Mobile Advocacy: Privacy & Safety

Tablets, laptops, and smartphones can help advocates reach survivors, access files, send and receive email, and complete paperwork while away from the office, including working from home. Despite the many conveniences and benefits that these tools provide us, it is imperative that we make the privacy and safety of survivors the priority. It's important to have clear policies and procedures while also meeting confidentiality obligations. Every employee including volunteer staff should understand these policies and procedures and the importance of protecting survivors' privacy and safety.

Read more about survivors' phones and mobile devices.

Best Practices

Programs Should Provide Devices for Advocates

- Programs should own and manage phones and other mobile devices. In the event that a device is lost or stolen, programs should have the ability to wipe the device or transfer to another advocate.
- This helps ensure the security and privacy of survivors' personal information. It also gives the program more control over the accounts that are connected, apps that are downloaded, or websites visited from the device.
- Providing program-owned devices also supports advocates' work-life balance by separating work from their personal devices and making it easier for them to disconnect when they are not on shift.
- Staff should not add personal accounts, phone numbers, or apps to a work phone.

Using Personal Devices or Adding Personal Accounts to Work Devices Risks Survivors' Privacy and Program Confidentiality

- Survivors' contact information could be seen by friends or family, or disclosed if the device is lost, stolen, or if it is required to be handed over by court order.
- When an advocate leaves the program, survivors' information could be disclosed, or inaccessible to the program.

If Advocates Must Use Personal Devices… *(although it's strongly recommended that program's provide agency devices for the highest level of privacy and security)*

- Advocates can keep their phone number private by program-provided phone numbers through a VoIP (internet phone) app, a dialer app, a virtual number, or other means. If the program is unable to pay for VoIP apps/phone numbers for advocates, advocates can get a free VoIP number (Google Voice) through a program-controlled Google account. It is very important that this Google Voice number be connected to a program-owned, work-only Google account and not the advocate's personal Google account.
- In the past, advocates have tried to prevent their number from showing in the receiver's Caller ID by blocking their caller ID either through settings on their phone or by dialing a code such as *67. However, these options are be unreliable. In addition, this does nothing to keep survivors' contact info out of the rest of the information stored on the advocates' phone.
- On Android devices that support it, advocates can have a managed work profile that separates personal and work data. The separate work profile

does not come with a separate phone number, so programs will need to specify a dialer app for advocates to use.

- iOS does not support profiles in the same way, but there are services such as Microsoft Intune that allow organizations that use other company services (in Microsoft's case that would be Outlook, Teams, etc) to create a managed work profile within an Android, iOS, Windows, or Mac device. Always review what implications a service would have for advocate privacy.
- Call logs and text message logs related to communication with survivors should be deleted immediately from the advocate's phone and accounts. Survivors' contact information should not be saved in the phone or the advocate's account.
- Programs should also consider having an agency specific Mobile Phone User Agreement that includes basic privacy and security practices for advocates.

Don't Share Mobile Devices

No one but authorized users should have access to a mobile device used for work purposes if survivors' information is stored on the device. Letting friends or family do so may violate confidentiality laws and obligations.

Mobile Device Policies

Not every employee needs a mobile device. Employee responsibilities will dictate whether an agency device, and what kind of device, is necessary for that role.

- Policies should outline the purpose(s) of mobile device use for work. Policies should be clear about expectations of advocates' availability by phone when away from the office and supervisors should regularly

check in about work-life balance, boundaries, and signs of vicarious trauma or burnout.
- Each advocate should sign an agreement.

Use Program-Controlled Accounts

Program-owned devices should be set up with program-controlled cloud accounts (either Google for an Android device or iCloud for an Apple device).

A supervisor should be able to access or delete these accounts remotely in case the advocate leaves the program.

- Minimize information stored in cloud accounts, particularly regarding survivors. (Phones and apps may allow users to determine which data, if any, is saved to the cloud or other connected devices.)
- Check for and purge survivor data from the backup regularly. (Make sure updates to operating systems or apps have not reset these settings.)
- Limit who has access to cloud account logs and information. Cloud accounts can reveal personal information about the user of the device, including the location of the phone and even messages on the phone.
- If the device has both internal memory and a memory card, save to only one and regularly delete from that. Saving data to a memory card may be easiest since a memory card can be removed and destroyed.
- Before getting rid of a phone or updating the device to give to a new advocate, reset the phone to factory settings to clear any data.

