

From: [DCF BWF Work Programs Help Desk](#)
To: [DCF DL DFES BWF W-2 Agency Directors](#); [DCF DL DFES BWF W-2 Agency CARES Coordinators](#); [DCF DL DFES BWF TJ TMJ](#)
Cc: [DCF DL DFES PTT W-2 Staff](#); [DCF DL DFES BWF W-2 REGIONAL STAFF](#); [DCF DL DFES BWF Supervisors](#)
Subject: COVID-19 Domestic Violence, Trauma, and Mental Health
Date: Thursday, April 23, 2020 7:05:28 AM
Attachments: [NNEDV_Email+Best+Practices_2018.pdf](#)
[NNEDV_Phone+Communication+Best+Practices_2019.pdf](#)
[NNEDV_Texting+Best+Practices_2019.pdf](#)

Hello.

W-2 agencies already support families in several ways, but additional supports may be needed during this time due to the increased likelihood of domestic violence in periods of crisis. As policy updates and clarifications continue to guide W-2 agencies during COVID-19, it is important to consider the impact of the pandemic on victims and survivors of domestic violence, and on individuals facing trauma or mental health problems. This e-mail recommends strategies to support individuals and families facing domestic violence, trauma, or mental health problems.

1. Background and General Information

-
Low-income families are undoubtedly experiencing incredible stresses related to COVID-19. Current data show that people in poverty often disproportionately feel the stresses of crisis. Unfortunately, increased stress is also a breeding ground for increased *frequency* and *intensity* of domestic violence, trauma, and mental health problems. This escalation can include all forms of domestic abuse, including, but not limited to physical, emotional, verbal, and financial abuse. Loss of health, employment, or other necessities can lead to increased trauma and re-traumatization for individuals and families. Research also shows that mental health is impacted in times of crisis, resulting in increased depression, anxiety, suicidal thoughts or actions, and other troubling responses to trauma and abuse.

2. Recommendations for Additional Support from W-2 Agencies

-
While W-2 agencies already have practices in place to support applicants and participants experiencing domestic violence, trauma, or mental health problems, the following recommendations offer additional considerations when working with families during crises. These recommendations are meant to supplement supports already provided in the W-2 manual and policy updates.

a. Communications

1. Domestic Violence

While W-2 agencies continue to communicate with applicants and participants on the

phone, via text, or in emails, victims of domestic violence may not be able to communicate at certain times during crises. For that reason, agency workers may modify phone communications to start like this:

“Hi, I’m _____ (your name) with _____ (your agency name). Are you able to talk privately with me now?” If yes, follow with: “If something changes and you need to hang up, you can call me back directly at this number _____.”

If no, consider asking the person if there would be a more appropriate time. If there is not an appropriate time, leave your phone number and email address, so the individual can choose to contact you when it is safe. You may also consider asking the individual if email, texting, or another platform would be more appropriate.

Mail communications may also be difficult for victims of domestic violence to access during the pandemic. Even if someone is part of the Safe at Home confidential mailing address program, the individual may be unable to retrieve or read mail privately during crises. Sometimes perpetrators are part of the W-2 group, but sometimes they are not. Victims may feel unsafe to communicate over the phone, or through email and mail during crises, especially if the perpetrator is unaware of the individual’s program application or participation. W-2 and other programs can be an avenue for victims to leave dangerous situations once employment and finances are secure. If domestic violence is indicated through assessment or other communications, the worker should consider keeping the case open even if there is less communication with the participant than usual.

Based on the conversation, if the worker chooses to provide additional domestic violence information to an applicant or participant, the worker should first determine the appropriate way to provide information that will keep the individual safe.

Attached to this document are three additional resources with best practices for electronic communication from the National Network to End Domestic Violence (NNEDV).

2. Trauma & Mental Health

Knowing that trauma and mental health problems may increase during crises, agency workers should consider adding questions to their communications. Here are some examples:

- “How are you feeling about your situation? What emotions are you experiencing?”
- “Who is supporting you during this time? How can I help you find more support?”

- “What strategies are you using to stay connected with other people?”

If the participant does not respond to open-ended questions, the worker should consider saying something like, “I am feeling very _____ (emotion) during this time. Do you feel this way? Tell me about your feelings.” While open-ended questions better allow individuals to express thoughts, a little prompting may be necessary.

