WCSAP
Washington Coalition of Sexual Assault Programs

THE ADVOCACY STATION

Principles for Integrating Technology into Services for Survivors

The increasingly pervasive use of technology in our everyday lives can feel disorienting, especially given the rapid pace of innovation and the expanding power of 21st century technology to collect, store, and distribute information about all of us.

The demand on programs to upgrade systems and to provide additional forms of communication is driven not only by this cultural shift, but by the increasing need to reach younger people. Youth embrace new technology faster than we can consider the precautions and then move on to the next. But hiding from technology just isn't an option; nor is jumping in feet first without research. As such, victim service providers need to thoughtfully integrate digital and web-based technology into our work with survivors.

The following guidance, while created with youth-focused programming in mind, can be useful for technology of any kind and for any age. We can adapt to new challenges, technologies, and systems when we stay grounded in the same advocacy philosophy and principles of best practice that have sustained anti-violence work since its inception as a grassroots movement.

1. **Stay Survivor-Centered.** Meet survivors where they are at and work with them to figure out the most supportive, empowering, and safe way to meet them there.

2. **Promote understanding.** Explain misinformation, and foster informed choice.

3. Design response systems with **privacy, choice, and safety** in mind from the very beginning.

4. **Seek answers** from institutions and partners. Collaborate with them to improve their response to survivors.

5. **Empower advocates and organizations** to provide the best possible services to survivors.

6. **Safety plan with survivors** while honoring their decisions about how to manage risks and define safety.

7. **Take steps to secure systems** against imposter or assailant manipulation.

8. **Disclose the minimum amount** necessary to accomplish a survivor's goals or comply with government requirements.

9. Strive to be a **privacy-centered** program.

10. **Be proactive.** Stay informed about changes or new risks that could change a survivor's situation.

This resource will provide helpful process steps and questions to answer when integrating technology so that you can do so in alignment with each of these principles. Because technology changes so quickly, the best resources for how to use or understand a particular technology are themselves online, regularly updated resources. A web search and review of timely reporting from trusted sources goes a long way.

For understanding technology specifically as it intersects with the needs of violence survivors, the best resource (as of this publication) is NNEDV Safety Net's techsafety.org blog, and specifically the two toolkits on the blog's resources page:

- Agency Use of Technology Best Practices & Policies Toolkit
  https://www.techsafety.org/agency-use

- Technology Safety & Privacy: A Toolkit for Survivors
  https://www.techsafety.org/resources-survivors

1. **Stay Survivor-Centered.** Meet survivors where they are at and work with them to figure out the most supportive, empowering, and safe way to meet them there.

If survivors are asking to connect using technology, then it is up to programs to look for ways to support survivors. Support may mean starting with an individual survivor on the technology and offering an opportunity to move to a safer method of communication.

EXAMPLE SCENARIO: Typical email is not secure. Companies that provide free email generally reserve the right to read or share the content of the emails. Email is typically unencrypted (unlocked) and can be stolen off the web relatively easily. And email routinely gets stored on machines and servers for a very long time.

If a survivor reaches out to you by email and discloses sensitive, private information, you can respond with an email that:

- Does NOT have survivor's original email attached
- Expresses empathy without repeating the details
- Offers resources and scheduling as appropriate
- Identifies your concern with email's lack of security
- Recognizes the upsides and convenience of email that might matter to the survivor
- Offers alternative methods for connecting including more protective electronic communication methods that your organization knows how to use and that gives the survivor the upsides and convenience of email
- When planning to work with a survivor over the long-term, find out from them what technology they have access to and are comfortable using.

EXAMPLE SCENARIO: A survivor may prefer to call you rather than coming back into the office.

Most advocates can comfortably discuss when and to what number it is safe to call and then plan what to do if an unexpected voice answers the phone. Advocates will discuss with survivors how calls might be stored or monitored, such as through phone records which might be accessible to parents or partners on-line and whether that poses a risk for this survivor.

- ✓ Apply the same problem-solving skills to other technology that survivors are comfortable with.
    - If a technology is unfamiliar to you, do research to find out what its security features and vulnerabilities are.
    - Tip sheets on specific technologies can be found in Safety Net's toolkit at www.techsafety.org/resources-agencyuse

Survivors are ultimately in control of their own communication with you, and will always be choosing which risks and burdens are okay or are too much. Support them in making those choices, then help them exercise that choice in the most protective manner available.

