nten

Published 10/21

A RESOURCE OF THE 2020 DATA EMPOWERMENT REPORT

Safe Communication Policy

NOTE ABOUT THIS SAMPLE POLICY

This sample policy includes elements inspired by GDPR privacy policies, ethical data use guidelines, and various other standards. We don't claim that it fully complies with the legal requirements your organization is subject to. Instead, it's a starting point for a policy that centers you community. This policy represents an ideal. It is more specific and more transparent than most nonprofits will be able to achieve.

Be sure in particular to adjust this policy for the specific risks your community members face. Staying safe from the police, from intimate partners, and from community members all require different measures. You need to understand and adjust for the technical and physical context in which your community lives. When in doubt, *ask* what they need to be safe.

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 of the high level elements outlined here.

This policy provides guidance for safe communication with our constituents, partners, and funders. This is an internal policy, do not share outside of our organization.

Top Risks

CONSTITUENT	WHAT WE ARE WORRIED ABOUT
Program Participant	• Intimate partner or guardian learning about their participation in our program and hurting them • Community member learning about their participation in our program and making them feel like their privacy was violated
Partner Organization	• Information about our strategies getting out of the coalition and compromising our organizing efforts
Staff Member	• Participation in our sensitive programming work getting out and bringing attention from online trolls who oppose our work
Our Organization	• Details of our work drawing public attention causing pressure on funders / government to restrict our activities

Considering Physical Context

When communicating with participants remember that they may not have autonomy or control over their physical environment and devices. It is important to communicate in a way that lets them make their own choices about voicemails, text messages, and other kinds of communication that could put them in danger. Program participants might have their communications monitored, their devices mirrored, or be physically surveilled.

During intake ask the program participant how they would prefer to be contacted, when they can be contacted, and if there are steps we can take to keep them safe. Document this in our database. Do not send text messages or leave voicemails with identifiable information. Always call from one of our anonymous lines without caller id.

Although not preferred, it is acceptable to communicate with program participants using their existing tools (e.g., Instagram DM, WhatsApp, etc.). Please don't use personal accounts for this – create a generic account that doesn't use our organization name. Talk to your supervisor if you need help.

If community members are scared but do not know how to stay safe, suggest that they create an email account just for communicating with us. After setting up conversations, use our anonymous phone line or an anonymous video calling platform like Jitsi for the meeting itself.

Approved Communication Tools

TOOL	DESCRIPTION
Signal	• Fully encrypted end-to-end messaging platform. Setup disappearing messages for all conversations. • This is the most secure method but most people haven't ever used Signal and may not be comfortable learning a new tool. • You can use Signal for all sensitive conversations with program participants and partner organizations. Do not use for conversations with funders or within our organization. Track all program participant conversations in our database.
Our Email Accounts	• Our email accounts hosted on Google Apps. Remember that these email accounts include our organization name, so don't send emails to program participants without their consent. • Email is moderately secure. You can use it for any conversation with program participants (with consent), partner organizations, funders, or each-other except for specially protected information like social security numbers and bank account information. • Consider using Signal for sensitive organizing conversations. It is less likely that Signal messages will be forwarded and get outside the coalition.
Google Meet & Chat	• Our internal meeting and chat platform, hosted on Google Apps. Please keep all internal conversations and meetings on this platform so that we can maintain a record of important conversations and make sure the proper security controls are in place.
Jitsi	• An anonymous and secure online meeting app, useful when meeting people outside the organization.
Our VoIP phone lines	• Our VoIP phone lines let you make calls from your computer or phone. We do not have our organization name linked to the caller ID to help keep our program participants safe. You can use these phone lines for any conversation.

Keeping your Devices Secure

Your work computers are kept safe by our IT provider. All of the data on our laptops is encrypted, strong passwords are enforced, and we can remotely wipe the device if needed.

However, we all have sensitive data and communications on our personal phones. It’s your responsibility to make sure that your phone:

- Has a strong passcode set (at least 8 characters)
- Has disappearing messages configured in Signal for all work-related conversations
- Is set to wipe after several unsuccessful unlock attempts