Frontline Services' Best Practice Guide: Your Website

This guide is for workers in frontline service organisations who have responsibility or influence over the organisation's website or online presence. It provides recommendations and issues for you to consider, to assist you in creating an online presence for your organisation that is effective and safe for victim-survivors of family and domestic violence.

Benefits of Being Online

Almost all victim-survivor frontline services have a website, social media page, or some other online presence. An online presence can help you share information about your services, raise community awareness about domestic violence and sexual violence, and make it easier for people to connect your organisation. However, we recommend you take steps to ensure that the safety and privacy of the individuals who reach out to your service for help is protected.

1. Add a Safety Alert to Your Website

Many abusers monitor survivors' online activities. Methods include simply looking over their partner's shoulder, manually going through the internet browsing history, or installing computer or mobile phone monitoring software. Adding safety alert information on your website reminds survivors that their activities could be monitored or viewed by someone else. Keep in mind, however, that safety alerts will not prevent the abuser from seeing what the survivor is reading online if monitoring software is installed or if the survivor doesn't erase the browsing history. A safety alert is more about educating and reminding the survivor about possible monitoring. Visit techsafety.org.au/resources for an example of the language we use in our safety alert, which we call a "safety check."

2. Create A Quick Exit Button

Some websites have a quick escape or quick exit button on the webpage so a survivor can be redirected to an innocuous webpage with a single click. Quick escape buttons only protect the survivor from immediate over-the-shoulder monitoring, such as when the abuser walks in and the survivor needs to quickly close a webpage. This button will not prevent the web browser from including the webpage in the browsing history. If survivors think that their abusers are going through the browsing history, they can manually erase specific webpages from the browser history. Deleting certain websites and related searches from the browsing history might be safer than clearing all history in case the abuser becomes suspicious that the entire browser history has been deleted.

3. Provide Information About Internet Safety

Providing information about internet and technology safety on your website can be helpful for survivors. This information may help them figure out how they are being monitored and strategise for their safety more effectively. If survivors can communicate with you through your website or

other online spaces, be upfront about the safety risks in using each form of communication. For example, if they send you an email, the email may be stored in their sent mail. The more knowledge a survivor has, the more informed her decision about how to access your agency's resources will be. You are welcome to publish a link to WESNET's technology safety information, rather than create your own content. Read more about our permission for use. [https://techsafety.org.au/permission-for-use/]

4. Use A Web Form Instead Of Email Addresses

Some survivors will want to email your service to ask for help or resources. However, it is safer for services to provide a web form where the survivor can submit their message, instead of listing the email addresses of staff. A web form doesn't leave a record of the email in the sender's email sent folder, which the abuser could find by going through the survivor's email account. Web forms also offer staff more privacy, because their contact details aren't publicly available, and can be configured so that enquiries are sent as email messages to staff. Be aware that if the abusive individual is monitoring the computer with spyware, a web form will not conceal that a survivor has reached out for help. If a survivor suspects her online activities are being monitored, it is safer for her to submit an enquiry from a safer computer.

For more information about safe email practices with survivors, read this handout. [https://techsafety.org.au/blog/2017/07/14/youve-got-mail-privacy-safety-tips/]

5. Limit Survivor Information Online

In general, agencies and workers should not share information about survivors without the permission of the survivor. When agencies are implementing social media/online campaigns to raise awareness about domestic or sexual violence, make sure you obtain written consent from a survivor before sharing any information about them. For survivors to be able to give informed consent, you need to inform them of exactly what information will be shared, who will potentially see the information, and possible consequences of sharing this information.

6. Posting Pictures & Videos

Before your agency posts any pictures or videos online, be sure to obtain informed consent from those in the pictures or videos. If you are hosting an event where you will be taking photographs or videos, allow anyone present to opt out of having their image captured. They can identify themselves to staff so the photographer keeps them out of frame or you can have a designated area for those who don't wish to have their image posted online. Don't forget that you should also get permission from staff, members of your board, presenters, and anyone else present; do not assume that because they work for your agency or were invited to speak publicly for you, that they are willing to have their images posted online.

7. Offering Services Online

Many organisations may be tempted to connect with survivors and provide services through online spaces, such as social media, forums, or chatting websites. Most of these websites are not

built to offer secure, private, and confidential conversations. Additionally, using the internet to communicate adds another layer of safety risks and privacy planning that workers and survivors must think through. While it might be possible to connect with survivors through these spaces, it's important to think through all the risks to privacy and safety that may exist, which include general online privacy concerns and possible misuse by the abuser. You may need to consult with someone who has technology safety expertise to ensure your risk assessment is thorough. If you decide to engage with survivors through online spaces, it's also important to develop detailed policies and procedures for staff, that address the identified risks.

8. Include Accurate Information

The internet is global, which means that anyone can access your website or online platform. If you have information online that is specific to your area (county, state, region) make that clear. Some laws and legal processes (such as orders of protection) or services (such as state-wide hotlines) are state or region specific. Survivors who visit your site may be from across the country or even another country and need to be informed that some or all the information provided might not be applicable to them. We also recommend you list area codes with any hotlines and phone numbers, as well as office hours and your time zone, so survivors know when to contact you for help.

9. Accessibility

Make sure your website is accessible to all people, including those who are blind or have low vision, or are deaf or have a hearing impairment. Check that images on your website have alternative text descriptions (html alt text). For links, make sure there is concise and descriptive text within each link (and within the html title tag) that describes where the link takes a visitor. Doing so will ensure that someone who is accessing your site or page via a screen reader can listen to helpful and accurate information. If posting video or audio, include captions or transcripts so those who are deaf or have a hearing impairment can also access the information. Ask your website developer to comply with accessibility standards, or you may like to consider accessibility guides, such as this Australian Government guide. (https://guides.service.gov.au/content-guide/.)

Summary

1. Add a safety alert to your website.
2. Add a quick exit button to your website.
3. Provide information or link to WESNET's information about internet safety.
4. Use a web form on your 'Contact Us' page instead of listing staff email addresses.
5. Obtain written informed consent from a survivor before sharing any information about them online.
6. Obtain informed consent from anyone before sharing their image (photo or video) online.
7. Conduct a thorough risk assessment (and get expert advice if you need it) before providing services to survivors via online spaces.
8. Make it clear when information relates to a particular country, state and/or region.
9. Ensure your website is accessible to all people, including those with disability.