Frontline Services' Best Practice Guide: Employee Smartphones & Tablets

This guide is for managers or workers in frontline services organisations who use mobile devices for work purposes and/or have responsibility or influence over policies on worker use of mobile devices, such as tablets or smartphones, for communicating with survivors.

Benefits of mobile devices for workers

Supplying workers with smartphones or tablets can make it easier for workers while they are on the road or away from the office. This can be especially useful when you serve a large geographic area or a rural area. Devices such as tablets and smart phones help workers reach out to survivors, access files from the office, receive email, and upload or update documentation. The compact size makes of mobile devices makes them easier to carry than a laptop. Despite their many conveniences and benefits, you need to be aware of security and safety risks that come with issuing mobile devices to workers.

1. Put passcodes on the device

Unlike a computer that is set up in a specific location, tablets and smartphones can be easily stolen or misplaced. It's also very easy for others (including a worker's friends and family) to pick up a tablet or phone and scroll through the information, which could include survivors' personally identifying information. Someone with malicious intent could install a spyware program on the device if they have access to it.

For these reasons, we recommend putting a passcode lock on all work tablets and smartphones. Most devices have a basic 4-digit security lock. For more security, some devices allow the user to set a more complex security code that includes numbers, letters, and symbols. Don't use the same passcode for every device, because if everyone knows the passcode, anyone can get into the phone or tablet. Although passcodes should not be shared with everyone, it may be useful for supervisors and managers to know the passcodes.

Some devices allow users to unlock devices with facial recognition or fingerprint scanning. The security of these features depends on the device. In some cases, facial recognition and fingerprint scanning can be relatively secure and only the person with the correct fingerprint or face can open the device. For some devices, however, merely a photo of the person can trick the device into opening. Research the particular devices your agency uses before using these other types of passcodes.

2. Run security and anti-malware software

For protection from malware, download security and anti-malware software or apps onto devices to strengthen the security. Some security software allows users to track down the device if it's stolen, and even remotely wipe the device so that whoever stole it cannot see the information it

contains. Anti-malware software will prevent malware from being installed onto the device, increasing privacy and security.

3. Create a "work" account for the device

Don't use a personal email account to set up a work device. Use your work email or create a separate email for the device. If you use your personal email account, it could mix your personal and professional information, such as contacts, calendar events, and even photos.

Ensure your policies address whether staff are permitted to sync their personal accounts to their work phones or tablets. We don't recommend this because it may lead to accidentally mixing work information (including survivor information) with personal information or accounts. For example, creating a new calendar event for a meeting with a survivor could inadvertently be added to the personal calendar that the worker's family or partner has access to.

4. Don't let others use your work mobile devices

If you are using a smartphone or tablet for work purposes, and particularly if client information is stored on the device (even if it's just their phone number), it is imperative that only authorised users are accessing the device. While it may be tempting to give the phone or tablet to a child to play a game or a friend to check something, if there is sensitive, confidential information on the device, allowing others to see it or have access to it may create safety concerns for the survivor. Similarly, limit access to devices to people in your organisation who need them to fulfil their work responsibilities.

5. Be cautious when connecting over Wi-Fi

One of the benefits of using a tablet or smartphone is the ability for workers to access or upload files without having to be in the office. However, this requires an Internet connection. Be cautious when using public Wi-Fi. Public Wi-Fi are typically insecure networks and can be vulnerable to hacking or interception. If sending information, particularly when it contains client information or sensitive details, use a virtual private network (VPN) to ensure security, the device's mobile network coverage, or wait until you're on a secure connection, such as a Wi-Fi connection that is password protected.

6. Pay attention to apps

Tablets and smartphones allow users to download all kinds of applications (apps). Be cautious of the types of apps that are downloaded. Only download apps necessary for the work that you are doing. Some free applications may access other data stored on the device, such as contacts or pictures. If survivor information is stored in email, contacts, or other areas of the device, it might be possible for the information to be accessed by these apps. Pay close attention to what data these apps are accessing and collecting by reading the permissions, either on the device or the app's website.

7. Think carefully about installing monitoring software

Some organisations may be tempted to install monitoring software on devices so they can monitor the location or activities of employees. First, check to see if it is legal for your organisation to monitor and track your workers. Second, think about the worker's privacy. Some monitoring software is more invasive than others. Third, some monitoring software requires that the device be jailbroken (if it's an iPhone) or rooted (if it's an Android), which means basic security protections are removed. This can make the device more vulnerable to hacks and malware.

8. Review device settings

Location: We recommend you minimise location sharing on mobile devices. Even if workers are not being abused or stalked, they are often with survivors and are sometimes targeted by abusers. Go through the location privacy settings or app settings and turn off location to apps that do not require your location information.

GPS and Wi-Fi: If these features are not in use, consider turning them off and only turning them on when needed.

Call & text logs: Particularly if you are calling survivors regularly, all logs of incoming and outgoing calls and texts should be purged regularly. If the phone uses both an internal memory and a memory card, save to only one and regularly delete.

Calendar events: Sometimes, workers will use their calendar to schedule meetings with survivors and include other details. Consider creating a separate calendar specifically for meetings with survivors. You can easily delete calendar events or the entire calendar if needed.

9. Consider whether to do backups

Determine if the worker's device requires a backup. If it's purely a communication device, there might not be any information that needs to be backed up. Not backing up a device means that private information (such as a meeting with a survivor at her house or a text message between the worker and a survivor) does not get saved. Backups will be saved until deleted, and may result in private information being kept longer than needed.

If a backup is required, review backup settings and only back up what is needed. Also make sure that access to the backup is secure.

10. Giving the phone to new staff

Before giving a used smartphone or tablet to new staff, it's important that the device be reset to factory setting. This will remove all content from the previous worker and ensure that the new worker has a clean device to set up.

11. Workers should not use their personal devices

Because many workers already have personal smartphones and tablets, it may seem more convenient to carry just one device, and more cost effective for the agency. While this may be the case, intermingling client and work information with personal information can be extremely problematic from a safety and privacy standpoint.

The risks for workers using their own mobile devices to communicate with survivors include the following:

> Worker's friends and family members could have access to the device and inadvertently see survivor information in the contacts, in email, or text messages. In addition, a worker's personal phone could also be part of a family plan, allowing all account holders to have access to phone records and other information.
>
> If the phone is lost or stolen, others could have access to the data in the smartphone or tablet. If the lost device was owned by the agency, the policy could instruct that all the data on stolen or lost device be remotely wiped immediately. If it was the worker's personal device, mandating a remote wipe would mean that they would lose all personal data on that phone. Keep in mind that remote wipes do not delete data saved from data backups.
>
> Organisations may not have authority to demand that workers use certain safety and security measures on their personal devices. For example, with work device, you can have a policy that unless needed for work purposes, mobile phones should not be used to access certain websites that may be vulnerable to viruses. Organisations do not have the authority to limit what a worker does on their personal device.
>
> If a worker leaves the organisation, the organisation will be unable to access the content on the phone. This could possibly leave the organisation in the position of being unable to pick up where that person left off and follow up with survivors.

Ultimately, your organisation should have ownership over the mobile devices used by its workers, and the content and data that is stored in phones.