

Policies on the Use of Social Media & Electronic Communication

1. Purpose

The Episcopal Diocese of Pittsburgh (hereafter, the Diocese) and its member parishes, people, and organizations use various media to communicate about the life, ministry, and purposes of the Church. Communication itself should be considered an important ministry of the Church, as it has the potential to help turn people toward God, encourage them in their journey of faith, address challenges encountered along the way, and reveal and celebrate God's work in the world.

Electronic communication has become a leading method for individuals and churches to share news, information, perspectives, and the Gospel message itself. Social media, in particular, shapes the lives of many persons – including children, youth, and vulnerable adults – and it has the potential to empower ministry. But behavior in the digital sphere is never private. Posted content may be used out of context and beyond the control of the individual who posted it, putting them and their organization at risk. In addition, these powerfully connective tools are subject to the same dynamic of unequal power and potential for abuse that presents 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. These policies are intended to address such challenges within our diocesan communities.

2. Applicability and Definitions

2.1. This document applies to communications on all electronic platforms for sharing content and information on which members of the diocesan community engage in discussions about the life, ministry and purposes of the Church or the Diocese, whether those platforms are controlled by the Diocese or by one of its parishes or organizations.

Section 3 (Mandatory Provisions) and Section 4 (Recommended Practices) do not apply to members of the diocesan community when they are communicating in a personal and private capacity on sites hosted or controlled by themselves or other non-diocesan entities. Note, however, the Additional Caution in Section 5.4 below.

2.2. This document applies to all members of the *diocesan community*. This includes diocesan staff members; all members of the Diocese's governing bodies and other committees and commissions within the diocesan structure; all diocesan clergy; and all

leaders, staff, and members in diocesan parishes, missions, ministries and organizations.

- 2.3. The term *social media*, as used in this document, includes social networking services, blogs, short-message ("texting") services, message boards, wikis, podcasts, image- and video-sharing sites, and other methods for information sharing among users. Because this is a constantly evolving area, this document also applies to all future social media platforms, whether or not they are specifically mentioned here.
- 2.4. *Electronic communication* includes, most commonly, websites and broadcast emails (that is, emails sent to a large group of people, or "subscribers"). Broadcast voice messages, though less common, are also covered by these policies.

3. Mandatory Provisions

- 3.1. All members of the diocesan community who are subject to the Commonwealth's mandated reporting laws¹ regarding suspected abuse, neglect, or exploitation of vulnerable persons shall observe and comply with those laws. These statutes apply in the digital world exactly as they do in the physical world.
- 3.2. Official statements of diocesan policy may only be made by the Bishop or the Bishop's designee. Users' social media and electronic communications are made in their personal capacity and not on behalf of the Diocese. Statements made by members of the diocesan community should not be represented (or taken) as expressing the formal position of the Diocese, unless the source of the statement is specifically authorized by the Bishop. This should not be construed to limit users' discussion of matters using the name of the Diocese or their ability to link to the Diocese's websites.
- 3.3. Any use of the Diocese's name or logo for branding or titling pages, blogs, or other similar elements of social media or electronic communications must be approved in advance and in writing. Requests for prior consent to use such names or logos should be made to the diocesan staff person responsible for diocesan communication. Permission to use the name or logo of the Diocese may be revoked at any time at the sole discretion of the Diocese.
- 3.4. All members shall safeguard the privacy interests of other community members in the following ways:
 - 3.4.1. Community members' personal information (e.g., their name, phone number, address, email address) shall not be published without their permission or, in the case of children under 18, the written permission of their parents or legal guardians.

¹ Mandated Reporters are required by state law to report reasonable suspicions of abuse, neglect, and/or exploitation of vulnerable populations to the appropriate state agency. See the Diocese of Pittsburgh's *Policy for the Protection of Children and Youth* and *Policy for the Protection of Vulnerable Adults*, accessible from the <u>Safe Church, Safe Communities</u> page of the diocesan website. Additional guidance, including how to report abuse, may be found at https://www.dhs.pa.gov/contact/Pages/Report-Abuse.aspx.

- 3.4.2. Photos and videos shall not be used for ministry purposes without first obtaining the informed consent of each person depicted, and all images shall respect the dignity of every such person. Images of children under 18 shall not be posted without the informed consent of their parent or legal guardian.² Images of vulnerable adults shall not be posted without the informed consent of the adult or, when the vulnerable adult is unable to consent due to impairment or lack of agency, the person's guardian, spouse, or other trusted family member.³ In all cases, obtaining permission in writing is a best practice.
- 3.4.3. The Diocese, congregation, or organization shall take reasonable steps to ensure people are aware when they may be videoed.
- 3.5. Individuals shall comply fully with copyright law when posting or uploading materials. Posting of materials to diocesan social media must be limited to materials in which the copyright is owned by the party seeking to post the information, or for which the owner has consented to the sharing of the materials. Images and other materials from diocesan websites shall not be copied and uploaded elsewhere without the prior written consent of the diocesan staff person responsible for diocesan communication.

