Social Media Policy

This policy governs the publication of, and commentary on, social media by employees of the Nina Mason Pulliam Charitable Trust (the Trust). This policy is in addition to and complements any existing or future policies regarding the use of technology, computers, email and the internet.

Social Media Defined

When most people think of social media, they think of the tools: social networking (Facebook), video-sharing (YouTube), blogging (Wordpress), micro-blogging (Twitter), photo-sharing (Flickr), podcasting (Blog Talk Radio), mapping (Google Maps), social voting (Digg), social bookmarking (Delicious), lifestreaming (Friendfeed), wikis (Wikipedia), virtual worlds (Second Life) and others. While all these tools do fall under the same category of social media, they are all different from each other, and new and hybrid tools are being introduced almost every day. This policy applies to all current and future forms of social media (hereinafter collectively referred to as “social media”).

The Trust and Social Media

The Trust regards social media as primarily a way to connect and build relationships with grantees and community stakeholders and raise awareness of causes related to the Trust’s mission. As social media becomes more a part of our daily lives, and as personal use of social media can affect the Trust’s mission and its grantees’ activities, it is important that Trust employees understand the proper use of social media.

The Trust has developed a two-part policy related to staff members’ social media activities: the first part of this policy addresses certain employees who have the authority to maintain the Trust’s official social media presence, and the second part of this policy offers guidance related to personal social media activities as such activities relate to the Trust. The Trust takes no position on an employee’s desire to start a blog or participate in social media activities, but it is committed to maintaining a workplace that is free from harassment and to prevent unauthorized disclosure of confidential and/or proprietary information.

Part 1: Official Trust Social Media Profiles and Administrators

As of the adoption of this policy, the Trust maintains an official social media presence on Facebook and Twitter. The profiles are managed by three Administrators: the president and CEO, communications manager, and an Indiana Social Media Administrator (collectively referred to as “Administrators”). All three Administrators are able to post to the Trust’s social media profiles, but the communications manager has the primary responsibility of maintaining, updating and responding to comments on the Trust’s profiles.

While only Administrators are authorized to post to the Trust’s official social media profiles, we recognize that many Trust employees may have connections to the Trust’s grantees, stakeholders and communities we serve, and can serve as valuable contributors of ideas and content for the Trust’s social media presence. All employees are encouraged to recommend to Administrators content for posts and suggestions for sharing of information from others’ profiles on Trust accounts.

Social Media Objectives

- To increase awareness of the Trust and its mission among target audiences
- To increase awareness of grantee activities and accomplishments, and expand the reach of grantee communications efforts
- To enhance relationships with grantees, stakeholders, key influencers and media
- To contribute to, and at times initiate, the dialogue surrounding topics of importance to the Trust and the communities it serves
- To help establish the Trust as an authority in key priority giving areas

Social Media Management for Administrators

- Professional (i.e., not personal) social media identities, logon IDs and usernames must be approved by the president and CEO.
- Administrators may not create social sites, pages, profiles, groups, events or identities on behalf of the Trust without authorization from the president and CEO.
- The communications manager is responsible for creating, monitoring and managing all official Trust social media accounts.
- The communications manager is responsible for posting and approving posts to all official social media sites.
- All account information (email addresses, usernames, passwords, etc.) must be shared with the President and CEO.
- While it is understood that social media norms and post-length constraints may sometimes result in use of less formal language and abbreviated language and symbols (i.e., ampersands, hash tags, etc.), Administrators should consider AP Stylebook guidelines and the Trust's brand voice when developing posts.
- Administrators must spell check each post prior to publishing.
- Monitoring
    - Monitoring of social media sites must be done DAILY.
    - The communications manager will monitor all comments, messages, reviews and instances when the Trust is tagged by another user and will respond as needed within a timely manner (within one business day).
    - While it is not necessary to respond to every general or favorable comment, it is good practice to do so in most cases, such as when another user compliments the Trust or Trust employees, acknowledges a Trust award or recognition, or makes a compelling or thoughtful contribution to a Trust conversation.
    - The Trust will quickly address any unacceptable messages or misuse. Examples of unacceptable content include spam, advertising, knowingly and deliberately posting false information, foul language, or unconstructive criticism of the Trust's services or its grantees and strategic allies. Unacceptable content also includes discriminatory, violent, vulgar, obscene, threatening, intimidating, or harassing messages.
    - The communications manager has the authority to remove comments that the communications manager deems unacceptable, block offensive commenters, or post timely responses to such unacceptable comments. The communications manager will

    - advise the president and CEO, and the Trustees when appropriate, of any such unacceptable comments and the communications manager's response.
    - The Trust will maintain a disclaimer on each of its social media profiles warning against unacceptable comments.
    - In addition to posting original content on Trust accounts, Trust Administrators will monitor grantee, strategic allies' and news profiles for relevant posts to share (with proper attribution) on the Trust's social media sites.
- Tagging
    - Administrators should use careful judgment when tagging individuals and organizations in posts. Be sensitive to whether the content and context is appropriate for those being tagged (i.e., consider whether individuals served through the Trust's social programs want others to know they have availed themselves of such programs; do not tag minors without written permission from the appropriate authority).
    - The communications manager will monitor all instances when the Trust is tagged by other parties and will address any unacceptable or inaccurately applied tags.
- Google Alerts
    - The purpose of setting Google Alerts is to know what is being said about the Trust online.
    - The communications manager will monitor all alerts and immediately address any discrepancies.