Agency workers should also consider their responses when someone answers these questions. Research recommends not starting a response with, “I know how you feel.” This phrase can create additional separation and isolation, because everyone’s experiences are different. In addition, avoid phrases like, “That must make you feel (emotion).” This minimizes the individual’s feelings and can lead to decreased responses to questions.

Instead, the worker can respond with something like, “Thank you for sharing that with me. How can we work together to help make things better?”

b. Assessments

1. Domestic Violence

-

The WWP informal assessment driver flow provides questions about domestic violence situations. However, W-2 workers should ask additional questions during crises even if the individual did not disclose domestic violence during recent assessments. Workers may ask questions like:

- “Who is at home with you? How is that relationship?”
- “How do you think _____ (your husband, partner, child, etc.) is feeling right now? Why do you think so?”
- “Has anything changed regarding safety in your home since we last talked?”

Workers can use open-ended questions to elicit honest and real feedback from the applicant or participant. Workers should try not to pressure a response; instead, workers should provide an opportunity for the individual to speak freely.

2. Trauma & Mental Health

Similar to strategies used to discuss domestic violence, workers can add questions about emotions or actions in communications with applicants and participants. Even if the individual did not report substance abuse, addiction, traumatic experiences, or mental health problems during previous assessments, worker should engage the individuals in dialogue about experiences and feelings during the crisis.

Formal assessments as well as mental health supports and treatments may be limited during crises. Agencies should all previous policy guidance regarding assessments. Workers can use any delays in accessing formal assessments or supportive services to engage the individual in self-reflection, conversations about self-care, or other engaging activities.

c. Activity Assignments

1. Domestic Violence

Victims of domestic violence may not be able to complete W-2 activities during crises. A perpetrator may create barriers for a participant's involvement in the program as a form of abuse. Agencies should use W-2 policy discretion when considering good cause for activity assignments for individuals experiencing domestic violence.

2. Trauma & Mental Health

Workers should consider assigning activities that support trauma survivors or those with mental health problems. Such activities include:

- Motivate someone to connect with others or practice healthy, daily routines
- Engage interaction between parent and child
- Promote reflection and dreams for the future
- Encourage self-care and independent living

d. Other considerations

When using these recommendations, safety is most important. It is unlikely that a W-2 worker can "fix" a domestic violence, trauma, or mental health problem. The W-2 worker's job is to support.

For more information about domestic violence services, workers can contact End Domestic Abuse Wisconsin (www.endabusewi.org) and local domestic violence organizations to ensure the agency is providing accurate information on how to support survivors during the pandemic. Shelters are still open, and in cases where they are full, many cities are turning to hotels for space. For a list of all DV agencies in Wisconsin, go to:

<https://www.endabuse.wi.org/get-help/>

Agencies serving Dane County residents should note that although the Dane County Circuit Court records office may be temporarily closed to the public, restraining orders can be filed online.

Statewide legal resource organizations such as Legal Action (www.legalaction.org), Judicare

(www.judicare.org), and End Domestic Abuse Wisconsin can provide legal assistance, including helping with technology.

DCF is also expected to provide a list of domestic violence resources on its public-facing website. We will send an announcement through the W-2 Help Desk when this list is available.

This email and the attached documents will be posted to the BWF Work Programs Help Desk Home Page located here: <https://dcf.wisconsin.gov/w2/partners/toolbox/helpdesk> and can be found in the Common Requests section under **COVID-19 Information**.

If you have any questions, please contact Sara Conrad at sara.conrad@wisconsin.gov.

Thank you.

Sara Conrad

Program and Policy Analyst, Advanced

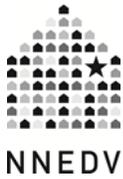
Department of Children and Families

201 East Washington Avenue

Madison, WI 53703

T: (269) 470-0996 (personal cell, only during work hours)

E: sara.conrad@wisconsin.gov



Best Practices When Using Email

Many victim service programs use email daily in their work, either communicating with survivors directly or coordinating services with other community programs. By its very nature, however, email is a risky way to communicate. Email can be forwarded accidentally or read by someone it wasn't intended for. The following are best practices for victim service agencies to ensure that their email communication is kept as private and secure as possible.