Device and Account Security

Devices should be set up by knowledgeable IT staff for enhanced security and should be checked by IT staff on a regular basis. The checkup should

include needed updates, a scan for malware, a check of all installed apps, and any other security concerns.

Basic Security Measures

- Passcodes or other device locks - Do not use the same passcode for every agency device. Supervisors and IT staff should always be able to unlock the device. Each device should automatically lock after a short period of non-use. Keep software and apps up-to-date. Updates should be automatic.
- Install anti-malware software or apps. Software or apps are available for all kinds of mobile devices. Some security software, in addition to settings, allows users to locate the device if it's lost or stolen and to remotely wipe the device. Anti-malware software will prevent malware from being installed onto the device, which will increase the device's privacy and security.
- Remote wiping. Programs should have the ability to remotely wipe the content of a phone that is lost or stolen.
- Parental or monitoring controls. Programs should avoid apps or features that control or monitor an advocate's phone. This same kind of software is often used by stalkers and abusive people.

Additional Security Measures

Avoid phone settings that send an audio recording or transcript via email or text message.

- Avoid automatically forwarding office voicemail to a phone. If voicemails are forwarded, delete audio recordings, emails, and text messages of survivors' voicemails messages as soon as they have been listened to.
- Use a secure passcode for voicemail on a mobile phone.

- Do not store survivor appointments in personal calendars. Try to have an appointments-only calendar that is regularly purged and doesn't include survivors' identifying information. Consider only referring to survivors, on the appointments calendar, with a program ID number.

Read more about Phone Communication with Survivors.

Be Cautious When Using Apps

- Only download apps that are necessary for work.
- By design, some apps request access to data stored on the device – this will include survivor information if it is stored in emails, contacts, photos, or other areas in the device.
- Review the device's privacy settings and limit apps' access to data on the device. Location sharing or tracking apps of any kind should not be used to monitor staff. Instead, staff should be engaged in conversations about any safety concerns they may have while on duty and a plan should be agreed upon and implemented.
- Specific locations such as home, survivor meeting places, or work should never be saved to apps or the phone.
- Turn off location in camera apps, which will prevent the storing of location information in digital photos or videos.
- Do not download apps from outside the official app stores. External apps could make the device more vulnerable to malware or spyware. Android phones have security settings that limit the device's ability to download and install apps from "unknown sources."

Texting and Messaging Apps

- Texting and messaging can increase access for some survivors, keep survivors engaged, and can be used to relay information when a survivor isn't able to talk on the phone. Read more about Texting with Survivors.
- When texting with survivors, delete messages as soon as possible from all devices as well as cloud accounts where messages could be stored.

Agency Remote Considerations: Email, WiFi, and Accessing Files

If access to email on a smartphone is necessary, ensure that confidentiality policies and practices include accessing email on smartphones. Read more about Emailing with Survivors.

WiFi Connections

- Generally, public WiFi networks are insecure and vulnerable to hacking or interception of information. Networks that have no password, or have passwords that are publicly posted, are insecure networks.
- A Virtual Private Network (VPN) protects data while it is in transit, and protects data from being accessed or monitored.
- Use a VPN when uploading files with client information.
- Other secure methods of connecting include using the device's data plan or waiting until the device is connected to a secure internet connection.

Remote Access to Files

- Sharing and accessing remote files can be done securely using cloud services.
- Look for encryption options that don't allow the tech company to see the content of the files because only the program holds the encryption key. This is sometimes called zero-knowledge, no-knowledge, or client-

side encryption. EmpowerDB (a database tool designed for victim services providers) and Proton Drive (a general cloud storage and file-sharing service) are examples of services with this kind of encryption.

- Choose a service that allows programs to control user-by-user access to the files so employee access can be added or revoked at any time. Read more about choosing Cloud or In-House services.

Supported by US DOJ-OVW Grant No. 15JOVW-21-GK-02255-MUMU. 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.