**Confidentiality Best Practices**

**Purpose:** Tohelp simplify the confidentiality agreement that is required by all staff/volunteers who work with CalFresh Outreach. Participating in CalFresh is a personal matter that the individual may want to keep private. In addition, someone’s personal information in the wrong hands can lead to a lifetime of trouble for that person.

**Personal information can be anything that identifies a person and can include:**

* Contact information
  + Name, address, phone number, email, birth date, social security number, etc.
* Physical identifiers
  + Height, weight, hair and eye color, tattoos and piercings, etc.
* Geographic identifiers
  + Region, name of dorm rooms or other residence location, groups/clubs associated with, class schedule, place of employment, etc.

**When collecting someone’s personal information:**

* Always write down their information yourself, or provide them with a blank page so that they are not seeing the information of other’s that you have already collected
* Store personal information in an envelope so that it is put away and protected until you are able to securely store it
* Do not hold on to someone’s personal information for long periods of time, make every effort to store it in a locked cabinet or drawer or input the information in a secure document immediately after obtaining
* When finished with using someone’s personal information the document should be deleted or destroyed by shredding
* If you do not shred the document right away, then store it in a locked cabinet or drawer until ready to be shredded

**Tips for protecting confidential data that has been collected:**

* Always confirm the identity of anyone who is requesting confidential data
* Never share personal information of someone you have helped with anyone other than that person or share personal information about co-workers or other organizations
* Discuss confidential information in a secure room or a room with closed doors
* Aggregate data that is to be shared or used for statistical and reporting purposesbyremoving personal identifiers, changing names to numbered codes, blacking out or removing contact information and only specifying geographic identifiers for large areas
* Encrypt data that is to be transferred electronically and do not fax confidential data unless over a secure line (such as to your local county office)
* Identify a Security Systems Administrator to maintain current records of all who have access to confidential data, and to maintain verification systems such as employee log-in’s and passwords, and for removing access to employees/volunteers who are no longer working with the program
* Require a secure user name and password when logging on to any system that contains confidential information and password protect specific files that contain confidential information
* Limit access to confidential data to only those who truly need it

**Safeguarding Workstations and Records**Here are a few tips for safeguarding your workstation and physical records:

* Store files you are not using in locked offices or cabinets
* Clear desks and workstations of sensitive information when you are out of the office or when others are in your office
* Promptly pick up print jobs, faxes, and photocopies
* Arrange computer screens, whiteboards, and documents so that they cannot be seen by unauthorized individuals
* Lock your office or secure your workstation at the end of each day if you have files about with confidential information
* Do not allow anyone to borrow your key, ID card, or access card

**Secure Internet Use**

* Set browser security preferences to medium or high
* Only download and install authorized programs
* Only visit trusted and known websites
* Avoid sending sensitive information over the Internet
* Comply with Internet and network security procedures
* Don't download or send confidential information if you are on an unsecured network (e.g. home, hotel, coffee shop, etc.
* Understand the social media policy before posting information about your campus on social media outlets

**Being Discreet with Private Information**

It is important to guard against unintentional disclosure of private information:

* Speak quietly in public areas (waiting room, hallways, elevators)
* Avoid using specific names and individualized information in public areas
* Use a private office when discussing sensitive information
* Disclose private information only to those who have a need to know
* Be cautious when entering your password or personal information on an untrusted computer

**Document Destruction**

Documents containing private information cannot simply be thrown in the trash or erased. Instead, most organizations have a document disposal policy that includes:

* Return original documents to their owners
* Shred paper files and documents when no longer needed
* Use a tool to erase or destroy data stored on hard drives, removable storage media, and other electronic devices