EXAMPLE SCENARIO: It is obviously more private to talk to an advocate inside a sexual assault program office rather than outside of a courtroom. And, survivors routinely choose to have conversations with an advocate in the hallway. Advocates having those conversations pay attention to finding a quiet corner, keeping their voice down, and watching out for eavesdroppers. If the survivor is having difficulties and the hallway no longer feels appropriate, the advocate looks for an empty office or room to take advantage of temporarily.

- ✓ Apply the same problem-solving skills to any technology that survivors might consider using.

2. **Promote understanding.** Explain misinformation, and foster informed choice.

Technology has become so accessible that people may use it without having much understanding of how it works, what the terms of service mean, or how information is protected or exposed. Help survivors be more informed about how they can use technology wisely.

EXAMPLE SCENARIO: Most people understand that documents and information used to live on the computer on their desk. You had to be at your computer and have it working to have access to your information.

Today, people know that information lives "in the cloud" but they don't always know what that means. If you are communicating with survivors using any cloud technology, then make sure that you and the survivor understand that the information in your communications lives on computers that are located in other places, owned and operated by other people, who have different rules and priorities than you do.

You don't need to understand how the cloud allows you to call up the information on your phone to make a decision that you don't want to put certain information in the hands of someone else.

Survivors may have easy access to security tools without realizing it, thus the tools are not turned on (or an invasive feature is not turned off.) There is a saying in the tech world: "If you are not paying for the product, you *are* the product." Put another way, find out how this company is making money because that will drive their approach to protecting and sharing information

- ✓ If they are not charging you to use the app, then they are either:
  - offering you a simple version hoping you will buy the premium version,
  - making money from advertising to you while you use the app,
  - making money by selling the information you put into the app, or
  - paying for the product through grant or government funding with no expectation of earning money.

- ✓ Avoid making assumptions that a survivor does or does not understand the pros and cons of a particular technology.

- ✓ Survivors may reflexively use the technology that they have already adopted for everyday communications without considering the downsides of seeking sexual assault services via this platform.

- ✓ Be prepared to suggest alternatives to popular, unsecure technologies.

EXAMPLE SCENARIO: Dropbox is a free technology and a very well-known platform for storing and sharing documents with other people. However, documents saved on Dropbox are not automatically encrypted, Dropbox could turn over documents to lawyers, and Dropbox has had security breakdowns which made documents and user information available on the web.

- There are other document hosting companies (such as Sync.com and SpiderOak) that use encryption which automatically prevents anyone at the company from being able to unlock and read the documents stored on those servers. The services may be free for smaller amounts of storage space or carry a small fee that could be very worthwhile for the privacy.

- There are companies that offer add-ons to Dropbox which encrypt files for greater security and protection.

- Even if one particular product feels unsafe, there may be a competitive product that gives the same convenience with more safety.

    - ✓ Identify what you or a survivor like about a technology so you can search for a more secure one with the same benefits.

- Get behind the hype to foster informed choice. Often the most used, more well-known technologies are just the ones with the biggest advertising budgets.

    - ✓ Don't assume it's the best just because "everyone" uses it.

    - ✓ Even if it is the best for everyday use, it may not be the best for people dealing with the aftermath of a sexual assault.

- Develop a better understanding of encryption and what different types of encryption are. At its simplest, encryption means information is locked, but someone always has the key. When a company states that their information is encrypted, ask who holds the key. The most private options are end-to-end encryption and zero knowledge encryption, which mean that your agency holds the key to unlock the information.

    - ✓ You can get more information about encryption and some well-known products in the victim services world by checking out EmpowerDB's Encryption Checklist at: https://www.empowerdb.com/EncryptionChecklist.pdf

3. Design response systems with **privacy, choice, and safety** in mind from the very beginning.

Where you do use technology to communicate with or about survivors, always provide it as an alternative, rather than the only way to communicate. This way survivors can make choices based on their own risk. When considering using a piece of technology, first clearly define the problem you are trying to solve by using it.

- ✓ Then ask "Does the technology solve the problem?"
- ✓ And "Does the technology create more problems than it solves?"
- ✓ If it does solve the problem, ask, "Is it the best way to solve the problem?" Is there an easier, less expensive solution available?

