HOW TO OPERATE AS A REMOTE WORKPLACE DURING A PUBLIC HEALTH CRISIS

This handout was adapted for the Australian context under license from the National Network to End Domestic Violence (NNEDV).

During a public health crisis such as the current COVID-19 pandemic, when public health officials recommend "social distancing" to slow the spread of infection, technology such as remote access to files, instant messaging, and video calls may be used to maintain service operations while allowing staff and volunteers to work remotely. Many of these tools may be beneficial for outreach work at any time.

In considering new technology, survivors must be at the centre of our decision- making. This is true in ordinary times and must still apply even in a public health crisis.

While Safety Net recommends a thoughtful and carefully planned approach to using technology, the urgent nature of the current public health crisis may lead some SADFV services to consider using technology on a quick timeline. We encourage any services that implement these technologies during the current COVID-19 pandemic to do so temporarily and re-assess once the pandemic has passed.

1. Consider what services can be done remotely with web chat or video calls. Read more about Using Technology to Communicate with Survivors During a Public Health Crisis, and see NNEDV's Digital Services Toolkit.

2. Use tools that allow staff and workers to work from home. This includes tools to allow staff and volunteers to communicate with each other (e.g. calls, instant messaging, video), and tools for sharing information while maintaining confidentiality (e.g. secure file sharing).

The following is a list of tools that programs might consider for communicating with survivors remotely that we think meet current best practice standards. Two key factors to consider in any tool are 1) encryption options where the tech company itself cannot see the content of the encryption key – only you do, and 2) user access options that allow you to control user-by-user access to the content.

While we do not endorse these tools, they are well-suited to protect privacy as they are currently set up.

- ResourceConnect – instant messaging for staff and volunteers
- Gruveo – video call
- Cyph – video call, messaging, groups
- Tresorit, SpiderOak's Semaphor, Mega, Sync, and pCloud – file sharing

We share this list in an effort to reduce the privacy risks that go along with rushing to adopt tools quickly without time for more thorough evaluation.

In addition to these newer tools, also consider how you can increase safety and privacy when using older technology like email and phone:

- Best Practices When Using Email
- Best Practices for Using Mobile Phones
- Best Practices for Texting with Survivors

We recommend offering service-owned devices and accounts. This allows for better staff management across shifts and can increase privacy and safety measures. Read more about best practices for when using mobile phones for program delivery.

Survivor safety and privacy is important. When frontline workers use mobile devices or tools to communicate about or with survivors, threads, conversations and other related records likely include personally-identifying information. Consider developing guidelines on how and when these communications will take place.

Using technology to work remotely helps to support worker health and wellbeing. A crisis like COVID-19 should not override our commitment to staff well-being. Workers should not have to risk infection to do their jobs. Staff should be able to be "off-duty" to make sure they are properly nourishing themselves and resting – both key points given by public health officials to maintain a strong immune system.

We know that with any type of public health crisis, access to services can be even harder for survivors who are seeking resources and support. By adjusting how we operate to meet the needs of survivors and their support workers, while also understanding the risks of using technology, we can help to ensure that survivors and advocates have the information they need to get help, and also do their jobs to the best of their ability.

The Infoxchange has a wealth of resources on technology for nonprofits, including discounted software licenses and hardware, technology training for staff, and information.

Keep in mind that these suggestions are geared towards nonprofit organisations generally. Many of the technology tools they suggest may be appropriate for day-to-day operations, but would not be appropriate for communicating with survivors or sharing survivors' personally-identifying information.

We update our materials frequently. Please visit TechSafety.org.au for the latest version of this and other materials.