Safe Sanctuaries Digital Safety

The internet and portable devices allow people to stay in contact with each other more easily than at any other time in the history of civilization. Some incredible ministry can take place using modern technology, but as with all forms of ministry there are some inherent risks involved with the use of electronic communications. However, following basic Safe Sanctuaries procedures can help to minimize those risks. There is no such thing as privacy in cyberspace. Consider anything and everything on the internet as public information. Here are our procedural guidelines:

Receive Parental/Guardian Permission

In addition to general permission to participate in an Apex UMC Family ministry, it is advisable to receive advance parental permission for children and youth, and personal permission for vulnerable adults in writing for:

1. E-mailing, Direct Messaging, calling, texting, or sending data to a child, youth, or vulnerable adult by computer, tablet, or cell phone; and
2. The sharing of any full name or other personal sensitive information.

Best Practices for Sharing Information Online

1. Never post Easily Identifiable Personal Information Online**.** Easily Identifiable Personal Information includes: address, telephone number, email address, social security number or other identifying number or code.
2. If you communicate by email, particularly with minors and vulnerable adults, try not to use "broadcast" emails. Use the "BCC" (blind carbon copy) so that each recipient sees only his or her address when a message is received.
3. Be cautious when transmitting easily identifiable information like event dates, times, locations, or participants.
4. Limit what is communicated in electronic prayer requests. When placing anyone on an electronic prayer list, consider using only first names.

Limit individual communications with children, youth, and vulnerable adults.

1. Conduct any communications in a professional manner. (Even though you may be a sounding board for a person having a bad day, the reverse is not true.)
2. Save all confidential cyber-communications you have with children, youth, and vulnerable adults (i.e., direct messaging conversations, text messages, emails, etc.). An electronic paper trail can be important. Do not use platforms such as Snapchat that do not allow for permanent records.
3. If you are uneasy about any topic addressed in an email or other platform, send a BCC or screenshot to a parent/guardian (if appropriate) or another trusted adult. Honor privacy, but not secrecy.
4. If abuse or threat to safety is divulged electronically, follow standard reporting procedures outlined in the Safe Sanctuary Policy, sections 6 and 7.

Safety Measures for Sharing Photos/Videos Electronically

1. Post notice that photos and videos may be used and invite individuals to self-select out.
2. When posting photos and videos, refrain from using names and never use last names or identifiable information, unless given permission by parents.
3. Only share photos and videos that are aligned with our mission and values.

Church "Admin" on Ministry Accounts

1. Where there is no real-time interaction between viewers (e.g., a video posted but not broadcast live) the two adult rule applies in that there shall always be two, unrelated authority figures with administrator rights on any account that is posting official ministry content.
2. Digital/on-line church media accounts shall be set up as ministry accounts and shall have two unrelated authority figures as administrators.

Safety Measures for Personal Use of Social Networking Sites

1. Remember that when you join the church's social network, your social networking profile is an extension of our ministry. Be mindful of the privacy settings on your personal social networking profiles.
2. Restrict who can be your friend / who can follow your page. It is prudent to use judgment in accepting requests from youth. Do not initiate friend requests with minors, and do not follow a minor's account (for example, on Instagram) unless they have requested to follow you.
3. Use higher level security features even if you have a restricted profile (such as requiring your approval of all comments posted to your site.)
4. Do not post anything to your social networking site that you would not want attached to your resume or printed in the church bulletin or newsletter (the same goes for blogs).
5. Remove or do not post inappropriate comments, photos, etc.
6. Encourage youth to follow these same guidelines.

Safety Measures with Digital Meeting Platforms (Zoom, GoogleMeet, Facetime, etc)

1. Always have 2 adults present in a digital meeting / gathering. The adults should be present in the call before any minor arrives. Until both adults are present, adult cameras should be turned off.
2. If more than one adult cannot be present at the same time, allow another user to have adult administrative privileges to go in and monitor accounts on a regular basis. This helps meet the "window in a door" or "open door" policies familiar for in-person meetings. Also, consider having an adult (like a parent) on the youth side of the call or video simply appear and wave, acknowledging that the adult knows this conversation is taking place.
3. If an adult and minor need to have a one-on-one digital meeting, the adult must make another adult or parent aware of the meeting.
4. Be mindful of privacy measures available on Digital Meeting Platforms, as well as how passwords are shared, to protect the meeting space.