EXAMPLE SCENARIO: There is malicious software that can turn on a webcam without the device owner even knowing it. If someone offered you an app to prevent that software, it wouldn't be the best way to avoid unwanted filming. The best way to combat unwanted use of your webcam isn't a piece of software; it is a reusable sticker or post-it note placed over the camera when it's not in use.

Consider the risks involved in using the technology, especially if the system is so complicated that you must contract with a third party outside of your agency to manage it. When you use databases managed by outside vendors or system administrators, you create problems with those outsiders getting access to confidential information (unless it is zero knowledge encrypted.)

- ✓ Assess whether use of the technology would put the organization in violation of local law or federal grant requirements.
- ✓ VAWA, FVPSA and VOCA all require that grantees shall not disclose personally identifying information about victims outside of the victim service provider unit.
- ✓ VAWA regulations also require that grantees take reasonable measures to prevent inadvertent release of personally identifying information.
- ✓ If a technology provider assures you that their system is HIPAA compliant that does not mean that it meets the much stricter privacy standards of VAWA, FVPSA and VOCA grants. Unlike HIPAA, there is no part of VAWA, FVPSA or VOCA that gives organizations permission to share survivor information with "business associates."

Once you decide to use a technology, research the most privacy-conscious, least risky way to use it.

EXAMPLE SCENARIO: If staff wants to use email to share information about a survivor and determines that it really is the best solution to a communication problem, then the staff should avoid putting personally identifying information into those emails, and should limit the description to the minimum amount necessary to accomplish the purpose.

- ✓ Assign someone on staff to manage the security of the organization's machines, including laptops, tablets and smartphones. That person should:
    - Ensure installation of all recommended updates and security patches on a timely basis.
    - Track who among staff or volunteers has possession of machines in order to do agency work.
    - Take responsibility for retrieving machines from staff or volunteers who leave the agency.

Have a very clear policy about whether it is acceptable to use personal devices and home computers to access information about survivors or communicate with survivors. In the era of text, chat apps and cloud-based databases, it is likely that a staff member or volunteer will use a personal device to do work for survivors at least occasionally. Decide whether staff is routinely allowed to use personal machines or only in exceptional circumstances.

- ✓ If they are routinely allowed to do so, have a clear policy about the protective measures that must be taken if they choose to use a personal machine to do agency work.

- ✓ If it is only allowed in exceptional circumstances, have a clear policy about contacting someone in the agency to ensure survivor information is protected from accidental disclosure through the private machine.

- ✓ See "Best Practices for Mobile Computing Devices" in the Agency Use of Technology Toolkit for tips on organizational policy. https://www.techsafety.org/resources-agencyuse/mobilecomputing-bestpractices

Encrypt and passcode your agency laptops, tablets and devices so that the information on them cannot be accessed if the machines are lost or stolen.
Ensure you have, and your policy allows you to use, the ability to remotely wipe client and agency information off devices if they are lost or stolen.

4. **Seek answers** from institutions and partners. Collaborate with them to improve their response to survivors.

Be aware of the difference between consumer technology culture (faster, cheaper, and more convenient are most important values) vs. survivor-centered services culture (safer, more private, and modifiable to individual needs are important values.) Get information from the company providing the technology:

- ✓ Read the Terms of Service and Privacy Policies
- ✓ Ask for clarification if you don't understand what something means.
- ✓ Find out how the company handles legal demands for survivor information, specifically:
    - Do they notify the user that information has been demanded before turning it over?
    - Do they require a court order before turning over information?
    - Do they investigate whether they are actually legally required to turn over the information?
    - Get information from the website when you can.

EXAMPLE SCENARIO: If a survivor wants to communicate with you by text, will those texts be accessible to or saved by the cellular provider? If yes, then for how long? The answer differs depending on the cellular provider; find out the answer for major cellular providers.

- ✓ Ask the representatives questions about how information is stored, protected, and shared.
    - Beware of assumptions that even when you delete information, you want it "archived."
    - Find out how they back-up and when they destroy back-ups.
    - Ask what happens if data is disclosed accidentally or stolen?

