# Safely Disposing of Your Devices

Getting a new computer, notebook, tablet or other technology for your business is often necessary to keep up with the times. After purchasing new technology, you may decide to dispose of your old devices. Whether you recycle, give to a family member or employee or donate to a charity, a school or a soldier, you need to protect the information on the devices from exposure. However, removing your information is harder than it seems. Systems are set up to protect us from losing information we need—when we delete a file, we can still get it back. Similarly, others who get your discarded computer or other device can get it back, too.

You need to take extra steps to remove information from your computing devices before you discard them. That private data could harm you, your employees or your business if it ends up in the wrong hands. Private data, such as insurance and banking information and account numbers, tax information, Social Security numbers, health information, customer names, addresses and accounts, employee payroll and benefit information and passwords all have value to hackers and thieves, opening the door for identity theft. Your business reputation is at risk, along with customer confidence, and significant financial losses are a very real possibility.

Removing information from computing devices is called “clearing.” The National Institute for Standards and Technology (NIST) states that clearing is “a level of media sanitation that does not allow information to be retrieved by data, disk or file recovery utilities. It must be resistant to keystroke recovery attempts from standard input devices [such as a keyboard or mouse] and from data scavenging tools.”

**Techniques for Removing Information**
Three ways of removing information from your computing devices, from the least effective to most effective, are deleting, overwriting and physically destroying the device holding your information.

**1. Deleting**

Deleting information is not effective. It removes pointers to information on your device, but it does not remove the information. This "holding area" essentially protects you from yourself—if you accidentally delete a file, you can easily restore it. However, you may have experienced the panic that results from emptying the trash bin prematurely or having a file seem to disappear on its own. The good news is that even though it may be difficult to locate, the file is probably still somewhere on your machine. The bad news is that even though you think you've deleted a file, an attacker or other unauthorized person may be able to retrieve it.

Do not rely on the deletion method you routinely use when working on your device, whether moving a file to the trash or a recycle bin or choosing “delete” from a menu. Even if you “empty” the trash, the information is still there. It can be retrieved.

**2. Overwriting**

Overwriting is effective on all computing devices. It puts random data in place of your information, which cannot be retrieved because it has been obliterated. While experts agree on the use of random data, they disagree on how many times you should overwrite to be safe. While some say that one time is enough, others recommend at least three times, followed by “zeroing” the drive (writing all zeroes).

There are software programs and hardware devices available that are designed to erase your hard drive, CD or DVD—but because these programs and devices have varying levels of effectiveness, it is important to carefully investigate your options. When choosing a software

program to perform this task, look for the following characteristics:

- "Secure Erase" is performed. Secure Erase is a standard in modern hard drives. If you select a program that runs the Secure Erase command, it will erase data by overwriting all areas of the hard drive, even areas that are not being used.
- Data is written multiple times. It is important to make sure that not only is the information erased, but new data is written over it. By adding multiple layers of data, the program makes it difficult for an attacker to "peel away" the new layer. Three to seven passes is fairly standard and should be sufficient.
- Random data is used. Using random data instead of easily identifiable patterns makes it harder for attackers to determine the pattern and discover the original information underneath.
- Zeros are used in the final layer. Regardless of how many times the program overwrites the data, look for programs that use all zeros in the last layer. This adds an additional level of security.

**3. Physical Destruction**

Physical destruction is the ultimate way to prevent others from retrieving your information. Of course, you should physically destroy the device only if you do not plan to give it to someone else.

Specialized services will disintegrate, burn, melt or pulverize your computer drive and other devices. If for some reason you do not wish to use a service, it is possible for you to destroy your hard drive by drilling nails or holes into the device yourself or even smashing it with a hammer. Never burn a hard drive, put it in the microwave or pour acid on it.

Some shredders are equipped to destroy flexible devices such as CDs and DVDs. If you smash or shred your device yourself, the pieces must be small enough that your information cannot be reconstructed; 1/125” is ideal. Wrap the CD or DVD in a paper towel when destroying it to limit shrapnel.

Magnetic devices, such tapes, hard drives and floppy disks, can be destroyed by degaussing—exposing them to a very strong magnet. Degaussers can be rented or purchased. Because of the expense, degaussing is more appropriate for businesses than for individuals. It should not be used if someone else will be using the device because degaussing destroys not only the information but also the “firmware” that makes the device run.

**Mobile Phone and Tablet Advice**

Although the exact steps for clearing all information from your mobile phone or tablet are different for each brand and model, the general process is the same:

1. Remove the memory card if your device has one.
2. Remove the Subscriber Identity Module (SIM) card.
3. Under Settings, select Master Reset, Wipe Memory, Erase All Content and Settings (or a similarly worded option). You might need to enter a password you have set, or contact a local store that sells the equipment for assistance with a factory-set password.
4. Physically destroy the memory card and SIM card, or store them in a safe place. (Memory cards can typically be reused, and SIM cards can be reused in a phone that has the same carrier.)
5. Ensure that your account has been terminated and/or switched to your new device.

For detailed information about your particular device, you can consult online documentation or the staff at your local store.

**Your Cyber Liability Experts**

For more information on how to safely dispose of your devices and keep your sensitive data safe, contact Huckaby & Associates today.