BC Society of Transition Houses

Anti-Violence Program's Guide: Online Chat and Messaging

Some anti-violence programs use online chat or messaging as another way to communicate with program participants. This platform can useful for those people who are not ready to speak to someone on the phone and it can increase accessibility for some program participants. Programs can use online chat and messaging as a hotline for crisis response and others use it to provide on-going support.

Understanding Chat-Based Services

For the purposes of this document, "online chat," is referring to browser-based platform where a participant connects to an anti-violence worker through a link on the program's website.

A person initiates the chat conversation by clicking on a link on the program's website. The conversation remains in the online chat box, and the participant does not have to worry about deleting messages out of an app or their text message folder. Online chats can be set up so that as soon as the conversation ends, the chat history is erased. A Canadian anti-violence program example of this is https://unsafeathomeottawa.ca/

Another option for chat-based services is to communicate with participants through third party browser-based platforms or apps that are connected to a phone number or social media account (for example: WhatsApp, Facebook Messenger). These platforms are often not as secure as the program's website chat-based services.

Understanding SMS Text Message-Based Services

If an agency is considering texting or messaging as the main method of providing services, the most secure type of messaging service are platforms meant for companies to engage with participants regularly via SMS text. While participants may use SMS text messaging or another messaging service to connect to your hotline or support services, it is best for your program to use a dedicated texting service platform, where the program on a computer rather than a cell phone receives the message.

Texting services that are tied to a program on a computer allows for programs to better manage staffing, hand off "messages" during a shift change, and allow for more than one staff member to respond to messages. Texting platforms can be customized to the needs of the agency, which may include sending standard disclaimer and other informative messages before or at the end of each text conversation. Platforms used for hotlines or message-based support services should include strong privacy and security protocols, in order to increase privacy for program participants and minimize

privacy breaches for the program. https://unsafeathomeottawa.ca/ also provides secure SMS text messaging options for women experiencing domestic violence in Ottawa.

It is important to understand the risks and benefits of both options. It is essential for programs to incorporate safety and privacy considerations into their support work to develop policies and protocols that make services easier to access while minimizing related risks. Chat and messaging tools come with their own unique set of safety and privacy considerations discussed below.

Minimize Interception

In the context of domestic violence, stalking, or harassment, there is always a chance that someone else is monitoring the device of a woman and her children. This could happen either by someone physically looking at the device (with or without her knowing), accessing information from her device that is saved to the cloud or because of spyware or malware installed on the device.

- Always check in with participants about their safety at the beginning of the conversation. Ask if they are concerned about their device being monitored. Let them know that chat can be a risky way to communicate if the device is being monitored. If they are worried, you can suggest options for safer communication (see below). If the participant suspects the device is being monitored but still wants to chat, respect that wish. Provide the safety information they need, but let them make the final decision about what is best for them in their current situation.

- If the participant does not want to continue the chat because they're concerned about interception, discuss other ways to safely communicate, such as using another device (for example, a library computer), making a phone or video call, or talking in person.

- Some chat services allow the program to set up the platform so that when the anti-violence worker ends the conversation, the chat window on the participants' device is automatically closed and the conversation history is erased. Inform participants what will happen when you end a chat conversation.

- Turn off options that allow chat messages to be saved or copied. Just as how hotline calls and in-person crisis interactions with participants are not typically recorded, chat conversations should follow the same privacy practices.

- Find out how the web address of the chat service will look in the participants' web browser and help them create strategies to eliminate or minimize risks related to the perpetrator seeing it.

Prevent Impersonation

Without being face-to-face or hearing the person you are communicating with, could allow someone to impersonate the participant. This can be a serious concern if the support worker has ongoing communications with the participant and will be discussing issues from previous conversations.

- Apply the same safety and privacy protocols to chat hotlines that you do on phone crisis hotlines when the caller could be a perpetrator or someone unknown. Address specific questions, but do not share personal information about anyone else, including other clients or staff.

