Anti-Violence Program's Guide: Texting

Benefits of Communicating via Text with Program Participants

Text messaging can be an effective tool to keep program participants engaged, relay information quickly, and stay connected during times of social distancing. This is helpful when a program participant needs information quickly and cannot speak on the phone. Sometimes, texting may be more reliable than connecting through a phone call. Texting is best as a form of communication when used to supplement in-person meetings or phone calls. Texting only relationships between an anti-violence worker and program participants can be challenging because of safety and privacy concerns discussed below. During circumstances such as the current COVID-19 pandemic, an anti-violence worker and program participant may only be able to text; in which case, it is recommended that workers check in regularly with participants about privacy and safety considerations and explore safer texting options.

Safety & Privacy Issues When Texting with Program Participants

Documentation

Unlike a verbal conversation, texts contain a full history of the conversation. This means that if someone has access to a program participant's phone, they can read the entire thread of a conversation between the program participant and their worker. This can have major implications for security and privacy. On the employee's side, the phone also contains a history of the conversation, which could be accessible by colleagues or other third parties who have access to the employee's phone.

Impersonation

When texting, it is difficult to be sure that the person you are texting with is in fact the program participant and not someone pretending to be them. Mobile phones are mobile, small, and easily accessible by roommates, friends, family, and even the perpetrator. If the program participant's mobile phone does not have a passcode on it (or another person knows what the code is), the phone is accessible in order to view and respond to text messages.

Miscommunication

Texting lacks the nuance of in-person and over-the-phone communications. What might be conveyed by body language or tone of voice is missing in texts, and text messages might be perceived as short or insensitive, or simply unclear. The employee may not be able to perceive a program participant's

intended meaning accurately. In addition, the many acronyms and abbreviations used in text messaging may not have the same meaning or connotation to the recipient or sender.

Text Messaging Practices for Anti-Violence Workers

Use a Program Mobile Phone

It is better to use a dedicated work mobile phone owned by your organization when texting or calling program participants. The Program's Privacy Policies should govern the use of a work mobile phone. Significant privacy and confidentiality concerns arise when using a personal phone to communicate with program participants. These concerns are detailed below.

Limit program participant information in contacts

Save as little information as possible, and when the communication is over, delete the contact information from the phone.

Delete text history logs

When appropriate, consider periodically deleting conversations, so the phone does not store months (if not years) of text conversations between the program participants and employees on mobile phones.

Check in regularly about security and privacy

It is easy to become comfortable with texting and assume that the person you are texting with is a program participant. Check in with the person that you are supporting through other ways, such as a phone call, video chat, or if possible an in-person meeting.

Be aware of the potential for miscommunication

Like email, it is easy to miss or misread emotional cues in text communications. Check in regularly to make sure that you both are communicating in a productive and useful manner.

Set expectations and boundaries

Before texting, always have a conversation with the program participant about when you can text one another. Set boundaries and expectations, so a program participant knows your available work hours and when you can and cannot respond to a text message and what resources are available to her after hours.

Safety Planning Suggestions for texting with Program Participants

Recommend the deletion of text history logs

Talk to program participants about deleting sent and received messages, as well as the organization's number from their text log to ensure her safety and security.

Determine with her if it is safe to keep the support worker's name and phone number in her contacts

If a perpetrator is monitoring her phone (either because he has physical access to her phone or can monitor it remotely), it might not be safe for her to store the worker's name and phone number in her contacts. This conversation can be part of safety planning with the program participant.

Encourage program participants to check in regularly

Because texting may not be the best method for communicating about safety planning and risk factors, encourage her to check in using other methods via a phone call, video call, and in person meeting rather than only communicating via text.

