

# The Electronically Safe Church Office



## Publication Considerations

### Supporting the Ministry

- Do not post material that undermines the church's mission.
- Does the content *further* the mission?

### Do Not Violate Copyright

- Is it yours to post?

### Advertising

- Some free web hosting services will advertise on your site.
- Social networking services will advertise on your page.
- If you accept advertising, what are your policies?

### External Hyperlinks

- Does the linked content further your mission?
- Check, check, check.

### Develop and Adhere to a Privacy Commitment

#### Authority

- Who makes decisions about content day-to-day?
- Who oversees that person or persons?

#### Report Illegal Activity

### Make sure materials you post are electronically "safe"

#### Error Policies

#### Members' Privacy

- What information are your members willing to provide online?
- Get permission!
- Password-protect online directories.
- Identification of children requires parent or guardian's permission.
- Images require permission.

#### Cookie Use

- Will the site use cookies, and for what?
- Inform users of the cookie policy.

### Make the site accessible to screen readers

## Data Security

### Physical Security

- Put computers with sensitive data behind locked doors.
- Consider security computers with cable locks.

### Employ User Account Security

- Require usernames and passwords to enter a PC.
- Disable the Guest account.
- Use strong passwords: 8 characters or better, not using words.

### Secure Transmission of Financial Information

- When buying online, double-check that the transmission has been encrypted.
- Do not send credit card numbers or sensitive data via email.

### Backup

- There are only two kinds of people in the world who do not regularly back up their computers: the ones who have lost data and the ones who will.
- Backup early, often, and preferably without requiring user intervention.
- Consider keeping a backup set offsite.

### Email

- Email is not secure.
- Do not send potentially sensitive information about someone else via email.
- Warn people sharing personal information with you that you may not be able to keep it confidential.

### Protect the Network

- On a broadband connection, use a router/firewall.
- Install and update security software on PCs.
- Use a comprehensive security application that includes a software firewall.
- Secure wireless networks with encryption.

## References

- [www.ctucc.org/staffblogs/index.php?story=140](http://www.ctucc.org/staffblogs/index.php?story=140)
- [www.ctucc.org/resources/websitepolicyguidelines.html](http://www.ctucc.org/resources/websitepolicyguidelines.html)