BC Society of Transition Houses

Anti-Violence Program's Guide: Mobile Phone Use

Many anti-violence programs frequently use mobile phones to communicate with program participants. While mobile phones are ubiquitous and offer convenience and ease of access, cellular devices also raise privacy and safety considerations. As with the use of any type of technology, it is important to have clear policies and procedures to outline proper use to maintain privacy and safety for program participants, your staff and the program under the applicable privacy laws.

Purpose of Mobile Phones

First, assess the reasons why your staff would be using mobile phones for work. These reasons will be the foundation for policies that address staff mobile phone use. Some common practice reasons include being easily accessible while out of the office, answering crisis calls off-site and texting with program participants.

Not all employees need a mobile phone for their work and anti-violence workers who have different roles may need a mobile phone for different reasons. The policy should reflect these varying uses. For example, a PEACE Program counsellor who travels to meet with children and youth at a school may need to make phone calls and send text messages to communicate with the program participants, while a community outreach worker may need to access on-line forms and applications and her work email while out of the office meeting with women.

Mobile Phone Policy Recommendations

- Policies should outline the purpose(s) of mobile phone use for work, and have an individual Mobile Phone Use agreement with each employee.
- Policies should be clear about expectations of staff availability by phone when away from the office to set boundaries that achieve work-life balance.
- The Office of the Privacy Commissioner of Canada recommends that organizations offer agency owned devices and accounts if programs are delivering digital services. Although a significant financial commitment, this practice allows for better staff coordination across shifts and can increase privacy and security for the program participants and the program.

Risks when Anti-Violence Workers Use Their Personal Mobile Phone at Work

When personal mobile phones are used, third parties could view confidential and personally identifiable information of program participants accidentally or intentionally. Mobile phones are mini computers and gather significant amounts of information in the contact files and email and text message histories.

If the personal phone of the anti-violence worker is part of a family plan, the account holder (which may not be the employee) could have access to phone records and other details that could include program participant's information breaching confidentiality and the privacy interests of the women, children and youth being supported. If the phone is lost or stolen, the program may not be able to demand that data on a lost phone be remotely wiped, or if an employee leaves the program, information on their personal phone may not be accessible to the program. If Programs do use an anti-violence worker's personal cell phone for work communications it may increase privacy risks if the phone is used for personal and work purposes and if evidence is stored on the phone, such as photographs, the phone may be subpoenaed in court proceedings as it holds potentially relevant information.

Benefits for Agency-Issued Mobile Phones

Agency-issued mobile phones enable organizations to better ensure the security of devices, strengthen confidentiality practices, and support a healthy work-life balance for staff.

When agencies own and manage a mobile phone, they can set up and have control over the phone and accounts associated with it. This includes the data on the device as well as data that is in the connected cloud accounts (Google account for an Android phone and iCloud for an iPhone).

If a phone is stolen or lost or if a staff person using the phone leaves, the program can easily transfer it to another colleague, or wipe the device clean. Owning and having control over the mobile devices allows the agency to control the accounts that are connected, apps that are downloaded and websites visited from the device.

Devices

A variety of mobile phones exists ranging from flip phones, voice and text only cell phones to an array of smartphones. The mobile phone can be matched to the type of support provided. For example, if a PEACE program counsellor primarily communicates with children, youth and parents through phone calls or sending texts, a simple cell phone model may be more appropriate and safer. For staff who plan to use video calls with their program participants, smartphones may be preferable. If employees need to travel for work, smartphones that can access apps such as maps or the Internet may be advisable.

Consider if staff need a mobile phone for their job responsibilities and if so provide the type of mobile phone that would be most appropriate for the support services they provide to women, children and youth.

Phone Security

Mobile phones 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. Additionally, you may consider implementing the following basic security measures:

- **Passcodes** - All phones should require a passcode, password, biometric factor, or other security measure to unlock the phone. Do not use the same passcode for every agency-owned phone however; supervisors or IT staff should have assess to the passcodes to unlock the phones in case staff cannot. All phones should automatically lock after a short time when not being used.
- **Anti-virus and anti-malware apps** - All phones should have anti-virus or anti-malware software or apps installed and updated regularly.
- **Remote wiping** - Agencies should have the ability to remotely wipe the content of a phone that is lost or stolen.
- **Parental controls** - Programs should exercise caution when considering installing or enabling features that permit controlling or monitoring of the phone. These features should be used with the employee's informed consent.

Smartphones and Cloud-Based Accounts

Most smartphones require a specific account to be connected to the phone. Generally, iPhones require an iCloud account and Android phones require a Google account. Depending on the type of phone, the manufacturer may also offer an account for the phone to offer different apps, manage security features, or store additional data. While phones connected to a cloud account may back up information from the phone by default, it is best that any personal information about a program participant not be backed up. This may mean turning off the synchronizing of most services and apps.

Recommendations

- Do not use the same cloud account on more than one phone. Doing this will connect all the phones to one account, which means that some information, such as contacts or messages, could be shared among the phones.
- Minimize the amount of information synced to cloud accounts, particularly information regarding participants. Most smartphones and apps allow users to determine which data, if any, is synced to the cloud or other connected devices. Check for and purge any program participant data from the backup regularly. Also, check to make sure that updates to operating systems or apps have not reset these settings.

