Many victim service programs have computers or WiFi networks available for survivors to use. Survivors can use a shared computer or WiFi network to do research if they are relocating, to apply for jobs, benefits, or housing, and more. Access to WiFi or a computer can also help survivors stay in touch with their support system and keep them from feeling isolated.

Programs should ensure that the computer or WiFi network is as safe and secure as possible to protect the privacy and safety of users. Below are some tips and best practices for securing shared computers and WiFi networks.

**Shared Computers & Devices**

1. Set up a guest account for survivors to use. Guest accounts don’t have administrator rights, making it more difficult for malware like viruses or spyware to be installed accidentally. Protect shared computers and devices from malware by running anti-virus and anti-spyware software and by keeping all operating systems, software, and apps up-to-date. Talk with your IT staff or consultants about additional steps to secure the computer or device.

2. Protect against accidental or inappropriate access from the shared computer. Set up your network so that the shared computer doesn’t have access to your program’s shared drive and vice versa. Set up a separate printer for use by survivors.

3. Place the computer in an area that allows for privacy. If the computer has a built-in camera or a webcam, provide a space for clients to use the webcam that will not reveal others in the background, or, in a shelter, give away any location information (i.e., street sign through the window, etc.). Place a removeable web cam cover over the camera lens when the camera is not in
use, to prevent accidentally showing the room or whoever is in front of the camera if it is turned on automatically.

4. On computers and other devices, install basic programs for word processing, a secure web browser, Adobe Acrobat reader, and other programs or apps users would typically need. Remind survivors not to save personal files on the shared computer.

**Data Storage for Survivors**

When survivors need to save documents like resumes, forms, or other information, one option is to give them USB drives. Some USB drives offer additional security options such as password protection and encryption.

Another option is to help survivors set up a new “cloud” accounts for online storage. If a survivor is concerned about the abusive person or anyone else accessing the account, discuss setting up a brand new account that doesn’t connect to older accounts through the same email account, phone number, or profile picture, for example. Online storage is available for free; paid services offer more space and options.

**Internet Access from Shared Computers**

For users to be able to use the shared computer most effectively, it should be connected to the internet. To support privacy and security, use a combination of technical security and education for survivors.

1. Set all browsers on shared computers and devices to the most private and secure modes by default. Detailed information for most major web browsers can be found in our resource [Browser Privacy Tips](#).

2. Educate users about online privacy and remind them to log out of online accounts. For more information, read [Online Privacy and Safety](#). Remind survivors not to save personal information, such as website favorites or
bookmarks, usernames and passwords, credit card information, or other personal information on the shared computer. Encourage survivors to use a password manager for usernames, passwords, and other sensitive information. For more information, read Password Security.

Shared WiFi Network Access

Survivors may bring their own devices, such as smartphones or tablets, to the shelter, program, or office. Set up an alternate guest network for survivors and visitors to use. This separate network can have a different network name and password than the one used by staff for program business. You can then easily change the password to that guest network when you need to, without having to update staff access. A guest network also protects against accidental or inappropriate access to WiFi administrator settings or to information from the traffic of the main network. For more information, read WiFi Safety & Privacy: Tips for Victim Service Agencies & Survivors.

Blocking Content or Websites

Some programs consider blocking potentially offensive content from web browsers on shared devices or networks. Most web browsers, and some WiFi network settings, allow you to block certain content. This is usually found under “parental controls.” If necessary, you can use these features or other site blockers to restrict access to certain websites.

Keep in mind that there may be legitimate reasons for survivors to access “adult” content. For example, victims may be harassed through revenge porn sites or online communities that might have sexual, offensive, or violent content, and access to those websites may help them stay up on the abusive person’s state of mind, activities, threats, or harassment. Alternately, survivors might want to look up information about sexual health and healing on websites that might be blocked because it includes adult or sexual content.
While some shelters may not want to allow adult content because children are around, having a blanket policy that prohibits access to adult sites, or certain search terms, might be a barrier. Bear in mind that requiring survivors to ask you for permission to access some content, or monitoring web browsing, doesn’t support survivors’ autonomy.

**Policies and Procedures**

Some programs may want to ask survivors to agree to certain policies or conditions before accessing shared devices or WiFi networks. Try to keep any such policies simple, clear, and relevant. Remember that some abusive people control access to devices and the internet as part of abuse, and advocates don’t want to replicate abusive behaviors. As much as possible, programs should support survivor autonomy and empowerment. Help survivors understand the reason behind any restrictions. For example, a shelter’s internet bandwidth might not allow for residents to stream videos. Explain that the limitation is due to budget or technology, not because survivors aren’t allowed to watch movies.

**Education & Resources**

Programs can offer (but should not require) internet safety information. Providing survivors with education and resources on technology safety and security empowers them and enhances self-advocacy. In turn, less staff time is needed to monitor shared technology security issues. These resources could be available through bookmarks on a shared computer, printed out, or discussed during support group meetings, for example.

Here is a list of resources you can share with survivors that help to increase privacy and security:

- [Password Security](#)
- [Online Privacy and Safety](#)
- [Video Series about Online Privacy and Security](#)