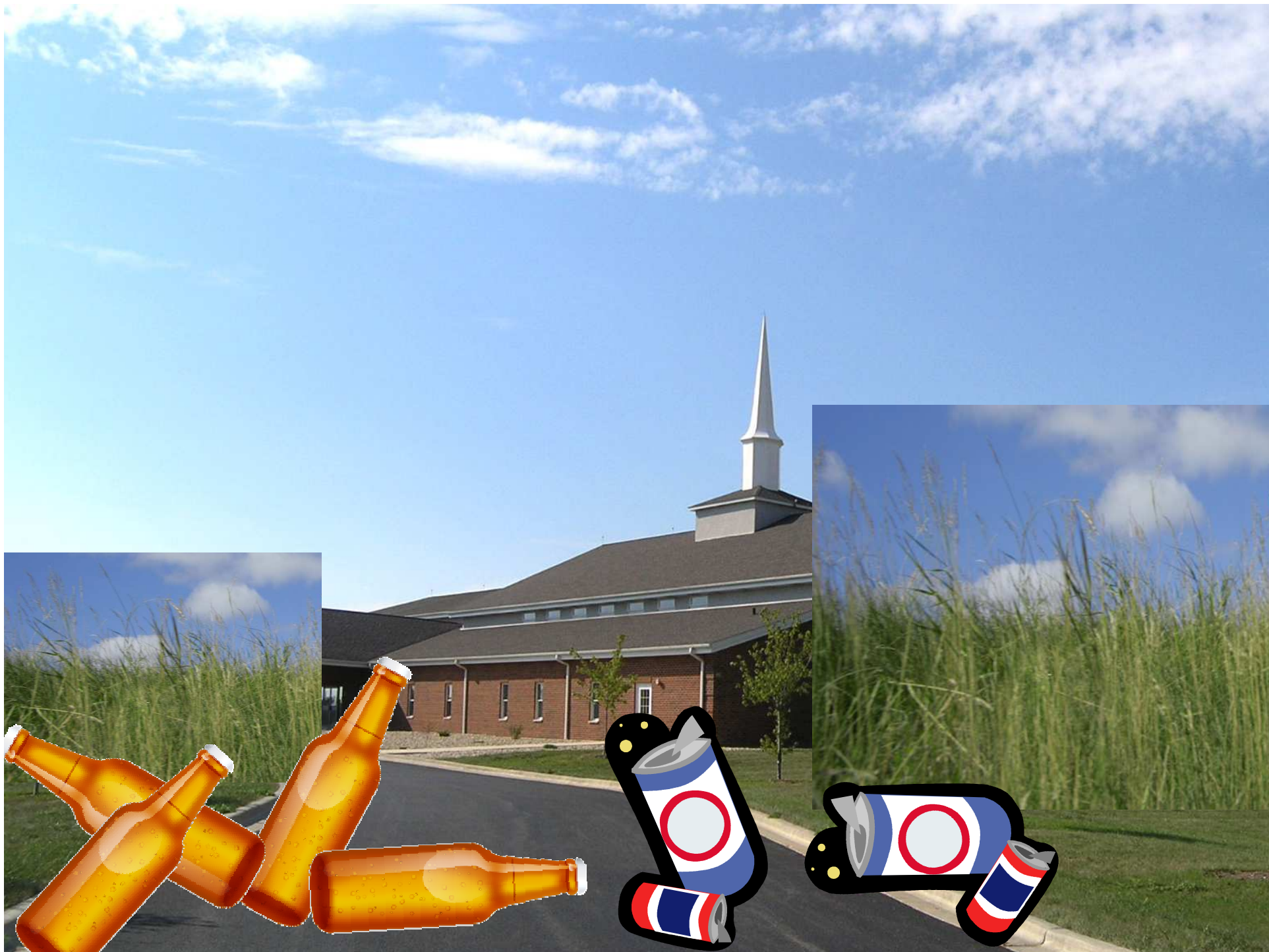


# Safe e-Sanctuary Policy

*Creating a safe, on-line  
media presence.*



# Church Property

*Your web presence is your property.*

1. Security
2. Maintenance
3. Emergency Procedures

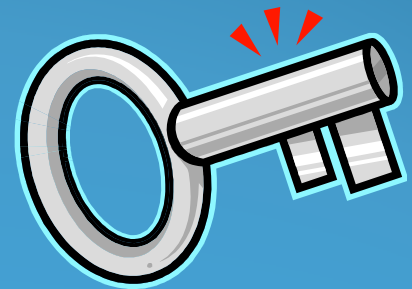
# Security

1. Who do we want to protect?

- Children
- Church/Conference
- At-risk People
- Volunteers

Protect = “keep from a violation of trust”

2. Lock up Private Information.





➤ Recco

re log-in.  
ontent.



# Maintenance



1. Appoint one person to check and maintain sites
2. Establish time-frame for updates (twice weekly)
3. Check posts and blog entries
  - Report Pastoral Concerns
  - Remove Tags
  - Who's invited to the youth Facebook page?

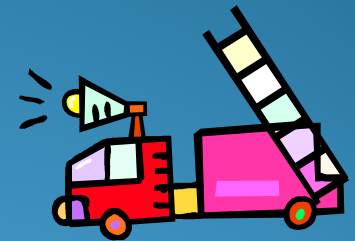
# What's Private?

1. Are Facebook Groups Private? Who sees it?  
Parents = NO Youth = YES
2. Controlled/Personal Data (covered by FOIA)  
SSN, Birthdates, grades, name, place of birth, addresses
3. Are Sermons Private?  
- Posted manuscripts are asking to be "private"
4. Are e-mails private?  
- If you are counseling someone over e-mail, it's not private. It's company property.  
- Recommended to use the Blind Carbon Copy.



# Emergency Procedures

1. Back up critical information.
2. Who approaches the 'perpetrator'?
  - Facebook bully
  - Helicopter Parent
3. What to do about pornography.
  - Don't send the image.
  - Confiscate the hardware.



# Sample Policy Review

1. Answers scope, security, and maintenance questions.
2. Suggested emergency procedures.

# Summary

1. Decide what is open and what is to be protected.
2. Create a log-in.
3. Designate a maintenance person.
4. Monitor what is posted at social media sites.
5. Establish emergency procedures.