- Limit who has access to the cloud's 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 sent through the phone.

Location Services and Apps

Phones should not have location sharing or tracking turned on without the informed consent of the employee. Some programs may want to track the location of a program-issued phone for the safety of the worker or to locate a lost device.

If using location services for apps (such as Maps), anti-violence workers should understand the benefits and risks of using location services. Location history could be stored on the device or cloud accounts associated with the device or apps. Keeping location history could violate a program participant's privacy or become a safety issue if the anti-violence worker met with the participant. Employees might also be targeted by a perpetrator and so should have their real-time location information protected as well.

Recommendations

- Phone location should not be stored in the history of the device and should be turned off or set to a less accurate setting if not needed by the anti-violence worker.
- When using location services for apps such as maps or navigation, the location history should not be stored. If this is not possible, it should be deleted regularly.
- Specific locations such as home, program participant meeting places, or work sites should not be saved to the app or phone.
- Turn off "geotagging" in camera apps, which will prevent the storing of location information in digital photos or videos.

Voicemail

Some phone systems offer the ability to receive an audio recording or a transcript of the voicemail in an email or text message. This creates a risk of interception or inappropriate access if the email or text is delivered to the mobile phone.

Recommendations

- Avoid automatically forwarding office voicemail to a mobile phone.
- If voicemails are forwarded, delete audio recordings, emails, and text messages of program participant's voicemail messages as soon as possible.

- Use a secure passcode for voicemail on a mobile phone.

Texting & Messaging Apps

Texting and messaging are other ways programs can connect with program participants. Messaging can increase access for some participants, keep participants engaged, and can be used to relay information when a participant is not able to talk on the phone. Communicating via chat is more secure when done through a web based chat tool rather than from a mobile phone.

Recommendation

- Delete messages as soon as possible from all devices as well as cloud accounts where messages could be stored.
- Do not store the program participant's contact information on the mobile phone.

Email

Depending on the employee's job responsibilities, they may need to access email while out of the office. Access to work email from a smartphone could create security risks. If access to email on a smartphone is necessary, ensure that confidentiality policies and practices include email access via smartphones.

Remote Access to Files & VPN's

If staff need to access files from a phone (or another device such as a tablet or laptop) while away from the office, secure file sharing "cloud" services exist to help manage security. Look for "No-Knowledge" or "Zero-Knowledge" encryption options where the tech company itself cannot see the content of the files because they do not hold the encryption key – only the program does. Also, choose a service that allows you to control user-by-user access to the files so you can add or revoke access at any time.

Another option is to use a VPN (Virtual Private Network) from a reputable provider, which will provide a strong layer of security for the data that staff is sending and accessing. Bear in mind that a VPN will not protect the data from access or monitoring while the data is on the phone, but will increase data security while it is in transit.

Contacts, Call Logs & Text Logs

Minimize the amount of information saved on the phone. Agency policies should include deleting information regularly, in most cases as soon as allowable under the program's privacy policies.

Recommendations

- Do not save program participant contact information on a mobile phone.
- All incoming and outgoing calls and texts should be purged according to the program's privacy policies.
- If the phone has both internal memory and a memory card, save to only one and regularly delete from that at the appropriate time. Saving to a memory card offers greater protection since a memory card can be removed and then destroyed at the appropriate time.
- Before recycling a phone or updating the phone to give to a new employee, re-set the phone to factory settings to clear any data that is on the phone and not needed to be stored per the program's privacy policies.

Calendars

If the calendar on the phone includes appointments with program participants, schedule meetings in a way that reduces the likelihood of being identifiable. Some calendar programs allow users to create multiple calendars. Consider creating a calendar for appointments only, which can be synced to the phone and then deleted when no longer needed.

Personal Accounts on Work Phones

Smartphones, and the apps installed on them, have the ability to have more than one account configured to it. Staff should not have personal accounts configured to a work phone. Having a personal account on the phone could lead to accidentally mixing program participant information with personal information or accounts.

Use of Personal Mobile Phones at Work

While the Office of the Privacy Commissioner of Canada recommends that organizations offer agency owned devices and accounts if programs are delivering digital services, in the situations when anti-violence workers use their personal mobile phone to communicate with program participants it should be done so with specific considerations given to privacy and security.

Recommendations

- Agencies should develop a Bring Your Own Device Policy as outlined by the Office of the Privacy Commissioner of Canada.
- Anti-violence workers can use a virtual phone service and voicemail to contact a program participant, allowing the employee to keep private their phone number.
- Alternatively, an employee can prevent their number from showing in the receiver's Caller ID by either dialing *67 before dialing the number or turn off "Show My Caller ID" in the smartphone settings.
- Call logs and text message logs related to communications with program participants should be deleted immediately from the anti-violence worker's personal phone. Participant's contact information should not be saved in the personal phone.
- Agencies might consider including privacy and security practices described above in a Mobile Phone User Agreement with an employee.

If your agency has any questions or needs guidance on how to implement the use of digital services and mobile phones, please contact the BCSTH's Technology Safety Project at rhiannon@bcsth.ca.

Adapted for Canada from and in cooperation with the Safety Net Technology Project at the National Network to End Domestic Violence, United States