4. Recommended Practices

- 4.1. For social media pages and groups ...
 - 4.1.1. The best practice is to have the diocese, congregation, or organization create and host all social media accounts representing the diocese, congregation, or organization respectively, and to have multiple administrators and/or supervisors with access to each such account.
 - 4.1.2. Where groups are created, they should be "closed" but not "hidden" or "secret."
 - 4.1.3. All comment and response areas should be moderated if possible, so as to ensure consistency with the goal of the forum. Leaders responsible for such moderation should review and approve comments prior to posting and should not post any comments that (i) do not meet the standards for civility contained in Sections 5.1., 5.4 or 5.6, (ii) misrepresent the position of the Diocese or The Episcopal Church (see Section 3.2), or (iii) include profanity, defamatory language or speech that is otherwise inappropriate or off-topic. In an unmoderated forum, leaders should delete any comments or content that does not meet these standards as expeditiously as possible. All moderation functions should reserve the right to ban repeat offenders. (The Diocese and its agents do not have a responsibility to review or monitor social media sites, pages or groups that are not sponsored and/or owned by the Diocese. However, the Diocese reserves the right to review or monitor such sites, pages, or groups for the proper use of its name and for adherence to these policies and to respond as appropriate.)
 - 4.1.4. A wise practice is to create a member covenant to govern the online behavior of all members of a digital group. Such covenants should include:

² For further details, see the Diocese of Pittsburgh's *Policy for the Protection of Children and Youth*.

³ For further details, see the Diocese of Pittsburgh's *Policy for the Protection of Vulnerable Adults*.

- A description of content that can be posted or published on the site or page.
- Criteria that define (i) who may join and/or view group activity, (ii) when participants should leave the group, and (iii) when, if and how the group will be disbanded.
- Criteria that define appropriate and inappropriate member behavior. (Examples of inappropriate behavior might include bullying and posting pictures that depict abuse, violence, illegal activities, sexual acts, etc.)
- The prohibition of "tagging" photos and videos of children and youth. ("Captioning" of photos and videos is permissible with written permission from a parent or guardian.) The tagging of vulnerable adults should also be discouraged, but may occur with appropriate written permission.
- A clear statement that mandatory reporting laws will be followed.
- A description of the consequences for breaking the covenant.
- 4.2. To ensure that personal websites and social media pages comply with Section 3.2 above, it is recommended that they include a disclaimer that makes clear the distinction between the owner's opinions and those of the Diocese, congregation or organization. Such a disclaimer might read as follows: "*The thoughts expressed here are my own and do not necessarily reflect the position of the organizations with which I am affiliated.*"
- 4.3. For communications with children, youth, and vulnerable adults, ...
 - 4.3.1. Prudent judgement should be exercised in selecting the time of day when contacting a child, youth, or vulnerable adult using any form of digital communication (including texts, chats, or emails). In general, it is wise to refrain from contact before 8:00 a.m. or after 10:00 p.m., except in an emergency.
 - 4.3.2. Parents and guardians should be informed whenever social networking sites and platforms are to be used in connection with a ministry.
 - 4.3.3. Nobody should <u>submit</u> connection requests for personal interactions (such as "Friend" requests on Facebook or "Add Me" requests on Snapchat) to children, youth, or vulnerable adults. A young person or vulnerable adult may not feel able to decline such requests due to the disparity of power between them and the person making the request. An adult who <u>receives</u> a connection request from a child, youth, or vulnerable adult should carefully consider the nature of the contact and whether it would be appropriate for healthy ministry. If she or he is uncertain, she or he should consult another responsible adult before acting on the request.
 - 4.3.4. When possible, communications (including photos, images, and videos) should be sent to entire groups, sent on an individual's "page," or posted in public areas, rather than as private messages.
 - 4.3.5. When sending an email to a child or youth that contains personal or private information regarding them, a copy should be sent to the responsible parent or guardian as well. Examples of these types of emails include payment-due information, specific medical requests or questions, etc. Mass emails sent to an entire group do not need to be copied to parents or guardians so long as the requirement in Section 4.3.2 has been satisfied.

- 4.3.6. Ongoing digital pastoral communications with children and youth should be disclosed to a parent or guardian and/or to a supervisor to determine when a referral to a professional provider or resource might be needed. Such communications with a vulnerable adult should similarly be disclosed to a supervisor.
- 4.4. For social media groups geared specifically toward youth ...
 - 4.4.1. Such groups should have at least two unrelated adult administrators, as well as at least two youth administrators. Youth administrators should be the ones to invite other youth to join an online group.
 - 4.4.2. The parents or guardians of current members should have access to the group site.
 - 4.4.3. The administrators of social networking groups should cancel the access of adult leaders and of youth who have moved away from the area, stepped away from the group, or "aged out" of the program.

5. Additional Cautions

- 5.1. Communications sent digitally (via email, social networking sites or platforms, texts, posts, etc.) are NOT CONFIDENTIAL. They are often visible to the entire world and can be shared by others in ways that the writer cannot control. Remember that what you write is public and will remain public for a very long time (perhaps permanently). Consequently and importantly, respect the confidentiality of matters that are shared with you in confidence, or that are meant to be kept confidential by the nature of your work or ministry.
- 5.2. Authenticity and transparency are important. Avoid anonymous posts and comments, using your real identity to the greatest extent possible.
- 5.3. The Diocese is a thoughtful and prayerful community that encourages free expression and values civil debate. If you disagree with others, do so with civility. Respect your audience, express your views with appropriate language, and be respectful of the Church and its teachings.
- 5.4. Even when members of the diocesan community are engaging in social media for personal use, their comments may be viewed as a reflection on the Diocese. Use your best judgment when engaging in social media activities and be on guard against actions and discussions that could harm the interests of the diocesan community.
- 5.5. Be vigilant when posting links to external sites. News sites and external web pages may contain additional unwanted content and advertising that does not meet our Christian standards.