Working Remotely: Tips for Setting Up Phones

Whether advocates are being asked to work from home during a public health crisis or they are able to work from home as part of their regular schedule, being able to securely receive and send calls, text messages, and chats is critical. Below are answers and tips to commonly asked questions when setting up remote phone access.

How can we route our hotline to advocates working from home?

1. Contact your phone provider and ask about options.
2. If possible, switch to VoIP (Voice over Internet Protocol). TechSoup offers access to Tech Impact hosted VoIP.
3. If you receive text messages through your hotline number, the tool you use to manage those text messages may offer options to route voice calls to another phone line.
4. Consider forwarding your hotline to the National DV Hotline if/when you aren't able to take calls. Read more from the DV Hotline.
5. If possible, use an answering service.

NOTE: Plan to route calls in shifts and ensure that no one person is on-call for a 24-hour period.

How can advocates make outgoing calls to survivors when working from home?

1. Block the outgoing number.
2. Use a spoofing service that changes the number on the caller ID. Google "spoofing" to find companies.
3. Send a link to a survivor to meet up in a voice-only internet call, for example with Cyph or Gruveo.

4. Use VoIP, internet-based services that allow for voice calls. Set-up accounts for the program, such as Google Suite for Nonprofits. DO NOT make advocates set up personal accounts using their personal information.

What about text, chat, or video?

Below are additional resources for using text, chat, or video to communicate with survivors.

- Texting and Messaging with Survivors: Best Practices
- Chat with Survivors: Best Practices
- Communicating with Survivors Using Video: Best Practices

What can we do if agency phones are not immediately an option and advocates have to use personal cell phones, tablets, or laptops?

Confidentiality obligations require that no one outside of your program can see survivors' personally identifying information, and this includes avoiding inadvertent disclosures. To meet these obligations, focus on these tips:

1. Prioritize security.
    - Do not share your device with others in your household. If multiple user accounts or profiles can be set up on a device, create a new user account for the advocate's work use rather than using the existing personal user account/profile.
    - Use a strong password, PIN, or other way to lock the device.
    - Install anti-malware software and keep it updated.
    - Enable the ability to remotely wipe the device if lost or stolen.
2. Use program-owned accounts for email, text, chat, video, voice calls, file storage, etc.
3. As much as possible, use computers rather than phones for email, file access, and even text messaging, video, and voice calls.

4. Don’t save survivor names, phone numbers, emails, @handles, or any other information in contacts, in email or text messaging threads, in calendars, or anywhere else.
5. Quickly and regularly delete all email or text messages, and if possible remove any identifying survivor information from logs of calls, messages, videos, etc. on the devices AND in cloud-based accounts or billing information.
   Note: Be sure to train and/or give advocates access to the cloud storage in order to delete information.

Advocate well-being is a priority at any time, but needs to be amplified in the midst of a public health crisis or disaster. With technology, the focus is to support work-life balance with these tips:

1. Don’t give out personal numbers to preserve advocate privacy and to help support boundaries. See how to make outgoing calls, above.
2. Plan shifts to share incoming hotline calls, texts, chats, and other communication with survivors.
3. Use a mobile phone use agreement and IT support. Be clear with advocates about the information above through training and a written agreement. If possible, have IT staff or consultants help advocates to secure their devices and set up account access.

Read More: Using Mobile Phones to Communicate with Survivors: Best Practices

How can advocates working from home access electronic files remotely?

If advocates need to access files from outside of the office, secure access and transmission is important. Some cloud-based services offer “zero-knowledge” or “no-knowledge” encryption options in which no one, not even the tech company that runs the service, can see the content of the files because only your program holds the encryption key. Also, look for services that allow you to control

individual user access, so you can add or revoke access to users as needed. Both Tresorit and SpiderOak's CrossClave offer no-knowledge encryption.

For information on ensuring secure internet at home, please review the WiFi Safety & Privacy: Tips for Victim Service Agencies & Survivors.

Supported by US DOJ-OVW Grant # 2019-TA-AX-K003. 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 for the latest version of this and other materials.