



APPNA Oklahoma Chapter

Digital Information and Social Media Policy

1. Access and Handling of Member Information by Office Holders:

- a. Office holders of APPNA Oklahoma are required to adhere to strict confidentiality guidelines when handling member information.
- b. Member information should only be accessed by authorized personnel and should be used solely for the purpose of carrying out official duties.
- c. Office holders should not disclose or share member information with any third parties without the explicit consent of the member, unless required by law.

2. Social Media Posts:

- a. Office holders should exercise caution and professionalism when posting on official social media platforms and website.
- b. Posts should not contain any confidential or sensitive member information, unless explicit consent has been obtained.
- c. Office holders should ensure that their official social media posts reflect positively on the non-profit organization and do not bring discredit to its reputation.

3. Use of Members, Volunteers and Participants Pictures and Videos:

- a. APPNA Okla will include photo/video waivers, disclaimers, and consents when members, volunteers, participants, and their accompanying minors are registering for events. These waivers, disclaimers, and consents will allow the organization to use their pictures or videos for promotional purposes.
- b. However, in cases where registration is not required for an event, a disclaimer will be included on the promotional materials and flyers. This disclaimer will state that by attending the event, attendees are implying their consent for the organizers to use their photos and videos for informational and promotional purposes. Additionally, at each of these events, an announcement will be made to notify the participants of this policy.
- c. Unofficial photos and videos shared by non officials on personal/private accounts is not the responsibility of the organization to monitor or control.

4. Consent and Waivers:

a. Outside of an event, APPNA Oklahoma will obtain written consent from its members, volunteers, and participants for the use of their information, pictures, or videos for promotional purposes. APPNA Oklahoma will also maintain records of the consent and waivers obtained.

b. Consent and waivers should be stored for 3 years and secured and accessible only to authorized personnel.

5. Training and Education:

a. APPNA Oklahoma will provide training and education to office holders, members, and volunteers on the importance of data privacy, confidentiality, and responsible social media use.

b. Regular updates and reminders will be provided to ensure everyone is aware of their responsibilities under this policy.

Exemption from Liability and Access Privileges for Officials

1. Membership and Roles:

The officials referred to in this policy include members of the Executive Committee and representatives of the Digital Media Committee or special members designated to the role by EC. These individuals are appointed to their respective positions within the organization and are entrusted with specific responsibilities related to the management and administration of the organization's digital platforms.

2. Access and Best Practices:

The officials mentioned above shall have access to the organization's website and social media platforms as necessary to fulfill their roles and responsibilities. However, this access is subject to compliance with the organization's digital information and social media policy, including following best practices of cybersecurity. The officials are expected to implement appropriate security measures, such as strong passwords, regular updates, and adherence to cybersecurity guidelines including limiting access to unauthorized personnel, to safeguard the organization's digital assets and member information.

3. Exemption from Liability:

In the unfortunate event of a breach of member privacy caused by circumstances beyond the control of the officials, such as hacking or unauthorized access, the officials shall be exempt from any liability. It is understood that despite implementing reasonable security measures and following best practices, cyber-attacks can occur, and the officials cannot be held responsible for such breaches.

4. Reporting and Mitigation:

Notwithstanding the exemption from liability, the officials bear the responsibility of promptly reporting any breaches of security incidents to the appropriate stakeholders/authorities and taking necessary steps to mitigate the impact and prevent further breaches. This includes investigations and implementing additional security measures as needed.

5. Obligations and Continuous Improvement:

This exemption from liability does not absolve the officials from their obligations to comply with the organization's digital information and social media policy. They are expected to continue maintaining the necessary security measures and safeguarding member information to the best of their abilities. The organization remains committed to regularly reviewing and enhancing its security protocols to prevent and mitigate breaches.

By including these provisions, the organization aims to clarify the roles, responsibilities, and access privileges of the mentioned officials while providing them with reassurance regarding liability in cases of breaches beyond their control.

Please note that this policy is subject to review and may be updated periodically to align with changing laws and best practices in digital information and social media management.