Published 10/21

A RESOURCE OF THE 2020 DATA EMPOWERMENT REPORT

Data Policies Your Nonprofit Needs

Policies can be useful, we promise. In this article, we explore the data-related policies your nonprofit should consider. These policies cover everything from security to privacy to ethical use.

Policies are only helpful if they are read and followed. So, don't treat this like a checklist. Instead, use your instincts to decide what policies (and in what format) will work for your organization.

Data Inventory

A data inventory is the most basic of all data policies. They list all kinds of data (client records, donor information, politically sensitive documents, etc.) that your organization needs to protect. For each of these kinds of data, a data inventory should include:

- A description of the data.
- Where that data can be stored.
- How that data can be shared securely.

For more details about data inventories, read **Getting Started With a Data Inventory** (an additional resource of the Data Empowerment Report). We've also created a sample data inventory to get you started.

Data Privacy Policy

Data privacy policies are *external-facing* policies that explain what data you collect, how you'll use it, and for how long. You might have one for your website, but nonprofits need privacy policies across all services. Our constituents should know what data we are storing, who internally and externally will access it, and why. Your privacy policy should tell constituents:

- How to opt-out (or the impacts for getting services of opting out).
- How to exercise their "right to be forgotten."
- How to request a copy of their data.
- When and how algorithms are used to make decisions about them.
- Who to complain to.

Many constituents will never look at our website. So be sure to distribute in paper, over email, and in whatever other ways your communities need.

We've written a sample data privacy policy to get you started.

If you are subject to GDPR or certain state governments, you might be legally required to include specified elements in your privacy policy. If not, the GDPR guidelines are a helpful place to start.

Data Sharing Policy

Data is a significant currency in the nonprofit world. We constantly share details about our work with donors, funders, partner organizations, and governments. But, have you written down what is OK to share and what isn't? A data sharing policy outlines your staff's legal and ethical responsibility to your constituent's data.

Your data sharing policy should include:

- Who within your organization is allowed to access various kinds of sensitive data?
- Standards for anonymizing data before it is shared widely.
- Any legal reporting or data sharing obligations.
- Under what circumstances and to whom can your staff discuss details about a constituent.
- What data you share with partner organizations, and how you vet their use to ensure it's ethical.

Further reading: How to Create a Nonprofit Incident Response Plan from Community IT

Safe Communication Policy

Organizations that work directly with community members may need a safe communication policy. This policy keeps your constituents safe from abusers, governments, or activists who might want to hurt them.

Your safe communication policy should include:

- How to ask your constituents what they need to stay safe.
- How to leave a voicemail and send text messages without risking identification.
- When encrypted messaging tools should be used (like Signal).

Web Content and Social Media Policy

Our websites and social media are powerful ways of sharing our work and connecting with others. But they can also be a major risk. What we post can misrepresent our communities, draw unwanted attention, or be the target of online trolls looking to discredit or harass.

Your web content and social media policy should include:

- How you manage politicized content – what you'll post and what you won't.
- Use of constituent photos and stories.
- How to achieve diverse representation without tokenizing or mispresenting your services.
- Security risks of posting locations, photos of people's faces, and other sensitive content.
- Accessibility.

Data Retention Policy

Don’t keep your data forever. The more data you have, the more that can be leaked or stolen. Besides, are those constituent records from 12 years ago still useful? Instead, have a documented policy for how long you’ll keep various kinds of data. You can add this to your data inventory or create something that stands alone. Be sure to consider email, files, client records, and staff records.

Your data retention policy also needs to cover *how* the data gets deleted. Who is responsible for deleting old data? How do they determine the date for deletion? What technology tools are used to enforce it?

Further reading: Document Retention Policies for Nonprofits from National Council of Nonprofits