"We carry a $1 million insurance policy" is not a method for protecting information. For most for-profit companies, data breaches are a cost of doing business. They assume they will get breached at some point and if there are damages, they will use insurance to pay off people harmed. For non-profit sexual assault providers, harm to survivors is irreparable and can't be fixed with money. Watch out for limitations in the contract that say damages are limited to the amount paid for the product, or the amount paid in one year's time.

- ✓ Find out how the company handles deleted information, and how they purge information.

A surprising number of tech companies assume that you would never want information to become inaccessible, and will back it up even when you tell the system to delete it.

- ✓ If it's a database you are looking at, find out how the company stores information, how they encrypt it, who has access to it, and how they share it.

- ✓ You can find detailed information on assessing databases, including detailed information about specific vendors, at techsafety.org by putting "database" in the search bar.

- ✓ Get information about a technology from someone other than the company selling it.

Technology is big business, and data mining individual information is even bigger business. Before using or suggesting survivors use a product:

- Look for reviews on-line from independent technology-focused news outlets
- Check out the App Safety Center at techsafety.org
- Ask for TA from the experts on survivors and technology at NNEDV's Safety Net, safetynet@nnedv.org
- Check whether the company has been the victim of a data breach by searching at https://www.privacyrights.org/data-breaches

If allies or funders are asking you to use a technology, ask the same hard questions you would ask of the company trying to sell it to you. You can't assume that the people asking you to use the technology have vetted it in the same way that you would.

- ✓ Ask allies and funders what access they or their staff would have to private information you put into this technology. If a funder or ally is insisting that you use a certain technology, ask:

    - What is the problem we are trying to solve by using this technology?
    - How did you take survivor's privacy and safety needs into account when you chose this particular technology?
    - Are there alternative technologies that would solve the problem identified with less risk to survivors?
    - Are there nuanced ways for us to use the technology so that we meet funder/ally demands without compromising survivor privacy and safety?

- ✓ Demand better, more private technology and apps.
    - Some companies will give you more privacy protective features only if you ask for them.
    - Take advantage of existing guides to privacy features within an app or platform, and ask for improvements.
    - For many popular apps, you can find guides on-line aimed at parents protecting their children's privacy.
    - Let vendors, funders and allies know when you refuse to use technology because it isn't private or secure enough.

Without consumer demand for privacy features, there will be no supply. Include the cost of privacy features and security (both in terms of dollars and staff time) in your plan for implementing technology.

5. **Empower advocates and organizations** to provide the best possible services to survivors.

- ✓ Make it a job duty of at least one staff member to stay abreast of technology that is available for communicating with or storing information about survivors.
    - Give that person appropriate space and time to do the research and provide support and training to other staff on technology.
    - Have that person give alerts to the rest of the team when very commonly used technology (like the iPhone) has an update.
    - That person should pay attention to news about and reviews of any apps aimed at sexual assault or domestic violence survivors.
- ✓ Utilize WCSAP Technical Assistance to work through scenarios in which technology intersects with survivors and your program.
- ✓ Take advantage of training offered by national TA providers, such as webinars and conferences by Safety Net, the OVW-funded TA provider on issues of technology, confidentiality, and the needs of survivors.
- ✓ Make regular use of the tips and recommendations in Safety Net's:
    - Agency Use of Technology Best Practices & Policies Toolkit https://www.techsafety.org/agency-use
    - Technology Safety & Privacy: A Toolkit for Survivors https://www.techsafety.org/resources-survivors
- ✓ Provide regular training and information for the entire team of staff and volunteers on how to use, assess, and understand technology resources.
- ✓ If you launch a new program, platform, or database, plan to devote the necessary financial resources and staff time to teach people how to use it and support them to use it well.
    - Include tech privacy education in your required basic training curriculum that staff and volunteers must complete before working with survivors.
- ✓ Create an internal culture where staff follow the privacy tips suggested for survivors, which can be found throughout Safety Net's Technology Safety & Privacy: A Toolkit for Survivors.
- ✓ Have an annual or semi-annual "Technology Privacy Check-up Day" where the whole team commits a half-day to checking their own work machines (and

personal devices) and habits in using those machines, including deletion of information that does not need to be stored.

- ✓ Have a very clear plan and policy around use of personal devices for any communication with or about survivors.

