



Questions to Consider: Technology Safety in Your Program

CALLER ID

- Do Staff and volunteers who make calls from home either have Line blocking or block each call made to victims?
- Do Advocates know what to do if they call a victim and hear a recording that the victim does not accept blocked calls? Unblocking the call is not always a safe option. Many operators will connect the call.
- Does your staff block caller ID on Fax lines when possible? Do they call ahead to ensure your fax is getting to the appropriate person? Do they know to cut the header off the page before sending it on or filing?
- Does your program test Line blocking on a regular basis since phone service can change without the domestic violence program realizing that the lines are unblocked?

EMAIL

- Do staff and volunteers refrain from keeping victim email addresses in a their computer address books? Do they make sure to delete all email from victims to prevent virus/worms from broadcasting emails from victims to the “world” and also prevent unintended “worm” emails from being sent to victims?
- Does your program regularly update virus protection programs?

DATA

- To avoid data breaches and hacking, does your program keep any confidential information about victims on computers that are not connected to the Internet?
- Does your program have a firewall installed to help protect your computers from hackers?
- Does your program have organizational policies that include electronic and paper information practices? Are these policies survivor-centered? For example: survivors should be able to see their records at any time.

- What physical security measures are in place to protect all electronic and paper victim records?
- What is your procedure for the secure disposal of confidential papers, computer hard drives, and other electronic media (i.e. disks, external or USB hard drives) that contain client-identifying data?
- How are backup copies of the data be made? What media do you use to back up data? Where is the original data and these backup copies stored?

DATABASES

- Access levels enable a very small number of staff to see all information in a database, and all other users to only see the appropriate information relevant to the specific clients who choose to access an agency's services and/or relevant to the role of the user (volunteer, staff, attorney, etc). How do you determine who needs to have access to the data and what level of access is appropriate? How is access to the data limited to these authorized persons?
- Audit trails are an important element in data security, providing a detailed record of every query and action of every user. How are audit trails designed into your databases and where are the log files stored?
- Since every user must have a separate and unique user name and password for every database, how are these accounts generated and what technical support resources are available if users forget or lose their passwords? Specifically, how do you ensure that users do not share accounts if passwords are forgotten?
- When protecting vulnerable victim information, it is important to strip personally identifying victim information (such as name or birth date) from a database as soon as possible and appropriate, perhaps at the end of a calendar year. Identifiable data can be removed, leaving demographic data for evaluation purposes. Databases can be designed at the outset to automatically purge certain data elements. How and when do you remove personally identifying information from a central system?
- Since victim safety issues are always changing, it is imperative that victims have the option to remove their information from databases. At initial intake a victim may consent to having minimal information in a database and decide only days later that her abuser may have access to someone inside the system which threatens her safety and confidentiality; thus she may request the removal of her records from the system. What is your process for allowing victims to have their information removed from databases?