Questions to Consider: Technology Safety for Programs

The type of technology that victim service programs use and how it’s implemented can have a profound impact on the safety and privacy of both survivors and agencies, whether the technology is used to communicate with others, to store and manage information about survivors, or manage daily work. Through proper security and effective technology policies, programs can minimize the safety and security risks.

The following is list of what agencies should think about when they are using a particular technology.

Phones

*Caller ID*

- Does your agency block your caller ID so that when you call survivors, your organization name doesn’t show up on their caller ID?
- Does your agency have a policy to purge or not collect Caller ID information from callers to avoid collecting personally identifying information about survivors who call?
- Does your agency have a policy to delete phone bills and other online documentation that might contain personally identifying information about survivors?

*Voicemail*

- Does your voicemail message ask for the caller to state whether it is safe to leave a voicemail when their call is returned?
- Do your advocates know how to call a survivor back in a safe way?
- Does your voicemail get forwarded to an email address or text message? If so, have you addressed security and privacy concern regarding emails and text messaging?

For more information about best practices and policy recommendations on the use of phones, read [Phone Communication Best Practices](#).

Cell Phones

*Phone Security*

- Do you have a passcode lock on your phone in case it is lost or stolen?
• Are you able to remotely wipe or disable the phone in case it is lost or stolen?
• Is there security and anti-virus or anti-malware software on the phone if it’s a smart phone?

Ownership & Privacy
• Are your cell phones owned by the agency?
• If advocates are using their personal devices, are they aware of the potential privacy and security risks? How does your agency enforce policies for survivor privacy on personal devices?
• If calling survivors from personal devices, is caller ID blocking being used by dialing *67 to increase the advocate’s privacy?

Information Safety & Privacy
• Does your agency have a policy that advocates should not save survivor contacts onto the cell phone?
• Do you delete call logs, messages, and voicemails to ensure that you aren’t keeping a record of callers on the cell phone?


Texting Messaging
• Does your agency have a written policy for text messaging clients, outlining appropriate and safe use, as well as protocols for increasing privacy?
• Do you delete text message logs regularly?
• Do you talk to the survivor about the risks of having the entire conversation history on her/his phone?
• Are you aware that even if the phone’s caller ID is blocked, that you cannot conceal your phone number when texting using a cell phone unless using a virtual number?
• Does your agency have an expectation that you don’t have to respond to text messages after hours? Are survivors clearly informed of your availability and alternative options?

For more information about best practices and policy recommendations for
texting, read Texting With Survivors Best Practices.

Computers & Tablets

- Are your computers running anti-virus and anti-spyware software and if so, is the software being scheduled to run frequently?
- Is the computer password-protected?
- Do you have a computer set up for survivors to use? If so, is it set up to optimize safety and privacy?
- If you’re using a tablet, is it password protected?
- Are you running security software on your tablets?

For more information about best practices and policy recommendations for computers & tablets, read:

- Who’s Spying on Your Computer: Spyware, Surveillance, and Safety for Survivors
- Best Practices for Mobile Computing Devices
- Setting Up a Community Computer or Device Best Practices

Online Communication

Email

- Do you delete survivors’ emails from your inbox and make sure not to store their email addresses in your contacts?
- Do you delete their original email when replying so you don’t reply with the history of the conversation thread?
- Do you talk to survivors about email safety when communicating with them?
- Is your email service backing up to a third-party cloud storage system? If so, are the emails being deleted from there as well?

For more information about best practices and policy recommendations on email, read Best Practices When Using Email.

Social Media

- Does your agency have a policy that prohibits posting private and sensitive information, including information about survivors without their permission, on social media?
- Do you know how to respond safely when survivors choose to
communicate through your agency’s social media platforms?

- Does your agency have guidelines about what to post, how to respond to friends/followers who engage, and who to “friend” or “follow” on social media?

For more information about best practices on social media guidelines & policy recommendations, read the Social Media Policy Guide.

**Video Chats**

- If you are using a website for video chatting, is your agency familiar with the privacy policies of the website?
- If you are video chatting with a survivor, do make sure not to save their contact information into your contacts or “friends” list?
- Do you talk to survivors about the possibility of your contact information being in their contacts or “friends” list?
- Do you talk to survivors about the possibility of computer monitoring?
- Do you make sure that video chat conversations aren’t recorded?

**Website Safety**

- Does your website include information about computer privacy and safety for survivors who visit your website and offer a method to quickly leave your site?
- Does your contact page include a web form for survivors to reach someone (which is a safer method of emailing) rather than an email address?

For more information about best practices and policy recommendations on website safety, read Victim Services Agencies & the Internet.

**Data Management**

- Do you only collect the minimum amount of information from survivors needed to provide services in order to minimize the risk of that information being inadvertently revealed?
- What physical security measures are in place to protect all electronic and paper victim records?
- Do you have a written and enforced data retention policy?
- Do you back up your data and does your retention policy include the backup data?
For more information about best practices and policy recommendations on databases, read [Frequently Asked Questions About Record Retention and Deletion](#).

**Databases – databases managed onsite by your agency**
- Is your client and agency data stored on a server in your office?
- Does your server have a firewall to protect your computers from breaches?
- Do you have and use appropriate access levels to ensure that staff only sees information relevant to their role?

For more information about best practices and policy recommendations on databases, read [Data Security Checklist to Increase Victim Safety](#).

**Databases – databases managed by a third party**
- Do you know what their security measures are?
- Do you know who else has access to your files?
- Do know if your files are comingled with files belonging to other clients?
- Are you minimizing or removing all survivor data from the files being stored by a third party?

**Cloud Computing**
- Do you have an agreement with the cloud computing company that allows you to retain ownership of your data and that prohibits them from using, sharing, or selling it?
- Does the cloud computing service own their servers or do they lease them through another company? If a third company is involved, what are their policies? Do you have a contract with them for ownership of and access to your data?
- How does the service respond to legal requests? Do they consult you first? Are you informed of any requests for information, data shared under a request, or any breaches?
- Do you know where their servers are located and what jurisdictions do they fall under?
- Are you able to permanently delete files from their server?

For more information about best practices and policy recommendations on cloud
computing, read [Cloud Computing Tipsheet](#).

**Cameras**

- If using surveillance cameras or if recording images/video at events, do you inform people that they might be recorded?
- Do you allow people to opt out of being recorded?
- Do you allow people to opt out of having their images stored by the agency or shared with others or online?
- Do you have a policy on deleting images or video footage after a period of time?
- Do you retain images of survivors?

For more information about best practices and policy recommendations on cameras, read [Video Camera Tipsheet](#).

**Technology Security**

*WiFi Security*

- Is your wireless connection password protected?
- Are you using WEP or WPA encryption on your wireless connection?
- Do you limit who (staff, guests, survivors) can access your network?
- Do you have guidelines on accessing insecure wireless networks?
- Does staff need to use a secure link, such as a VPN, to upload or download files from your agency’s servers?

---

© 2014 National Network to End Domestic Violence, Safety Net Project. Supported by US DOJ-OVC Grant# 2011-VF-GX-K016. 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.