  Though it would be ideal if all communication with or about survivors is done only through agency-owned machines, the widespread use of internet-connected devices and web-based resources means that people will almost certainly, at least once, take a call, check an email, send a text, or open your client database on a personal machine. The policy should cover:
  - Security protections that must be on personal machines
  - Protection of personal login and password information
  - Plan for machines with survivor information that are lost, stolen or in possession of former staff/volunteers.

6. **Safety plan with survivors** while honoring their decisions about how to manage risks and define safety.

If a survivor is going to use technology, and especially use technology to communicate with you, review basic tech privacy and safety planning techniques with them. Help them access (and if asked, help them implement) tech privacy and safety planning tips at www.techsafety.org/resources-survivors

At the very least, discuss:

- Pass coding devices and machines
- Having awareness of who (e.g. partners, parents, employers) can access and read information stored in devices or on email accounts, and
- Erasing text logs, email chains, and call records they want kept private – from inbox, sent box, deleted and trash.
- Share with survivors that have smart phones the Tech Safety App from NNEDV (more information at https://www.techsafetyapp.org) so they can decide whether it might be helpful to them.

✓ Let survivors know about these reasons for updating their software and operating systems.

We all get the notices that there is an update available for our phone or for a program. A large number of those updates contain security fixes because the company (or hackers) discovered a way to break in. Ignoring those updates is like having the lock broken on your front door and ignoring it because it's annoying to get a new key.

✓ If a safety or evidence-collection app is being considered by a survivor, suggest they check out the privacy policies, reviews, and news reporting about that app. Many third-party apps aimed at survivors are reviewed at Safety Net's App Safety Center https://www.techsafety.org/appsafetycenter

EXAMPLE SCENARIO: There are several apps designed to give sexual assault victims a method for recording and storing statements and photos right after the assault. Some of them give the survivor control over what happens next to the information; some of them send the information directly to law enforcement and survivors have no further control.

It is important to be aware and to help survivors make an informed choice between the different apps if they have decided using one is a good idea.

7. **Take steps to secure systems** against imposter or assailant manipulation.

"Social Engineering" or "Phishing" (tricking people into voluntarily turning over password, login ID, and personally identifying information) is the most common way of using technology to obtain information or steal identity. Stay alert and trust your instincts!

- ✓ Don't share sensitive information or documents unless you've taken steps to confirm who you are communicating with and obtain written consent where required.

- ✓ Pay attention to changes in tone or style of communication.
    - It could mean a survivor is in crisis, not in control of communication being sent, or is having identity stolen.
    - Remember, you can always suggest confirming identity and wishes via voice call or video call.
    - Be willing to pause and assess when something seems off.
    - Decide how you are going to confirm that it is really the real person communicating with you if you can't see or hear the person.
    - For on-going communication, you could establish a code word to confirm identity.
    - Be aware that imposters might hijack your attempts to confirm identity.

EXAMPLE SCENARIO: You receive an email from a trusted colleague asking you to click a link and enter password information into what appears to be a Google Docs website.

You reply to the email and say, "This seems unusual. I just want to make sure it is really you." You get a response, "Yes, its me. Please follow the link."

You later discover that the organization's email was hacked. Both the original email and the reply were sent by identity thieves in control of the person's email address.

- ✓ If you think a technology is compromised, move to a different technology or method for confirming identity.
- ✓ Set up boundaries in the working relationship about how a survivor will and won't use technology to communicate or make requests of you.
- ✓ Let survivors know of the risk of impersonation so they are aware of the benefits of letting you know when an account or device is compromised.
    - A survivor could arrange a code word or even just a letter that tells you the account or device is no longer safe and you should stop using it to communicate.

8. **Disclose the minimum amount necessary** to accomplish a survivor's goals or comply with government requirements.

Anytime you write out information (whether in an email, a text, a chat app), that information could be copied or distributed beyond you and the intended recipient. As soon as information is written down and shared with even one person, you then need a strategy to control and destroy your copies as soon as appropriate. If you use the internet to share written information, remember that Vint Cerf, one of the inventors of the internet described it as a "giant copy machine."

- ✓ Even when a survivor has given informed consent for you to use technology to communicate, don't disclose more than you need to for the immediate purpose.

- ✓ Don't attach prior email text to the reply that you send unless there is a conscious and clear reason why that is what the survivor wants.
    - Pay close attention to what email address and/or text number you are using so you don't inadvertently disclose to unintended recipients.

