Best Practices When Using Mobile Devices for Advocacy

Mobile devices make it easier for advocates to work while away from the office, especially those that serve large geographic or rural areas. Tablets, laptops, and smart phones can help advocates reach survivors, make files from the office accessible, send and receive email, and upload or update paperwork. Despite the many conveniences and benefits, local programs using mobile devices should be aware of their security and safety issues.

Avoid using personal mobile devices for advocacy

We recommend that advocates not use personal devices for work purposes. Although it may be more convenient to carry just one device and save money for the agency, intermingling client and work information with personal information can be extremely problematic from a confidentiality standpoint.

- If an advocate uses apps to communicate with survivors, the survivors' contact information may automatically be saved in the advocate's personal contacts and may show up on their personal phone bill.
- If friends or family use the device, they can potentially access survivors' personal information, violating the organization's confidentiality obligations not to share Personally Identifying Information (PII) with third parties.
- It will be difficult to ensure that advocates regularly purge text messages, call logs, and voicemails from survivors, or that they remotely wipe their device if it is stolen or lost.
- If survivor information is on a personal device, the advocate may have to turn over their personal device in response to legal requests for information, such as a subpoena or search warrant.

Don't share agency mobile devices

No one but authorized users should have access to a mobile device used for work purposes if survivor information is stored on the device. While it may be tempting

to lend the device to a child or a friend, it may violate confidentiality laws and obligations if survivors' personally identifying information is inadvertently shared because someone else accessed the device.

Use agency-controlled accounts

Agency-owned devices should be set up with agency-controlled accounts; for example, Google Suites for non-profits or the Apple iCloud equivalent. User access for these accounts should be accessible by a supervisor in case the advocate leaves the program. Advocates should not access personal accounts from work devices.

Use passcodes

Mobile devices can be easily stolen, misplaced, or picked up by an unauthorized user, and others could see survivors' information. Someone with more malicious intent might install a spyware program. For these reasons, the first line of defense is to lock the device.

Most devices have a basic 4-digit security lock. For stronger security, some devices can be set up with a more complex security code that can be a passcode using a longer combination of numbers, letters, and symbols; a pattern; or biometric features (like fingerprints or facial recognition). Check the settings on the devices to find these features.

Keep software and apps up-to-date

Updates to device operating systems, software, and apps ensure that the device is running the latest software version. These updates often include fixes for security issues.

Review security settings

Most smartphones and tablets have built-in security settings that will make the devices more secure. Specific security settings will depend on the type of mobile device, but a general tip is to limit automatic connections to other devices via WiFi, Bluetooth, or other connections. Some security settings may also help to

locate or remotely wipe the device if it is lost or stolen.

Install additional security and anti-malware software or apps

Software or apps are available for all kinds of mobile devices, just as they are for desktop computers. Some security software, in addition to settings, allows users to track down the device if it's stolen or remotely wipe the device. Anti-malware software will prevent malware from being installed onto the device to increase the device's privacy and security. For suggestions on software and apps, please contact Safety Net.

Be cautious with WiFi connections

One of the benefits of using a tablet or smartphone is the ability for advocates to access or upload files via WiFi. Be cautious of using public WiFi when uploading or accessing files. Generally, public WiFi networks are insecure and can be vulnerable to hacking or interception. This includes when the network has no password and when the password is publicly posted. Use a virtual private network (VPN) if uploading files, particularly when they contain client information or sensitive details. Other more secure methods include using the device's data plan or waiting until the device is connected to a secure internet connection. Read more about WiFi safety and privacy.

If advocates need to access files from outside of the office, secure access and transmission is important. Some cloud-based services offer "zero-knowledge" or "no-knowledge" encryption options in which no one, not even the tech company that runs the service, can see the content of the files because only your program holds the encryption key. Also, look for services that allow you to control individual user access, so you can add or revoke access to users as needed. For suggestions on cloud-based services, please contact Safety Net.

Be cautious with apps

Apps can make mobile devices useful for mobile advocacy. However, be sure to only download apps that are necessary for the work. Some apps may request access to data stored on the device, such as contacts or pictures. If survivor

information is stored in email, contacts, or other areas in the device or in a cloud-based account, it might be possible for some apps to gain access to that information. Review the device's privacy settings and limit apps' access to data on the device.

Do not download apps from outside the official app stores (such as Apple's App Store and Google's Play Store) since external apps could make the device more vulnerable to malware or spyware. Most mobile devices have security settings that limit the device's ability to download and install apps from "unknown sources."

Check List When Using Mobile Devices

- ❑ Do not use personal devices for work purposes.
- ❑ Do not mingle personal and professional data on the devices, particularly if professional data includes survivor information.
- ❑ Put a passcode on the device.
- ❑ Install security updates and download anti-malware protection on all devices.
- ❑ Review the privacy and security settings on the device and in each app.
- ❑ Do not use public Wi-Fi if accessing client information or other sensitive information. Instead, use a secure network or VPN to connect with the office or to share files. Also, consider using a secure cloud-based file-sharing system.
- ❑ Only download apps that are necessary for work.
- ❑ Limit apps' access to the device's location, contacts, and other potentially sensitive information.

 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 for the latest version of this and other materials.