



NNEDV

Privacy Policies and Terms of Service: Best Practices

When survivors search for help online, they're often accessing websites of victim service programs. In addition to getting educational information about domestic violence or sexual assault, many websites make it possible for survivors to reach out to the program through email, contact forms, or web-based chat, and to engage online with the program in other interactive ways. Because of the significant privacy and safety issues survivors of domestic and sexual violence face, it's important that programs offer clear information about the benefits and risks of seeking information and help online.

As with all victim services, it's important to make sure that the policies and practices related to your website and chat hotlines support informed consent. You should inform survivors about any potential risks they face when using your website. Depending on the terms of service and privacy policies, some survivors may choose to limit their use of your website or chat service, or choose not to use them at all. Providing clear information about privacy and safety risks gives survivors a chance to make choices that match their privacy and safety concerns.

Privacy Policies & Terms of Service

Privacy Policies are important (and in some places required by law) if you collect any personal information from visitors to your site, including name, email address, phone number, IP address, etc. The policy should describe what information you collect, why you collect it, how you protect it, how long you keep it, how someone can opt out, and how you use it.

Terms of Service set out an agreement about how your site can be used, and offers important disclaimers to those who decide to use it. Terms of Service are not required but are highly recommended. They can complement your privacy policy, and offer guidance for survivors about the benefits and risks of using your website or online chat services.

Both Privacy Policies and Terms of Service should be meaningful, clear, and include specific information (see below).

Meaningful

A major concern is that most people don't actually read Terms of Service or Privacy Policies. When prompted to review them, many people simply click "agree" or "ok" and move through the site. For a survivor with elevated privacy and safety risks, that could be disastrous. So be sure to briefly and clearly explain why you are telling them about your privacy policy and terms of service, and encourage them to read through them. Of course, there may be many circumstances where survivors in crisis don't have the time to thoroughly review these, so it's important to succinctly and prominently highlight the primary safety and privacy risks they need to consider.

Both the privacy policy and terms of service, as well as the way you share information about them, should be rooted in foundational values like respect, empowerment, and choice. Make it clear that you value their privacy.

Clear

Use plain language as much as possible. This means sharing content that is easy to read and understand, and that avoids jargon. Share the key points of your confidentiality and privacy policies and practices, and provide links to the more legal or specific information so that survivors have the choice to dive deeper if they want to.

Include Specific Information

As you seek to balance being clear and brief with the need to be thorough, the following information should be included in your Terms of Service:

1. Privacy and Safety Information

- a. Key points from your Privacy Policy
- b. What kind of information could be personally identifying
- c. Your organization's obligation to protect personally identifying information, and the limits of that protection, including:
 - i. How mandatory reporting may impact that obligation
 - ii. How your program responds to court orders, warrants, government requests, and subpoenas
- d. How your organization handles breaches of personal data
- e. Third parties that have access to the person's information (including digital services platforms, internet service providers, IT personnel, backup data storage providers, or cloud servers)
- f. How their information is used in grant reporting, for example explaining that personal information is not shared but aggregate data is.
- g. Liability information (as advised by attorney)
- h. Anything that needs to be disclosed related to the website developer or online chat vendor's Terms of Service, with links to those policies.

2. What they can expect from your service

- a. Any limitations of the service (not 24 hours? Wait times? No records kept even if someone contacts more than once?)
- b. What can minors accessing the service expect?
- c. What languages your services are offered in, and when you use interpreters
- d. Who to contact with questions
- e. How your program will respond to abuse of the services (e.g., harassment of advocates, spamming, hacking, etc.)

Here are some examples of Privacy Policies.

- [Electronic Frontier Foundation](#)

- [Electronic Privacy Information Center](#)
- [National Network to End Domestic Violence](#)
- [National Domestic Violence Hotline](#)
- [RAINN](#)

[Read more](#) about the differences and what should be included in Privacy Policies and Terms of Service.

© 2019 National Network to End Domestic Violence, Safety Net Project. Supported by US DOJ-OVC Grant #2017-VF-GX-K030. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ.

We update our materials frequently. Please visit [TechSafety.org](https://www.techsafety.org) for the latest version of this and other materials.