Part 2: Personal Social Media Activities With Respect to the Trust

Representing the Trust

All Trust employees could be viewed by third parties as representing the Trust, so you must be thoughtful about how you reference the Trust in your personal social media profiles. Employees are representing the Trust in situations that include the following:

- Identifying the Trust and your present affiliation with the Trust as the source of your expertise and/or knowledge of a subject
- Using the name or logo of the Trust in any profile or description
- Acting as a designated speaker authorized by the president and CEO
- Attending a Trust event or other event on behalf of the Trust
- Authoring an article, blog post, commentary or official social media post on behalf of the Trust
- Serving as a member of a board or committee as a result of your employment with the Trust

Employees may not create social sites, pages, profiles, groups, events or identities on behalf of the Trust without authorization from the president and CEO.

Guidelines

When representing the Trust in personal social media profiles, employees must abide by the following guidelines:

- No lobbying. Employees are specifically prohibited from lobbying while serving in an official capacity as a Trust staff member. See the Trust's Code of Ethics policy and the Employee Manual for guidance relating to lobbying and advocacy. Please note that joining online groups or using social media in any form that takes a position on legislative efforts could be construed as lobbying. While not prohibited, officers of the Trust are discouraged from doing so, and any employee engaging in such commentary should be specific in stating, “My opinion and political views do not reflect the ideology, strategy or mission of my employer.”

- Remember who you represent. Be aware of your association with the Trust when representing the Trust in online communications. A good rule of thumb is to think of all social media as the same as writing a signed letter to the editor or a newspaper. Clearly state who you are and your relationship to the topic, particularly if you are participating in a professional or community discussion. Do not write anything that you would be embarrassed seeing in a news headline. When making comments on, or replying to others’ comments on, the Trust’s official social media profiles, avoid topics or comments that may be considered generally objectionable, offensive or inflammatory. Please bring any misrepresentation of the Trust that you notice to the attention of the Trust’s communications manager and feel free to ask for guidance in considering your social media responses.

- Protect confidential and proprietary information. Employees should be mindful of the trust placed with us by our grantees and applicants, trustees, and stakeholders. They have a right to expect we will protect their information and maintain their confidentiality. Employees must maintain the confidentiality of the Trust’s private or confidential information discussed at board meetings. Do not post internal reports, policies, procedures, or other internal business-related confidential communications. Do not discuss grantees’ or other stakeholders’ internal personnel issues or confidential information.

- Discussing the Trust in Social Media. If the Trust is the subject of the content you are creating, be clear and open about the fact that you are a Trust employee, and it should be clear that the views and opinions expressed are yours alone and do not represent the official views of the Trust. It is best to include a disclaimer on your social media profile such as “The postings on this site are my own and do not necessarily reflect the views of the Nina Mason Pulliam Charitable Trust.”

- Respect copyrights and fair use. Respect all copyright and other intellectual property laws. Always give people proper credit for their work, and make sure you have the right to use something with attribution before you publish. Cite and link to your sources.

- Compliance. Know and ensure your compliance with all applicable Trust organizational policies. In using social media, you may confront scenarios addressed within the Trust’s Employee Handbook and Code of Ethics Policy, especially those regarding conflict of interest, confidentiality/privacy and technology use. Comply with the Terms of Service of each online site you use.

Using Social Media at Work

Updating personal social media accounts must not interfere with the timely accomplishment of your regular work duties and expected productivity levels. Writing, managing and updating personal blogs is not permitted during work hours.

Disclaimer

This policy does not, in any manner, prohibit employees from discussing among themselves or others wages, benefits, and other terms and conditions of employment or workplace matters of mutual concern that are protected by the National Labor Relations Act.

Enforcement

The Trust may access without notice all electronic communications made at the workplace or on employer-issued devices. Employees should have no expectation of privacy related to any information or data placed on any Trust computer or computer-related system, or that is viewed, created, sent, received or stored on any Trust computer-related system, including without limitation, electronic communications or Internet usage.

Failure to follow the Trust's Social Media Policy may lead to disciplinary measures, up to and including termination of employment.