- When using chat services for ongoing communication with a participant, establish a method that verifies their identity. Code words can be used at the beginning of each conversation to confirm the identity of the person chatting. Let them know that you may ask them for it again during the conversation just to make sure that you are still speaking to the same person. Update the code word regularly.

- Do not rely on user accounts as a method to confirm a person's identity. While it may seem that they are more secure because they require a username and password to sign on, they are not a guarantee that the person you are communicating with is the account holder. A perpetrator could access the account by guessing the username and password or discover them by monitoring the participants' device. Also, creating a user account may create a barrier to access services.

Ensure Data Privacy

Most chat platforms on the market were created for customer service or telehealth communication and not for providing anti-violence support services. By design, these platforms gather a lot of information. This can include incidental data, such as the participants' IP address, the type of device used, and general location. The platform may also store detailed personal information, such as how many times someone has reached out, the dates and times they reached out, and full transcripts of conversations. Some platforms can be set up to collect specific data as part of the chat communication.

For businesses, this information can help build customer satisfaction and increase profits. For anti-violence support organizations, capturing this information can create complex privacy and safety risks and potentially violate confidentiality best practices.

Participant's Data

- Collect the least amount of information necessary to provide the appropriate service for the time requested and keep that information for the period mandated by the applicable privacy laws. Do

not collect more information than you would for a traditional hotline/crisis call or in-person conversation.

- Choose a platform that does not store the content of conversations; if the platform allows saving or recording conversations, turn off that feature.

Collecting Demographic Data

- If your program chooses to ask demographic questions (or any questions) before a chat starts, the participant may think they are required to answer the questions if they want to get help. It is important to convey that these questions can be skipped and that you can opt out of asking these questions.

- If the participant chooses to answer the questions, next explain why you are collecting the information and how sharing information may affect their privacy and safety. Give them the opportunity to make meaningfully informed choices on whether they want to participate.

Incidental Data Collection

- Incidental data (IP address, device type, general location) may be collected by the chat platform automatically. Ask the chat platform vendor: do they collect such data, who has access to that data, if they share data and with whom, and how regularly they delete it. Most of this information will be in their privacy policy. If the platform allows it, opt out of collecting incidental data. Otherwise, ask to customize the system to delete the information as quickly as possible (ideally automatically). If their data access and sharing practices do not match your privacy and safety needs, find another platform.

- Some platforms may have the ability to integrate with your program's databases, automatically storing data about the contact. This practice is not recommended given the anonymity of the chat function and it is not recommended that you store or include chat data in any program database.

Data Security

- Choose a platform where employees of the company cannot see or retrieve content of chat conversations. This is sometimes called "zero-knowledge" or "no knowledge" encryption or "no view" services. In such a system, your program holds the key to unscramble the data and the company does not. No one at the company can see that content, accidentally or on purpose. In addition, if they were to receive a subpoena or court order, they would not be able to reveal any readable information because the data is encrypted in that way.

- If the platform company has the ability to see personally identifying information or content from participants, negotiate language in the contract that imposes strict consequences should the company access this private information. If a breach occurs, the company should notify you immediately.

- Support workers should minimize sharing personally identifying information of participants and others over the platform.

- Inform participants of the platform you are using so they can choose, based on their own safety planning, whether to communicate with you via the platform. Some may choose not to use a particular technology because they know or suspect that it is vulnerable to being accessible by a perpetrator.

Inform all participants of their Rights and Choices

Just like with hotline crisis phone calls and face-to-face meetings, your program should have a process that informs participants of their rights and choices. These include the right to:

- voluntarily access services,
- choose what they do or do not want to share with you,
- decide if and how their personal information is shared with third parties, and
- be aware any mandatory reporting obligations your program may have.

With chat services, your program will need to create processes and policies to pre-emptively inform participants of their rights. As an example, if an anti-violence support worker is a mandatory reporter and they are having an in-person conversation with a participant who is about to disclose something that may fall under MCFD reporting obligations, the worker can respectfully interrupt to remind them of those obligations. The participant can decide whether to continue disclosing. In a chat conversation, it is more challenging since the disclosure may come through the chat before the support worker can interrupt with information about their mandatory obligation. It is important to ensure that the notice of rights are given upfront.