When Emailing with Survivors

- Don't ban emailing with survivors as a general practice. Although email has risks, refusing to email with survivors isn't the solution. Let the survivor determine the means of communication that can best accommodate their ability, access, needs, and preferences.
- If a survivor contacts you through email, your response should:
 - Delete their initial email and/or any previous thread. This way, if the email gets intercepted or accessed by the abuser, the request for assistance or the entire history of the conversation isn't revealed.
 - Include information about the risks related to email communication (example below) and discuss email safety and privacy with survivors, encouraging them to delete the messages they have sent and received, and to clear out their deleted folder.
 - Ask if there are safer ways that you can communicate. (For some survivors, it may be the only method available to get help, but for others a phone call or in person visit might be safer.)
 - If communication continues, check in periodically to see if email is still a safe and preferred method of communicating.
- Do not store victims' names and email addresses in address books.
- If you must print out an email exchange, shred the email conversation as soon as you no longer need it.

- Most email programs will autofill the rest of the address for you after you type the first few letters of the name. To prevent sending emails to the wrong person, make sure to double check the address before hitting send.
- Staff should regularly delete emails from survivors so as to not keep identifying, confidential information for longer than needed. This includes purging the “sent” and “deleted” folders as well.

When Emailing Coworkers About Survivors

- Internal communication about survivors should be restricted. Before emailing a coworker about a survivor, consider more privacy focused options, like telling the colleague in person or over the phone.
- Do not include a survivor’s name or other identifying information in emails, including initials.

When Emailing Outside Parties About Survivors

Before using email to communicate with outside parties (including using encrypted email), you should first determine if there are other options that are more survivor-centered, and that don’t create a digital trail. Opening the door to communicating confidential information over email is very risky. Before doing so, you’ll need to make sure that every staff person in your agency who will be using email to communicate confidential client information is fully trained on the VAWA, FVPSA, and VOCA confidentiality obligations, and that they understand the risks and nuances related to email communication. It can be very easy when caught up in the back and forth of an email conversation to forget or accidentally overlook the specific limitations a survivor has set regarding their permission for you to release their information. Advocates can easily share more than they’ve been permitted to by answering follow-up questions.

If you decide to move forward with using email, be sure to follow the best practices outlined below:

- You can only communicate about a survivor with another agency over email when the survivor wants you to do so, and you can only communicate the specific information they have given you permission to share. When doing this, you must have a written, informed, and time-limited release from the survivor before sharing any information. Refer to the [NNEDV Confidentiality Toolkit](#) for more information about releases and confidentiality obligations.
- Make sure that every survivor is fully informed about what sharing their information over email will look like and the related risks of doing so, so that they can make an informed decision about if they want their information shared that way or not.

Advocates will need to be prepared to talk about how your agency is working to ensure that the emails are secure, and any potential risks (for example - that you can't control what the other person does with the email once they have it; that they may send a reply to you in an unencrypted format; etc.).

Secure Email

There are many products on the market that claim to offer secure, encrypted email. Most email providers (even many of those marketed as encrypted) have access to the content of the emails sent and received by account holders. If they can access the content, then the communication may not be regarded as truly confidential. For more information about confidentiality requirements for victim services providers under federal law, please see our [Confidentiality Toolkit](#).

A stronger protection is known as “zero knowledge encryption,” which makes the data being sent back and forth unreadable to the software company that hosts the email. It is important to know that while this kind of security adequately protects victim data (as long as spyware is not on the device), it also complicates the process of sending and receiving email, so staff and any outside parties will need to be trained on how to use such software.

Agency Best Practices & Policies

Agencies should have a data retention policy ensuring that information that isn't needed is regularly deleted. (Visit NNEDV's Technology & Confidentiality Resources Toolkit for [best practices on record retention and deletion](#).) This policy should include emails received from and sent to survivors, and emails containing information about survivors. Don't forget that emails are often backed up or archived, and email conversations between you and survivors will be saved, so backups and archives containing survivor information will also need to be deleted.

When communicating with others about survivors, make sure you are following your organization's confidentiality obligations and requirements for privilege (if your state has advocate-client privilege). Email is a form of written record; guard it responsibly.

