**How To Safely Erase Your Data In This Digital Age? Data Erasure vs. Degaussing**

There are several standards for deleting data with confidence, as well as various ways for doing it. There might be major security concerns if this isn't done appropriately.

Most of you are probably aware that when data is accidentally deleted from an IT device, it may be restored using basic data recovery software. As a result, in recent years, the necessity of being able to wipe data with perfect assurance has grown.

Assume you're cleaning out a hard disc that contains sensitive information. It might be anything from a hospital's medical data to a company's credit card information to designs for secret weapons in a defence facility. What do you do with an IT device's hard drive? There are severe questions of compliance at stake here.

**Keeping Your Information Safe**

According to a 2012 research, the globe would create roughly 5.2 TB of digital data for every IT device user by 2020. According to many analysts, this number will skyrocket in the next years as the number of Internet of Things (IoT) devices grows by the day.

Furthermore, as the culture evolves away from hard drives and toward digital platforms, data protection throughout the lifespan of a piece of hardware – including IT disposal – is becoming a growing problem.

**What are the various methods for erasing data from old hard drives?**

There are three approaches for ensuring that the data cannot be recovered:

1. Degaussing
2. Overwrite on existing data
3. Physical destruction on hard drive.

**Method 1 - Degaussing**

Hackers can retrieve data from a hard disc using data recovery software, so if you want to assure complete data destruction, you'll need to utilise a more effective way. In this case, you should call a competent IT equipment recycling company to guarantee that your IT devices are properly disposed of.

Degaussing is a useful process for erasing data from magnetic cassettes or hard drives.

The physical technique of data destruction used by the degaussing equipment is based on the effect of a high electromagnetic pulse on the drive. As a result, the carrier's magnetic domains are evenly magnetised to saturation. The information contained on the medium is lost as a result of the loss of magnetic transitions. Furthermore, total destruction of the carrier's original magnetic structure ensures the annihilation of all data ever stored on it.

Degaussing has a number of drawbacks in addition to its advantages. Previously, this technology could only be used with magnetic cassettes.

**Method 2 - Using Software to Remove Data**

One of the most common ways to permanently remove sensitive data is to use software. Without specific gear, data on flash storage devices and hard drives is wiped.

Different data destruction apps utilise different approaches, but they all follow the same rule: the data on the hard drives is rewritten. The software works its way across the hard disc sector by sector, setting each bit to zero or generating random data. This is often repeated several times to ensure that no remnants of the original magnetic pattern remain.

Software-based data erasure, however, has two major drawbacks:

* The procedure of erasing all data from electrical equipment may take a long time.
* Many sections of hard drives are inaccessible, and the software will be unable to erase them.

**Method 3 - Crushing**

Shredding services are provided by several firms that specialise in eliminating private data.

It would be nearly hard for someone to put the parts back together and reconstruct it in this manner, especially if the crushed pieces are mixed up with others, making it impossible to tell one from the other.

You may also purchase a crusher for your own usage, but this is a prohibitively costly investment that does not always prove to be more profitable than renting a crushing service. Furthermore, these data destruction businesses will generally provide you with a certificate confirming that the data has been deleted, which can come in handy if you need to prove it legally.

1. Is it going to erase confidential data quickly?
2. Is there an erasing service offered by the company? Many vendors can erase your data onsite. This reduces the time and risks involved in the deletion process. This is especially useful when there are large amounts of data to be deleted.
3. Are they able to provide a certificate of data deletion?
4. Is it able to erase all data types?

**What Should You Use: Data Erasure or Degaussing?**

When it comes to erasing information from hard drives, software-based data erasure isn't always the best solution. As a result, you should use the degaussing procedure to wipe all of your personal information.

Secure data destruction services are quickly becoming the go-to option for companies looking to decrease the environmental effect of throwaway technology. Explore how [Recycle Pro](https://www.recyclepro.co.uk/) can satisfy your recycling needs if your company is searching for a safe way to dispose of hardware, hard drives, or any other technology that satisfies regulatory criteria.