

Appendix B: Recommended Practices and Guidelines for Social Media and Electronic Communications for Vulnerable Adults

Social media is an ever-increasing part of adult lives, and has the potential to empower ministry. Behavior in the digital sphere is never private. Posted content may be used out of context and out of the control of the originating individuals and organizations, putting them at risk. In addition, these powerfully connective tools are subject to the same dynamic of unequal power and potential for abuse that present a risk in all ministry relationships. Churches face the challenge of identifying and proactively addressing areas of potential risk in social media use in the midst of rapidly evolving technology. The following recommended practices and guidelines are designed to be a flexible template for developing policies and covenants governing the safe use of social media and digital communication in ministry settings.

General Information about Digital Communications

- All communications sent digitally (email, social networking sites or platforms, notes, texts, or posts, etc.) are NOT CONFIDENTIAL and can be shared or reposted to others.
- Interactions in the virtual world need to be transparent; that is, occurring in such a way that it is easy for others to see what actions are performed.
- In the virtual world, healthy boundaries and safe church practices must be adhered to as they are in the physical world.
- In the virtual world, “friend” can mean anyone with whom you are willing to communicate through that medium. In the physical world, friend can mean much more in terms of intimacy, self-disclosure, mutuality, and expectations for relationship.
- Laws regarding mandated reporting of suspected abuse, neglect, or exploitation of vulnerable adults apply in the virtual world as they do in the physical world. Check your local applicable laws.

Recommended Practices and Guidelines for Churches and Organizations:

- Establish a policy that outlines professional and institutional standards for profiles and interactions on social networking sites and platforms.
- Establish a policy of transparency regarding social media accounts. The best practice is to have the diocese, congregation, or organization create and “own” the social media accounts representing the diocese, congregation, or organization respectively and have multiple administrators and/or supervisors with access. If personal accounts are used, a system of monitoring should be established.
- Establish a policy regarding the identification or “tagging” of individuals in online photos. For example, on Facebook, “tagging” someone in a photo or video creates a hyperlink to that person’s profile page that can be clicked by anyone. The best practice is for the diocese, congregation, or organization

not to identify or “tag” individuals. The “tagging” of vulnerable adults should be discouraged. The captioning of photos or videos may be permitted when written permission is provided by a vulnerable adult (or the person’s guardian, spouse, or other trusted family member when the vulnerable adult is unable to consent due to impairment or lack of agency). The caption should not include the individual’s full name, nor should it create a clickable link to someone’s personal profile. A policy of whether or not an individual can “self-tag” in a diocese, congregation, or organization’s online photo should also be established.

- A diocese, congregation, or organization does not have a responsibility to review or monitor the personal pages or groups that are not sponsored by the diocese, congregation, or organization respectively, except as described in #2 above. The preceding statement should be included in the diocese, congregation, or organization’s Social Media Policy.
- Email can be a good method of communication, and it also has the opportunity to be misunderstood. Having a clear understanding and procedure when responding to digital communication that raises concern is prudent for all. Best practices can include not responding immediately and sharing the communication with a supervisor before responding. Phone and face-to-face meetings are preferred when responding to emotionally driven communications or pastoral emergencies.
- When using photos and videos for ministry purposes, obtain a media release for each person and only post images that respect the dignity of every person depicted.
- Dioceses, congregations, or organizations must inform participants when they are being videoed because church buildings are not considered public space. Signs should be posted that indicate a service or activity will be broadcast when worship services or activities are streamed or distributed on the web or via other broadcast media.

Recommended Practices and Guidelines for Vulnerable Adults:

- Prudent judgement should be used in the time of day a vulnerable adult is contacted through social media. Under normal circumstances, refrain from contact or exchanging texts, chats, or emails before 8:00 am or after 10:00 pm, unless it’s an emergency.
 - Privacy settings and personal boundaries should be implemented.
 - Create and use profiles on social networking sites that meet professional and institutional standards.
 - Apply privacy settings that are consistent with all vulnerable adults, across all social networking sites and platforms. Avoid playing favorites or the appearance of playing favorites.
- Policy for the Protection of Vulnerable Adults Page 24
- Establish a regular ongoing and consistent system of review that focuses on settings, accessible content, photos, and videos to ensure compliance with professional and institutional standards.

- When possible, send communication (1) to entire groups, (2) on an individual's "wall," or (3) in public areas, rather than in private messages. This includes photos, images, and videos.
- Disclose ongoing digital pastoral communications (ie: e-mails, Facebook messages, texting, etc) with a vulnerable adult to a supervisor to determine when a referral to a professional provider or resource is needed.
- Create covenants to govern digital groups, which include:
 - Appropriate and inappropriate behavior of members (bullying, pictures that depict abuse, violence, illegal activities, sexual acts, etc.) and the consequence for inappropriate behavior;
 - Who may join and/or view group activity, when participants should leave the group, and when/if the group will be disbanded;
 - Description of content that can be posted or published on the site or page;
 - Discourage "tagging" photos and videos of vulnerable adults. However, the captioning of photos and videos is permissible with appropriate written permission as described above;
 - Notification that mandatory reporting laws will be followed; and
 - Consequences for breaking the covenant.
- Delete inappropriate material posted in digital groups, address the behavior and report, if necessary, in accordance with legal and institutional requirements.
- In video calls, follow the same criteria used in telephone calls. In addition, prudent judgement regarding attire and surroundings should be observed.
- Comply with the following best practices regarding "groups" on social networking sites:
 - Have at least two unrelated administrators;
 - Use closed groups, but not "hidden" or "secret" groups, for vulnerable adults;
 - Remove any content that shows or describes inappropriate behavior outside the bounds of the established behavioral covenant; and
 - Observe mandated reporting laws regarding suspected abuse, neglect, and exploitation.