Social Media Best Practices Checklist for Ministries

A strong digital strategy begins with a good foundation. Social media represents a bold new frontier for mission and is a powerful communications tool. In order to fully realize the untapped potential of the digital mission field, each denominational entity, ministry, or local church is encouraged to download the latest version of the NAD Social Media Guidelines for an in-depth manual with resources and guidance regarding best practices for professional social media communication.

Whether you're just getting started or conducting a social media audit, this check-list is designed to help you make sure basic best practices are in place for your organization or ministry.

The Basics:

- ☐ **Name:** For all denominational entities under the North American Division, use the North American Division name alongside your ministry name whenever possible, and include the full division name (not NAD) in the description for all social media accounts. Please refer to the NAD Brand Guidelines.
- ☐ **Consistent branding:** Use the same name, profile image, header images, and bio on each platform to affirm brand recognition and help members identify official accounts.
- ☐ **Logo:** The branding and logo guidelines for the North American Division apply to social media as well as print and all other forms of communication. Please refer to the NAD Brand Guidelines for more information and downloadable logos.
- ☐ **Optimize images per platform:** Be sure to use the optimal image sizes for each social media platform to help your brand stand out and look professional. Refer to this cheat sheet.
- ☐ **Contact information:** Provide additional contact information such as a phone number, business address, and email address, where relevant, in the about section of your social media account profiles.
- ☐ **Ownership:** Posts should appear to come from the official brand of the account, not from individuals. An exception to this rule would be Church or ministry officials providing a public statement.
- ☐ **Organization:** Plan out your regular content and schedule posts in advance whenever possible. We recommend that you create a shared content calendar for your team.
- ☐ **Content:** Post consistently and be sure to always include an image/video, short teaser text, a call-to-action, relevant hashtags, and a link.
- ☐ **Link back to your website:** Your website is your biggest communications tool; link back to your website in most posts.
- ☐ **Promote your social media:** Include your social media handles (names) in all of your other communication channels, such as your website, emails, print material, and spoken announcements.

Account Management:

- ☐ **Work Facebook accounts:** We strongly recommend that you create a separate work Facebook account to manage official pages to help separate your work from your personal social media.
- ☐ **Facebook page admins:** Facebook pages should have more than one staff admin on the page to prevent lock-out.
- ☐ **Connected emails:** Never connect an organization's social media profiles to private email addresses or even an individual's work email addresses.
    - ☐ Create a dedicated social media address (**socialmedia@yourministry.com**) for your organization and grant multiple people access. Contact your IT department for assistance.
    - ☐ Connect accounts like Twitter, Instagram, and Hootsuite to the work social media email address.

- ☐ **Page roles and access:** Regularly check Facebook page roles and account access to make sure it is up-to-date and does not include former employees. When social media managers/page editors/admins leave your organization and no longer require access to your social media accounts, update page roles immediately and change passwords to all social media platforms, management accounts, and emails.

Account Protection:

- ☐ **Security:** Please keep your account privacy and security settings up-to-date with the latest best practices. This also applies to your laptops and devices.
- ☐ **Facebook:** We highly recommend that you set up the following safe-guards:
  - ☐ **Two-factor authentication:** Two-factor authentication creates an extra layer of protection for log-ins from unknown browsers. This will safeguard against hackers who could otherwise take control of, not only personal profiles, but also organizational pages, ad accounts, and credit cards through hacked personal profiles. Click here to learn more about two-factor authentication.
  - ☐ **Trusted contacts:** Choose coworkers to be trusted Facebook contacts to help you regain access to a compromised account.
  - ☐ **Follow Facebook's recommended security updates:** Learn more about Facebook security features and tips here.
- ☐ **Passwords:** For all social media accounts (personal and organizational), please choose strong, unique passwords and change them every six months.

Ideally, organizations should conduct a basic social media audit every six months as part of a larger digital communications strategy review. The digital mission field is dynamic and ever-changing, and our department is here to help you stay informed. If you were able to check off everything on this list, visit SDAdata.org for more resources, tips, and tutorials to continue to enhance your digital evangelism and discipleship strategies.