Sample Email Disclaimer Language

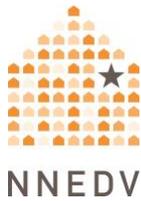
Since few people actually read the information in signature lines, being creative in your use of a disclaimer may help get the message across more effectively. The language below can be included at the beginning of every email with a survivor.

Communications between [agency name] and clients are protected by [state, if applicable] privilege and federal confidentiality law. [Agency name] does not reveal or share client communications without a client's written permission except where required to do so by mandated reporting. However, we want to make sure you are aware of the privacy risks related to email communication:

- Email is not a secure way to communicate.
- Emails can be easily seen by other people without your knowledge or consent. Because of that, please limit the personally identifying information you send in emails to only what is necessary.
- [Agency name] staff can talk to you more about ways to increase your privacy and safety online.

©2018 National Network to End Domestic Violence, Safety Net Project.
Supported by US DOJ-OVC Grant # 2016-TA-AX-K064. 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.



Phone Communication With Survivors

Best Practices

One of the more secure and easier methods of communicating with survivors is via phone calls. To ensure privacy and safety, follow these best practices when communicating with survivors via traditional phones. For information about other ways of communicating with survivors, including using text, chat, video calls, and email, please see our [Digital Services Toolkit](#).

Calling Survivors

Before calling a survivor, have a conversation with them about if and when it is safe for you to call. Some survivors may have abusers who are monitoring phone calls. Some survivors may have privacy concerns as well, if they have not disclosed abuse to friends, family, roommates, or coworkers. So, it's important to allow the survivor to determine the call back time and process.

Leaving Messages and Voicemails

Before leaving a message with someone other than the survivor, or a voicemail, talk to the survivor about their safety and privacy needs, and what kind of information (if any) to leave in your message. Work with the survivor to choose options that best suit their current situation, and remember to check in with them regularly to see if their needs have changed.

If you have not been able to discuss safety issues before leaving a message with the survivor, leave a vague message. You might decide to include your name, the reason you are calling, but not the name of your organization or even your phone number. Your message could be: "Hello, this is [your name]. I'm returning your call from this morning. [If it's vague enough, include about what.] You were asking for some information. You can call me back between the hours of 9-5, Monday through Friday."

Dropped Calls

Since many callers may be using cell phones, dropped calls may occur; or they may need to hang-up quickly for safety or privacy reasons. Ask the survivor ahead of time what protocol works best for them. Do they prefer that you call them back, or to have you wait for them to call you back? This is particularly important for hotline calls. Let the caller know what your program's practice is when a call is dropped; for example, you can't call them back, but they can call the hotline again at any time.

Programs' Caller ID

Most phone carriers will allow you to block your number from showing up on the caller ID of the person receiving your call. You can also do this manually for each call by dialing *67 before you dial the number. Some smartphones offer this option in the settings, where you can turn the caller ID on or off.

If your phone system is set up to block your number on the caller ID, check it regularly to make sure that it still works. Upgrades and changes by the phone carrier or your smartphone could unblock the caller ID.

Some survivors may have their phone set up to reject calls from blocked numbers, and some survivors may have installed apps that can reveal numbers that are blocked. This may be a safety strategy to protect against harassment. If the person you are calling is using that feature, let them know about your organization's policy, and the reasons you block your caller ID (potential safety and privacy risks for some survivors). Then strategize with them about the best way to reach out.

Some programs, particularly those that are under a larger social service agency, may have a different organization associated with their phone number. Instead of the caller ID showing up as "domestic violence shelter" or "rape crisis center," it will say "Salvation Army" or something else, which may be safer or more private. Another option is to use a caller ID spoofing service to replace your program's number with an alternate number in the survivor's caller ID.

Phone Systems & Safety

The type of phone systems your program uses will have an impact on privacy and safety as well. Your program may be using a traditional land-line phone system, a Voice over Internet Protocol (VoIP) phone system, and/or cell phones. One isn't more secure than the other, but depending on the phone system you are using, be aware of the privacy and safety risks that each system poses. Read more about [using cell phones to communicate with survivors](#).