EXAMPLE SCENARIO: You want to give the survivor the email address for the investigating detective so you type the detective's name into the address bar and it shows you the email address. You then type that address into the body of your email and hit send. But you didn't pay attention to the fact that the email for the detective was automatically entered into the recipient line, and you've sent the private survivor communication to the police.

Be aware that survivors might forward your communications to other people that they trust. While it is their decision whether to take that risk, you can minimize the risk by limiting your comments to the minimum amount necessary to achieve the immediate goal.

- ✓ Have a routine destruction policy for electronically stored information just as you would for paper documents.
    - Then ensure that you follow the schedule for routine destruction.
    - Do not store information (electronically or on paper) that you are not using to serve survivors, that you have no legal requirement to keep, and that poses only risk to survivors if disclosed.
    - If you are concerned a survivor might come back one day and want the thing you routinely destroyed, then talk to survivors when you are serving them about your policies and about strategies for them to get and store information for themselves.

9. Strive to be a privacy-centered program.

- ✓ Thoroughly assess the impact on survivors and their privacy of technology solutions that are designed to meet the goals of funders and/or government.

- ✓ Releases of information (ROI) can never be made a condition of services (neither explicit nor implied.)

  The Violence Against Women Act states that a release of information cannot be required in order for a client to work with your agency. If a funder/government entity wants you to use a technology for which survivors are supposed to sign a Release of Information, find out:

  - What is the benefit to the survivor of consenting to this release of information?
  - If there is no benefit to the survivor, then it would not be survivor-centered to ask them to give that consent.
  - What happens if a survivor does not want to sign?
  - If you are prohibited from serving that survivor without an ROI, then it is a condition of services.
  - If you can't serve the survivor under that funding stream without an ROI, and therefore your agency wouldn't serve the survivor at all, then it is a condition of services.
  - What happens if a majority or nearly all survivors choose not to sign?
  - If the funder would penalize you for not getting "enough" signed forms, then it is funder demand for you to put the program's needs above the survivor's needs.

- ✓ Avoid prohibiting survivors from using technology because of fear that your program or its services will be identified through the technology.

EXAMPLE SCENARIO: Survivor comes to a confidential location for services. The program is concerned that the survivor might be tracked by an assailant via the cellphone, which could reveal the location of the service provider and create risk for the survivor. Using best practices, the advocate discusses the concern with the survivor and is prepared to help her check her phone to see if location services are turned on, or to consider best strategy for survivor in managing a discovery that the phone is being tracked.

10. Be proactive. Stay informed about changes or new risks that could change a survivor's situation.

The 21st century is defined by rapid advances in technology and continuous product updates. Make a commitment to keep your staff informed about the products that they use to store or share survivor information.

This is where the staff member(s) who are responsible for staying abreast of technology can pay attention and notify other staff about changes.

- ✓ Create a culture of staying informed about technology that impacts survivors.

- ✓ Curiosity is key to staying informed.
    - If some team members aren't curious about technology, establish a baseline of expected competency.

- ✓ Integrate information about technology updates and changes that effect survivors into your organizational communications.
    - Annual/routine meetings, newsletters, new staff training.
    - Get key staff on listservs and set up for news alerts for technology advances.
    - Regularly read Safety Net's blog at https://www.techsafey.org

- ✓ Budget time and cost to have staff and volunteers participate in training on survivors and technology.

Author

This resource was created for WCSAP by Alicia L. Aiken, J.D. from the Confidentiality Institute.

Reading, Resources & Tools

The National Network to End Domestic Violence, Safety Net Project Blog contains information and resources mentioned in this resource.
https://www.techsafey.org

Safety Net's App Safety Center
https://www.techsafety.org/appsafetycenter

Agency Use of Technology Best Practices & Policies Toolkit
https://www.techsafety.org/agency-use

Technology Safety & Privacy: A Toolkit for Survivors
https://www.techsafety.org/resources-survivors

EmpowerDB's Encryption Checklist
https://www.empowerdb.com/EncryptionChecklist.pdf

Best Practices for Mobile Computing Devices https://www.techsafety.org/resources-agencyuse/mobilecomputing-bestpractices

Privacy Rights Clearing House
https://www.privacyrights.org/data-breaches