A RESOURCE OF THE 2020 DATA EMPOWERMENT REPORT

Sample Web Content and Social Media Policy

NOTE ABOUT THIS SAMPLE POLICY

This policy is written from the perspective of an organization offering stigmatized services and doing community organizing. Your organization may face more or fewer risks, but your policy should still include all the high-level elements outlined here.

When writing a web content and social media policy, balancing free speech and effective organizing with safety is crucial. This policy isn't intended to keep everyone wholly safe but to help guide people towards that healthy middle ground.

Our Accounts

We have a Facebook Page, Twitter account, and Instagram account. Our website runs on WordPress and is hosted by DigitalOcean. All accounts are managed by the communications team. If you'd like something posted, please reach out to them.

Our communications strategy is set by our Director of Communications in collaboration with the rest of our organization. If you have a concern or idea about our strategy, please add it to the agenda for one of our organization-wide staff meetings.

Politicized Content

We use our social media and website to further our work towards an equitable society. Therefore, we do post content that endorses a particular worldview and might be considered political. However, we will not (without specific discussion) post the following:

- Direct attacks on an individual or institution.
- Unverified information / re-posting of other content without proper vetting.

We may, at times, choose to directly confront individuals or institutions. These posts must be approved by our communications director.

Use of Stories & Photos

We may sometimes post stories about our program participants. When we do so, we take the following measures to protect our constituents from harm and properly represent their needs:

- We speak with constituents about the possible risks of using their stories and make sure that consent is fully informed.
- We provide our constituents with a final version of any post before it goes live and offer an opportunity to make corrections.
- We use strength-based narratives and do not sensationalize stories of struggle.
- We make clear that consent can be revoked at any time, for any (or no) reason.
- We compensate constituents for stories that are used in fundraising events or campaigns.

Although we do not follow the same consent process for photos, we do take steps to ensure we don't use people's photos without their permission:

- At all events, we ask participants for consent and work with photographers to avoid taking pictures of those who are unwilling.

We will take down any photo of any constituent or partner at any time for any (or no reason).

Security

Content posted to social media can reveal sensitive details about our work and about our constituents. Remember the following when posting:

- Disable location tagging in posts.
- Do not post pictures of people's faces without consent.
- Do not tag people without their consent.
- Check for visible documents, whiteboards, and other written content in photos before posting.

Representation

When posting to social media, consider who we are featuring in our pictures and narratives. It is vital to represent varying races, genders (including gender variant presentations), abilities, and cultures. At the same time, we want to avoid misrepresenting our community or tokenizing any individuals within it.

It is hard to manage this balance. Talk to our Director of Communications if you need help. First, however, a few basic guidelines to get you started:

- Consider who is currently present in our programs, funders, staff, and community and who we want to be present. Post content that represents where we want to go but does not suggest a vastly different membership than already exists. For example: do not use stock imagery of an all-Black community for programs almost entirely staffed and attended by white people. But also do not use a photo of all white people in a board room.

- Do not use a photo or a narrative of the "one Black/Latinx/Trans/Woman" in the room to suggest we have achieved greater diversity than we have.
- If it is not relevant to a person's narrative, do not name specific identities with the hope of suggesting we have achieved greater diversity than we have.
- Avoid using stock imagery that is based on corporate white supremacist norms. Instead, be sure that the people featured in images are culturally accessible to our community.
- Consider many kinds of representation: race, gender, sexual orientation, family composition, ability, class, geography, and culture.

Accessibility

The U.S. federal government has a surprisingly helpful social media accessibility toolkit you might want to use as a reference.

Like anything else we publish, social media posts should include accessibility. So be sure to consider the following when posting:

- Include an image description in the description or a pinned comment for all photos and illustrations.
- Our community uses both English and Spanish. Therefore, post in both languages, when possible, or alternate the language of posts if not.
- Post on multiple channels. Not everyone uses Instagram, be sure to post content to as many channels as possible.
- Use accessible language (avoid white-supremacist corporate talk). Use common words, active voice, and avoid jargon. Prioritize readability over style.
- Close caption all videos in English and Spanish or use a platform that provides automated captioning (e.g., YouTube).
- Use descriptive text for all links. Make sure that the full description of the link is included in the text of the link.
- Use built-in styles (e.g., header 1, body text, subtitle) in any platform that supports it. These styles are used extensively by screen readers.

Personal Social Media

Your social media is your own. However, we ask that you:

- Do not post using the voice of our organization. It is OK to re-post or share content from our accounts.
- Do not post any information about individual constituents you might work with – including photos.
- Do not post anything that might reveal sensitive information about our activities – including photos of meetings, information about our strategy, etc.

It's possible that the work you do could make you a target of online trolls or activist hackers. They might attempt to gain access to your social media (either through hacking or just by viewing public information) to discredit you or harass you or your family. To protect yourself, we recommend you take the measures on the following page.

RECOMMENDATION	APPLIES TO	DESCRIPTION
Use strong passwords	All social media networks	Use strong passwords on all of your social media accounts. You should use a password manager to make this easier.
Use multi-factor authentication (MFA)	All social media networks	Using multi-factor authentication on your accounts is the best way to prevent your account from being taken over. App-based MFA is more secure than SMS codes.
Use a recovery PIN	WhatsApp & Signal	Recovery PINs prevent people from stealing your WhatsApp and Signal accounts by creating a copy of your SIM. Whenever you set up these accounts on a new device, you'll need to enter this PIN to confirm your identity.
Hide your friends list	Facebook	Trolls and hackers will use public friends lists to map out networks of activists. Hide your friends list to keep your community safe.
Hide contact information	Facebook	Trolls and hackers will use any public contact information (especially your phone number, email address, and birthday) to find other information about you. Make sure these are hidden.
Don't post sensitive photos	All social media networks	Governments often use pictures taken at political events to find other people to target. Never post photos of political activities that include other people's faces.