Susquehanna Conference
Safe Sanctuaries Policies

Cyber Safety & Electronic Communications

The internet, apps, social media and portable devices allow people to stay in contact with each other more easily than at any other time in the history of civilization. Excellent ministry can take place using modern technology, but as with all forms of ministry, there are inherent risks involved with the use of electronic communications. **Assume anything and everything in cyberspace is public information.** Here are some recommendations.

1. **Obtain advance written parent/legal guardian permission.** In addition to general permission to participate in a conference ministry or event, obtain written advance parent/legal guardian permission for children and youths, and personal permission from vulnerable adults or their guardian if applicable, for:

    a. Taking and using photos or videos of participants, for example, posting on sites, sending by e-mail or by cell phone, reproducing photos in brochures, posters or newspapers.
    b. Communicating or transmitting data electronically with children, youths or vulnerable adults sharing any full name or contact information.

2. **Never post identifiable information.** For example:

    a. Do not use “broadcast” emails. Use the “Bcc” option (blind carbon copy) so that each recipient sees only his or her address when a message is received.
    b. Be cautious when transmitting easily identifiable information such as event dates, times, locations, or participants.
    c. Limit what is communicated in prayer requests. When placing a child, youth, or vulnerable adult on a prayer list, use only first names and only if you think a name is necessary.

3. **Use caution when sharing photos.**

    a. Consider using stock or purchased photos.
    b. Obtain all necessary legal permission to use photos or other content (poems, songs, etc.).
    c. If sharing photos, refrain from using names, and never use last names or other personally identifiable information.
    d. Check photos for vulnerable/compromising situations and to make sure they uphold your mission.
    e. Check to make sure nametags are not distinguishable.
    f. Use low-resolution photos whenever possible and slightly blur/pixilate photos.
    g. Block "save photo as" options on websites.
    h. Limit access to photos by employing the use of a password.

4. **Social media sites (Facebook, Blogs etc.)** Do not use your personal social media presence for ministry. Use a group social media site that is monitored by senior leadership, for example a Facebook site for the specific group.

    a. Include a code of conduct/terms and conditions for the site that expressly states expectations for posts and a clear expression of how violations, offensive and objectionable material will be addressed.
    b. Monitor the site and remove inappropriate comments, photos, links, etc.
    c. Restrict who can be a friend.
    d. Do not post anything that you would not want printed in the newspaper, church newsletter or bulletin.
    e. Be familiar with, and comply with, social media provider policies, restrictions and terms and conditions. For example, according to Facebook's own terms, children under 13 years of age may not sign up for a Facebook account.
    f. Encourage children, youths, and vulnerable adults to follow these same guidelines as appropriate.

5. **Do not collect online, or allow third parties to collect online, personal information from children under the age of 13. See Children's Online Privacy Protection Act ("COPPA") and Federal Trade Commission Rules implementing COPPA (the "Rule").** COPPA and the Rule require specific permissions and privacy policies if a website or online service collects, or allows third parties to collect, personal information if the service is directed to children under the age of 13. Restrictions also apply if the site is directed to a general audience and the organization has actual knowledge that it collects personal information from children under 13 years of age.