Callers' Personally Identifying Information

Your program may be collecting identifying information about the people who call, even if you aren't doing so on purpose. Most phone systems now are designed to collect and store call history, caller ID, voicemail, transcribed messages, and more. How you collect, keep, and store survivors' personally identifying information can impact their safety and privacy, as well as your confidentiality obligations.

Some phone systems, particularly VoIP and mobile devices, offer the ability to translate voicemail messages into email or text messages. If your program wants to take advantage of this feature, keep in mind that you will also have to consider safety and privacy concerns for [email](#) and [text messaging](#). While it may be harder for someone to intercept or accidentally forward a voicemail message, it is much easier to intercept a text message on an advocate's personal cell phone or to forward an email that has a voicemail message attached.

If your phone system collects caller ID, voicemails, etc., you should have a policy detailing why that information is collected and how long that information is retained. It is best practice to keep the minimum amount of information necessary to meet the survivors needs (and your reporting requirements), and to only keep information for as long as you absolutely need it. Read our [FAQs on Record Retention and Deletion](#) for more information about handling personally identifying data.

Hotlines that promise anonymous calls are particularly obligated to ensure that

callers are truly anonymous, which means not keeping callers' phone numbers. A person's phone number can be identifying since a reverse phone number lookup online can reveal who owns that phone number and even where they live.

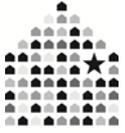
Many phone carriers offer their customers access to call logs and other information through online accounts or billing records. When determining data retention policies, don't forget to consider access to these accounts. You may want to limit who on staff can access these accounts. When receiving bills, you may want a policy in which your program immediately destroys the portions of the bill that contain personally identifying information.

Hotline management systems may also collect survivors' personally identifying information. These systems should be set up to delete information about calls as soon as possible, and should never keep copies of the content of conversations. Also, while some systems offer to integrate with client databases, routinely or automatically collecting this information is unnecessary and goes against best practices for confidentiality. The level of detail about when and how frequently a survivor contacts you is generally not needed in order to provide quality services.

For more information about communicating with survivors using technology, see our [Digital Services Toolkit](#), or [contact Safety Net](#).

© 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.



NNEDV

Texting & Messaging with Survivors: Best Practices

Many victim service programs are using text messaging and other messaging platforms to communicate with survivors. In addition to in-person meetings, voice or video calls, and [online chat](#), messaging is another option programs can use to connect with survivors. Messaging can increase access for some survivors, keeping survivors engaged, and can be used to relay information or send reminders of important dates, particularly when the survivor isn't able to talk on the phone. Messaging or texting can also be an option for offering digital services, such as a hotline or ongoing advocacy. Read more about [Best Practice Principles for Digital Services](#).

Communicating with Survivors Using Messaging

Texting as an Additional Form of Communication

When texting is used to as an additional form of communication, such as phone calls or face-to-face meetings, survivors and advocates usually use cell-based texting or messaging apps. The most common is to use the native texting service offered through the wireless phone carrier or messaging service specific to a type of smartphone, such as iMessages on iPhones. Some survivors and advocates may use apps such as Facebook Messenger, WhatsApp, Signal, Snapchat, or others. These third-party apps need to be downloaded by both users in order to be used, but may be preferable by some survivors, because they feel safer using those apps or (depending on the app) it is more secure.

It is important to meet survivors where they are and not require survivors to use a specific communication tool to contact your agency. Once an advocate has spoken with a survivor, assessed the survivor's unique safety risk, and discussed device and app safety, both the survivor and advocate can then decide on which messaging platform best meets the survivor's risks and concerns.

Texting/Messaging for Hotlines or Message-Based Advocacy Services

If an agency is considering texting or messaging as the main method of providing services, such as a hotline or texting/messaging-based advocacy, the best type of

messaging service are platforms meant for companies to engage with clients regularly via text. While survivors may use SMS text messaging or another messaging service to connect to your hotline, it is best for your agency to use a dedicated texting service platform, where the message is received by the program on a computer rather than a cell phone.

Texting services that are not tied to one cell phone allows for programs to better manage staffing, hand off “messages/calls” during a shift change, and allow 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 advocacy services should have strong privacy and security protocols, in order to increase privacy for survivors and minimize confidentiality violations for an agency. See our guide to [Choosing a Platform](#) for more information.

