NNEDV

Setting Up a Community Computer or Device
Best Practices

Many victim service agencies have computers or laptops that are intended for survivors or residents to use. Having a computer in a shelter or program is a great way to empower survivors by allowing them to apply for jobs, fill out housing forms, research new locations or schools, and more. Access to a computer can help survivors stay in touch with their support system and can keep them from feeling isolated. The goal of the agency is to ensure that the computer is as safe and secure as possible so that spyware or viruses aren't inadvertently installed. Below are some tips and best practices for protecting your community computer or laptop.

Computer Set Up

If you can, set up the computer so that it has guest accounts without administrator rights. This will make it more difficult for anyone to download anything onto the computer without administrator access. Work with your computer technician to lock down the system from unauthorized changes to the hard drive. Also, enact features that will allow saving of documents to external devices only and not the internal hard drive.

If you can afford it, give survivors USB drives, so they can save important documents on it. That way, they are able to save it to their own storage device and not onto the computer where anyone can open it and see. If this is an affordable option, remember to discuss the importance of password protecting the USB drive.

Don't connect the computer to the rest of your computer network. This will lessen the risk of someone using that computer to access your agency server or files. You can do this by making sure that the computer's discovery mode and file sharing are turned off, since some computer operating system allows computers to share files with each other when computers are on the same network.

Software

Protect the communal computer from viruses, malware, or spyware by running anti-virus and anti-spyware software and by keeping up-to-date firewall protection. Ensure that all software, patches, and updates are regularly installed to keep the computer from unwanted viruses and glitches.

Install basic programs on the computer, such as Microsoft office, a secure web browser, Adobe reader or writer, and other programs users would typically need.

Internet

For users to be able to use the community computer most effectively, it should be connected to the internet.

Most web browsers will allow you to block certain content, and you can find it under parental controls. If necessary, you can use these features or other site blockers to restrict access to certain sites. Restricted access should only be limited to sexually explicit sites or other inappropriate websites since some shelters may not want to allow adult content because children are around. But keep in mind that many abusers harass and abuse victims on porn/revenge porn sites and on sites that are not "family-oriented." If the survivor is trying to stay up on what's happening, having a blanket policy that prohibits access to adult sites might not be helpful for them. Consider allowing concerns and needs of individual survivors to guide these decisions and do so on an individual basis.

You can increase victim's privacy by limiting the information that web browsers collect. Most browsers have incognito or private browsing that doesn't save the browser activity history. This is helpful so others can't scroll through the history to see what was being viewed. An example of a browser that doesn't store browsing information is duckduckgo.com.

Utilize the browser settings and tools to automatically delete internet tracking, history, cookies, site blocking, auto-complete features, and login information. Do not allow browsers or other sites to auto-save logins and passwords. Go through the privacy and security settings for each computer to set the defaults in the most

protective way (for example, a default setting can tell the computer that you never want to save a password versus having to remember each time a site checks the "remember me" box by default). Educate users and remind them to log out of online accounts.

Portable Online Browsing

It is possible to use a USB drive to run web browsers (so it's not using the actual program on the computer). This provides an extra layer of privacy and security for the user. They can bookmark pages and save their personal materials onto that specific drive and not on the computer. Mozilla Firefox, Chrome, and even Tor have versions of this. You download the program onto a USB and use that USB to run the program.

Education & Resources

Programs can offer (not require) survivors and their children internet safety information and strategies. Providing survivors with education and resources on technology safety and strategies empowers them and enhances self-advocacy. In turn, less staff time is needed to monitor safety concerns or issues. Computers with internet access can also be used to place phone calls, send text messages, etc., so include education on safety and privacy when using those types of technology as well.

Other Safety Tips

Place the computer in an area that will allow for some privacy from others. If the computer has a built in camera or a webcam, provide a space for clients to use the webcam that does not give away any location information (i.e., street sign through the window, etc.). The space should also minimize exposing others in the background.