Security and Privacy Risks Associated with Using Personal Phones for Texting

If an anti-violence worker uses their personal mobile phone to text with participants, resulting privacy and safety issues to consider are as follows:

- The program participant will know the worker's personal phone number. Unlike phone calls, when you text, you cannot make your number "private." This could become a safety issue if the perpetrator discovers the employee's personal phone number. It can also make it difficult for employees to set boundaries as to when they are available and not available for work.
- If workers are using their personal phones, third parties, family and friends may access their phones and see confidential text conversations between the worker and a program participant. This is a potential privacy and confidentiality breach.
- If workers store confidential text communications on their phone, the phone could be subpoenaed in court proceedings if litigants believed the phone contained information relevant to a court proceeding.
- When an employee leaves a program, the organization loses control over any information stored on the phone, since the phone belongs to the employee.

Third-Party Messaging Apps/Services

Because of the inherent lack of privacy with texting, some programs have considered using third-party texting apps. Some of these apps allow texts messages to disappear after a period of time and include more secure encryption. There are pros and cons to using these third party texting services.

The benefits are that some of the apps/services offer additional features, such as:

- Messages can be set to disappear after a period of time.
- Additional encryption, making the messages less vulnerable to "hacks."
- Access to the service from a tablet, computer, or another phone, which can be helpful if a program participant's phone has been compromised or if she gets a new phone.
- It can be another method of communication if the program participant believes the perpetrator is monitoring her texts.

The risks posed by these apps/services are as follows:

- Downloading a messaging app or service could be inconvenient to accomplish and unsafe for a program participant if a perpetrator is monitoring the apps and services they download.
- Most (if not all) of the third-party messaging app/services require the user to create an account. Depending on how they set up the account, it could inform a perpetrator that they have downloaded a new messaging service.
- Because the apps/services are accessible via different devices, this also means that if the perpetrator has access to the program participant's digital devices and passwords, he could be monitoring the text messages without having access to her phone. Be sure to go through the security and privacy settings on these apps to make sure no one else is accessing the account.
- Some third party apps/services require access to other content on the phone, such as contacts or photos. Anti-violence workers should check to see if the program participant is comfortable with sharing that access and opt out.
- Some messaging apps/services when connected to the program participant's contacts, inform people in her contact list who are also using the same messaging app/service that she has an account. The program participant may not want others to know that she is using the third-party messaging app/service. Learn what type of access, connections, and automatic sharing the app does and see if the participant can opt out of those connections and sharing.

Text Crisis/Help Lines

In some cases, organizations may want to include texting as a way for women, children and youth use to contact a 24/7 crisis/help line. Programs can do so in a safer way by using a web based SMS text platform. The Ottawa Coalition to End Violence against Women launched in April of 2020 https://unsafeathomeottawa.ca/ which allows women to safely text domestic violence support workers.

Investing in a crisis line via text through a SMS text web based platform is an important consideration because using text messaging for crisis/help lines raise the following privacy concerns.

Texting is not anonymous

Texting, by its nature, is difficult to make anonymous. The person texting cannot hide her phone number when she texts (unless she uses a virtual number, which although doable is uncommon), as a result the program managing the text crisis/help line will be collecting mobile phone numbers from the text messages. If the crisis/help line promises anonymity, the program will need to implement privacy policies as to how it collects, retains and deletes this information. Program billing records may also contain actual phone numbers associated with the text messages. Programs need to adopt privacy policies as to who can has access to those billing records and how they are maintained under records management guidelines.

Consider treating text messages the same way that the program manages phone conversations

The Program's privacy policies can consider not recording or keeping the phone number or text log of a crisis/help line text conversation. If the program's crisis/help line does not record and keep phone calls, text conversations can be managed the same way to maintain anonymity and privacy of the person who texted/called.

Assess for safety

Although a text crisis/help line may not be conducive to a thorough intake, organizations should still assess for safety and inform the program participant of support and safety planning resources. Regarding privacy of the text messaging, employees can advise the texting person of the program's privacy policies, the necessity to make mandatory reporting disclosures and tips on safe texting practices.

If your program has any questions or needs guidance on how to implement text messaging as a digital service, please reach out to BCSTH's Technology Safety Project at rhiannon@bcsth.ca