Minimize Interception

When texting, both the sender and receiver has the history of the entire conversation thread, date and time, and perhaps even location; this amount of information could pose major risk for a survivor’s safety and privacy. A survivor’s family members, friends, roommates, or others might see those messages if they have access to the device. Message history can also be revealed if the abusive person is monitoring the phone through physical access, monitoring software on the phone, or backups online.

Best practice:

- Talk to survivors about how to increase privacy if there is a concern that the phone might be monitored. Strategies may include deleting the message history and not saving contact details such as the program or advocate’s name in the phone.
- Remind the survivor about cloud accounts such as iCloud or Google that may backup the messages or make them available on other devices.

- If there are concerns that the device or account may be monitored, offer other options for more secure communications.

Prevent Impersonation

One concern when messaging with survivors is impersonation—someone else pretending to be the survivor. Someone other than the survivor could view or send messages either on the survivor’s device or on another device connected to the survivor’s account. This can be fairly easy to do, particularly if the survivor’s phone doesn’t have a passcode (or the abusive person knows the passcode).

Best practice:

- Establish a method to verify identity, which may include a previously agreed upon codeword or phrase.
- Check in regularly with the survivor to make sure messaging is still a safe method of communication.
- If either the advocate or survivor becomes uncomfortable with messaging, check in by other methods – over the phone or face-to-face.

Ensure Data Privacy

Because texting can store a significant amount of information, it is essential that programs’ policies include keeping minimal information on the devices used to text. It is not recommended that advocates use personal cell phones to text with survivors. A personal cell phone can easily be accessed by the advocate’s family or friends. If someone other than the advocate saw a copy of the messaging history, this would not only invade the survivor’s privacy, it could potentially violate confidentiality.

Another reason programs should not keep copies of messages is that if they have it, they may be required to release it. How your program responds to legal requests will depend on your confidentiality obligations per federal and state laws. The less information you keep, the less information you will have to release if compelled.

Best practice:

- Advocates should not use their personal phones to message with survivors. Use program-provided cell phones.
- Advocates should save as little information as possible on the phone, which includes not saving survivors' full name, phone number, or other contact information. (Since contact details are not saved, double check the phone number, especially if there is an "autofill" option, to prevent sending the message to the wrong person.) When the client-advocate relationship is over, delete all contact information from the phone.
- Messages should be deleted regularly from the phone. Just as your program would not record hotline calls or ongoing phone calls with survivors, similarly the history of a message conversation should not be saved.
- Review billing records and backups for any personally identifying information and delete those records. (Visit our Agency Use of Technology Toolkit for more information about [record retention and deletion](#).) Also, be aware of what information your phone company or messaging service will release about your account in response to legal requests.
- Do not offer to store or keep evidence for survivors. Discourage the sharing of pictures of abuse or forwarding abusive messages since advocates should not become part of the chain of custody for evidence. For more information about messaging evidence, see our [Legal Systems Toolkit](#).
- Some computer-based text messaging platforms (for text hotlines or message-based advocacy services) may offer to integrate detailed message conversations into your client database. Keeping this level of detail is not recommended.

Data Security for Hotlines or Messaging-Based Advocacy

When using a messaging platform to offer a text hotline or a messaging-based advocacy service, it is critical that the messaging platform chosen uses a type of encryption that doesn't allow anyone, not even the platform vendor to see the data. This type of encryption is sometimes known as "zero-knowledge" or "no

knowledge” or “no view” encryption. With this type of encryption, your program holds the key to unscrambling the encrypted data and the company does not, which means that no one at the company can see any content shared between advocate and survivor 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.

Other types of messaging service or apps do not have this level of encryption. Text messaging services via a wireless phone carrier are generally not encrypted; iMessages or Android messaging is end-to-end encrypted but the messages can be accessible via the iCloud or Google account; and security protocols on third-party messaging apps vary widely. For example, WhatsApp and Signal have end-to-end encryption, making them more secure, but it doesn’t necessarily guarantee complete security and privacy. Moreover, asking survivors to download a separate messaging app and create an account to connect with a program may be an additional barrier.