Initiate conversations at the beginning of each hotline chat about the participants' rights and safety, any limitations to confidentiality, and any other issue commonly covered in voice calls. Some platforms can set up "canned" messages that automatically appear at the beginning of each chat session. If the software does not allow for canned messages, you can cut and paste the standard message from an electronic document. However, keep the language short, meaningful, and in plain language, with a link

to more details elsewhere. Give participants a chance to discuss these issues with you if they have any questions or want more information.

Ensure Appropriate Staffing

Chat conversations are often longer in duration than traditional phone calls, and participants tend to disclose more graphic information. In addition, chat conversations can end abruptly if the participant simply stops responding. Because of this, staffing chat conversations may require different skills, in addition to more support and staffing than traditional support services.

- Develop processes on how to respond if a participant stops communicating. Draw on existing practices for when a phone call is dropped.

- Prepare clear messages that support workers can share with participants to let them know that if a certain amount of time passes and the participant has not responded, the conversation will be closed.

- Since chat conversations often last longer than phone calls, consider how the staff will handle shift changes if the conversation continues beyond a staff member's working hours. You may transfer a chat conversation from one staff member to the next; however, be sure to include processes for informing the participant of the change so they know they are speaking with someone new. Or you may create a policy that participants do not start new conversations within the last 30 minutes of their shift.

- Because chat conversations tend to have more graphic disclosures than phone calls, ensure that staff have appropriate debriefing and supports.

Training for and Implementation of Chat Services

It is essential that anti-violence support workers using a chat platform receive training in the nuances of communicating non-verbally with participants. It is also important to ensure participants have a clear understanding of when chat is available (days of the week, times of day) and that they know what the alternatives are if the system is down.

- Clearly post on your website the hours that chat is available. If those hours change unexpectedly or if there are technical issues, ensure that is clearly communicated. Always include alternative ways to reach the program if a program participant is in a crisis.

- Train staff so they are comfortable communicating in writing with participants in crisis. Verbal cues that can be helpful in a phone call do not exist over chat, meaning staff need to check in more often to ensure they understand.

- Do not assume that you understand the meaning of the words someone writes or why they are using a particular writing style. Just because someone is using all capital letters does not mean they are shouting, and someone who is typing slowly with many pauses is not necessarily hesitant. Check in with the participant about meaning, tone, and emotion to help minimize miscommunication.

- Avoid using Internet slang, acronyms, and emojis. Not everyone has the same understanding of what they mean, and some may not be familiar with them at all.

- Do not use machine-based language translation. Currently, this type of translation is not high quality and is unable to translate domestic violence issues with nuance and sensitivity. Consider using chat platforms that allow for three-way conversations. Then, use a live, qualified language interpreter. Be sure to follow proper consent and disclosure guidelines when including third party interpreters.

- Find out how the platform will handle messages sent in characters and alphabets other than those often called “Basic Latin” (meaning English and other European languages). Make sure that all character sets and alphabets are supported, including those for languages such as Arabic, Mandarin, Hindi, etc. If the platform does not support other languages, have a plan on how to respond to participants, which may include providing notices on your website inviting them to call the hotline if interpretation is available there.

Plan Ahead

There will always be situations that affect your chat service that are not related to speaking with participants. This may include natural disasters or emergencies. It will also include contact from people who are not in need of anti-violence support, such as prank callers, abusive individuals, or callers with mental health crises including suicidal ideation.

- Identify unintended and unexpected scenarios that could impact your chat service and plan accordingly.

- For inappropriate callers, some chat platforms allow for conversations to be transferred to a supervisor. Draw on existing policies and procedures.

- Include chat services in your program's emergency and disaster planning, and ensure that participants know when your service is unavailable and alternative options to get help.

If your agency has any questions or needs guidance on how to implement Online Chat or Messaging programs and digital services, please contact BCSTH's Technology Safety Project at rhiannon@bcsth.ca

Adapted for Canada from and in cooperation with the Safety Net Technology Project at the National Network to End Domestic Violence, United States