Developing Program Policy on Staff Use of Personal and Remote Devices: Ten Tips

Victim service provider staff are increasingly using electronic devices offsite to communicate with survivors and to access survivors' personal information remotely. Many of these organizations, however, have been slow to develop and implement policies that address staff use of these devices. While each provider's needs and services are unique, there are some general principles and policies that organizations should consider and address. The following "Ten Tips" are a starting place for this discussion. They highlight some key policies and practices organizations may wish to consider.

1. Require passwords for all electronic devices. Passwords may not be stored in obvious or accessible locations (e.g., passwords should never be stored on slips of paper tucked under the keyboard!)
2. Passwords for all devices that contain survivors' personally identifying information should be changed at regular intervals.
3. Determine whether you will allow staff to use personal devices to access client-related information, whether by email, text, remote computer access. If you will allow it, develop specific policies to govern their use.
4. If staff may use personal devices for work purposes require deletion of survivors' personal information stored on personal devices at the end of each week, month or quarter or as appropriate.
5. Require deletion of all client-related documents from staff's personal devices at the end of a staff person's affiliation with the program.
6. For any personal device that receives client-specific, personally identifying information, prohibit notification/banners for emails or texts so that such information does not appear on the home screen, and instead may only be viewed after a password has been entered.
7. Consider who, if anyone, will have remote access to electronic client files. Maintain adequate safeguards. For example, require approval for every ISP address authorized to access client information.
8. Develop and implement policies regarding staff use of home computers and other devices for client-related purposes. For example, address whether participants' personal information may be left up on a screen if the staff person steps away or if documents may be printed on a home printer with participants' personal information, and whether they must be shredded or kept secure pending a return to the office.
9. Specify the level of security required on devices carried outside the office. For example, require mobile devices to be protected with fingerprint recognition or with a 6-digit (rather than 4-digit) password.
10. Require staff, contractors, and any other individuals who access participant information outside the office on personal or work devices to sign an agreement to abide by the organization's policies governing use of personal and remote access of electronic devices.

 This project was supported by grant number 2013-TA-AX-KO18 awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, and conclusions expressed are those of the author(s) and do not necessarily represent the views of the U.S. Department of Justice.