Best practice:

- When offering texting hotline or message-based advocacy services, look for platforms that offer a level of encryption in which no one, not even the platform vendor, can view the data.
- If the company providing the texting platform doesn’t offer “zero knowledge,” “no knowledge” or “no view” encryption, ensure that your own lawyers negotiate contract language that includes strict penalties should breaches of your data occur. In addition, contract language should include that any breach of data should be disclosed to you immediately.
- Advocates should minimize sharing personally identifying information of survivors and others over the platform.
- It is best not to require survivors to download a specific app or service in order to access help. Provide alternatives for survivors to reach out for help.

Inform Survivors of their Rights and Choices

Most programs have a process to inform survivors of their rights and options when accessing services. For example, programs might need to inform survivors of certain obligations, including mandatory reporting. Unlike a verbal conversation, where the advocate can interrupt a disclosure to let the survivor know that it may trigger a mandatory disclosure, in a messaging conversation, the advocate may receive the disclosure while messaging and not be able to interrupt and inform the survivor of their options.

If offering a text hotline, programs will need to determine how to inform survivors of their rights and choices during the conversation. Programs will need to also consider how to find balance between sharing necessary information and not overwhelming a survivor with too much information at initial contact.

Best practice:

- At the start of a messaging conversation, be prepared to initiate conversations with each survivor about messaging limitations, device safety, mandatory reporting requirements, and other issues commonly covered in voice calls.
- Prepare short and clear messages about these topics, but incorporate them into the conversation in a way that invites discussion or questions.

Set Survivor Expectations and Appropriate Staff Boundaries

The nature of messaging means that survivors may think they can send a message at any time, including after hours. In an ongoing relationship, the survivor and advocate may be messaging regularly. Make sure the survivor is aware of when the advocate can be reachable and have clear expectations of when they will receive a response.

Best practice:

- Set boundaries about work hours and availability with advocates and survivors when using messaging. Sometimes an advocate might be able to respond quicker by message, but at other times, a phone call might best if the issue is urgent. Communicate this to survivors so they know how and when they'll get a response.

Provide Appropriate Support for Staff on Text Hotlines

Staff working text hotlines might require more support and debriefing. Text hotlines tend to have more numerous and graphic disclosures of abuse. Moreover, in a text conversation, the survivor may just choose not to continue a conversation and stop communicating. This lack of closure could be difficult for some advocates, particularly if it was a heavy conversation. In some cases, text conversations may be longer in length than a phone hotline call, but with long breaks in between.

Best practice:

- Plan for adequate support for advocates working a text hotline.
- Plan for adequate staffing, and consider the fact that text conversations might be longer than a phone conversation and could require more than one advocate to continue the conversation.
- If long pauses in text conversations means that it's more efficient for an advocate to be on multiple text conversations at one time, ensure that advocates don't try to take on too many conversations at once.

Provide Quality Messaging Services

Because messages are mostly written words, it can be easily misunderstood. It can also be more difficult for the advocate or survivor to assess for emotion and tone, leading to potential misunderstanding. In addition, the nature of messaging means that users can have two or more topics of discussion overlap, as one person responds to a previous message and the other moves on to another question or statement. Furthermore, slang or shortened words like "LOL" may not have the same meaning or connotation to the recipient.

Best practice:

- Check in regularly to make sure that both survivor and advocate understand one another.
- Using slang or shortened words are ok, but advocates should take the lead from survivors.
- Stop and clarify points or statements if there is any confusion.

Plan Ahead

There will always be situations that impact digital services unrelated to speaking with survivors. This may include unexpected situations like natural disasters or emergencies. It will also include people who contact your service who aren't survivors, such as prank callers, abusive individuals, or callers with mental health crises including suicidal ideation unrelated to domestic violence or sexual assault issues.

Best practice:

- Identify unintended and unexpected scenarios that could impact your messaging service and plan accordingly.
- For inappropriate callers, some messaging platforms allow for conversations to be transferred to a supervisor. Draw on existing policies and procedures for inappropriate callers.
- Include messaging services in your program's emergency and disaster planning, and ensure that survivors attempting to reach out know when the service is unavailable and are offered alternative options.

© 2019 National Network to End Domestic Violence, Safety Net Project. This product was supported by cooperative agreement number 2017-VF-GX-K030, awarded by the Office for Victims of Crime, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this product are those of the contributors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

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