# Safely Disposing of Your Devices

New, revolutionary technology is released constantly. Every day, new gadgets are touted as the must-have tool to ensure future business success. Some businesses, in their scramble to cash in on the technological gold rush, ditch their old devices without a second thought.

Neglecting to safely dispose of your devices can spell disaster for your business. However you dispose of them—whether donating, selling or recycling—you must remove the sensitive information on the devices to prevent third parties from obtaining it.

But removing that information is harder than it seems. Systems are constructed to protect users from losing the information they need. Take extra steps to remove information from your computing devices before you discard them, lest your data ends up in the wrong hands.

Private data, such as account information and passwords, represent a significant vulnerability to your business' cyber-security. The theft of sensitive data can threaten your business' reputation and customer confidence, and can generate steep fines under the General Data Protection Regulation (GDPR).

## Common Techniques for Removing Information

Simply hitting the delete key does not completely remove your sensitive data from devices. Deleting removes pointers to information on your device, but it does not remove the actual information. Deleting a file sends it to a 'holding area' from which you can restore it. So even when you think you have deleted a file, unauthorised people can recover it.

Do not rely on file deletion. Instead, choose one or more of these five options recommended by the Information Commissioner's Office (ICO).

### *1.* Physical Destruction

Physically destroying a device can be a viable option for preventing others from retrieving your information. You can destroy your hard drive by drilling nails or holes into the device or even smashing it with a hammer. Never try to destroy a hard drive by burning it, putting it in the microwave or pouring acid on it.

Some shredders are equipped to destroy flexible devices such as CDs and DVDs. If you smash or shred the device yourself, the pieces must be small enough that your data cannot be reconstructed—0.2 millimetres is ideal. Wrap the CD or DVD in a kitchen towel when destroying it to limit shrapnel.

Magnetic devices such as tapes, hard drives and floppy disks can be destroyed by degaussing, which is exposing devices to a very strong magnet. You can rent or purchase degaussers. They destroy not only the device's information but also the firmware that makes the device run. You should only use degaussers when you plan to dispose of the device.

### *2.* Overwriting

Overwriting is effective on most computing devices. It replaces your sensitive data with random data, and because of this your data cannot be retrieved. While experts agree on the use of random data, they disagree on how many times one should overwrite to be safe. 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 can overwrite your hard drives, CDs and DVDs. However, because these programs and devices have varying levels of effectiveness, it is important to carefully investigate your options. When choosing software or a device to overwrite your data, look for the following characteristics:

- 'Secure Erase' is performed. Secure Erase is a standard in modern hard drives used to completely erase and overwrite all data on a hard drive.
- Data is written multiple times. It is important to ensure that not only is the information erased, but new data is

written over it. By erasing the original then adding new data, the programme makes it difficult for an attacker to uncover any traces possibly left behind by the original. Two passes is usually sufficient.

- **Random data is used.** Using random data instead of easily identifiable patterns makes it harder for attackers to discover any original information buried underneath.
- **Zeroes are used in the final layer.** Regardless of how many times you overwrite your data, rely on programmes that use all zeroes in the last swipe—this adds an additional level of security.

### *3.* Restoring to Factory Settings

Many devices have the capability to revert back to their factory settings. Activating this function will return the device to the state in which you bought it. Unlike other deletion methods, restoring to factory settings works for devices both with and without removable or accessible storage media.

However, not all manufacturers implement a secure data wiping stage during the factory reset process. Check with your device's manufacturer to determine whether the factory reset process is sufficiently secure.

### *4.* Sending It to a Specialist

There are numerous organisations which will securely delete data from a range of devices and types of media. These organisations erase or overwrite data for businesses and individuals. As an added bonus, some specialist organisations may be able to return, reuse or recycle your media or device after they have securely deleted your data.

However, because you trust this business with wiping your devices clean, you should make sure their deletion processes are secure. If possible, perform another secure deletion method or restore your devices to their factory settings before sending them to a specialist organisation.

### *5.* Formatting

To 'format' something means to prepare a storage medium like a hard drive for use. When you format a hard drive, your operating system erases all 'bookkeeping' information your drive uses to organise data.

But formatting a hard drive does not erase all of that drive's data—it sequesters and retains it until it is overwritten.

Formatting is often used in conjunction with overwriting to provide further assurance that data cannot be recovered. Formatting a drive without relying on any additional data deletion methods is never sufficient to remove data, since it can be easily recovered using freely available software.

## Mobile Phone and Tablet Advice

Although the exact steps for clearing all information from your mobile phone or tablet vary among different brands and models, the general process, enumerated below, remains the same across the board.

1. Remove your device's memory card.
2. Remove the SIM (Subscriber Identity Module) 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 the manufacturer for assistance with a factory-set password.
4. Physically destroy the SIM and memory cards or store them in a secure 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 or switched to your new device.

For detailed information about your particular device, consult your manufacturer's online documentation or the staff at your local mobile store.

## Your Cyber-Liability Experts

Data is valuable. Letting it fall into malicious hands simply because you neglected to safely dispose of your devices could be a costly mistake that jeopardises the future of your business. For more information on securely protecting your data and safely scrapping your devices, contact the insurance professionals at Sentio Insurance Brokers Ltd today.