Electronic Data Disposal

c-hq security services
Technical Consulting

WHAT IS DATA DESTRUCTION?

Data Destruction is the process of removing data form an electronic storage device and making it unrecoverable. This vital process protects your private information from being reconstructed and used in a malicious way.

You may be surprised to learn that simply deleting a file does not necessarily remove it from your system. There are several methods to securely delete files and this article discusses the various steps that you can take to protect yourself, your company and your private information.

> “simply deleting a file does not necessarily remove it .”

WHY DO I NEED DATA DESTRUCTION?

Sensitive data may include bank account details, passwords, personal information, commercial and security information or even information relating to national defence. Whatever the nature of the data, it is important to ensure that it is secure; even after it has been deleted.

Most offices have a paper shredder and it is now common practice to shred anything containing personal information, why then do we not take the same precautions when removing files digitally. If your mobile laptop or tablet computer are lost or stolen it may be possible for someone to recover the deleted files using standard off the shelf file recovery software.

Simply deleting data does not permanently remove that information from the storage device, file information is kept in a directory on the hard disk and when a file is deleted, that file is removed from the directory only and marked as available space leaving the original data in place to be overwritten.

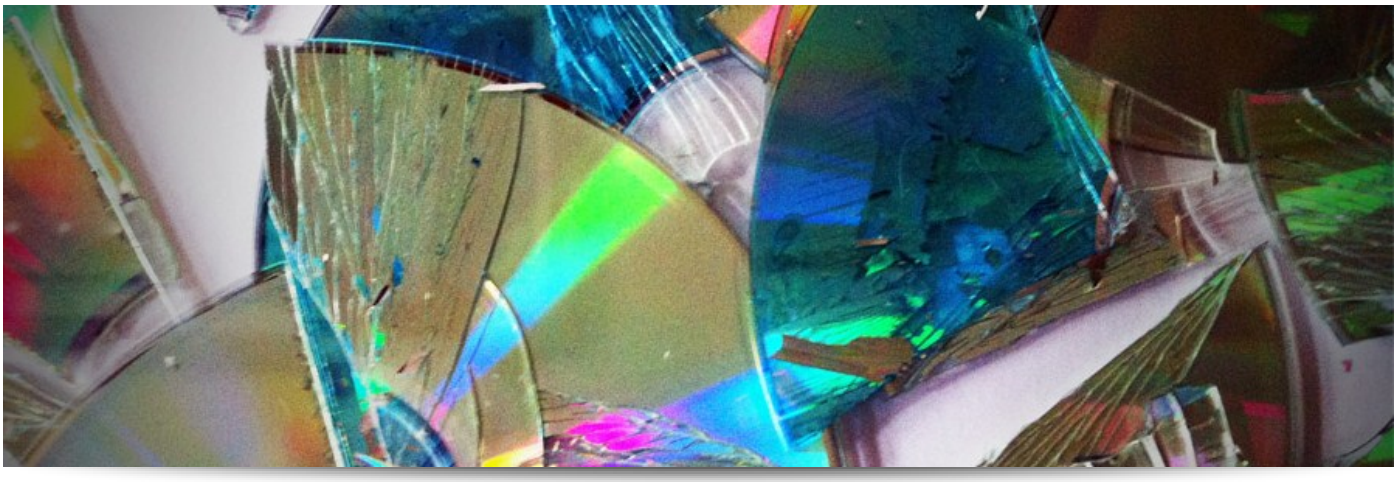
WHAT HOLDS MY DATA?

Your computer’s hard drive isn’t the only device that can hold sensitive Information. Other electronic equipment may hold sensitive data and even though it has been deleted, it may be recoverable.

- USB storage devices
- CD’s
- Mobile phones
- Cameras
- Printers and plotters
- Dictaphones
- Media Tablets
- Local Servers
- Voice mail machines

Smart phones can hold as much important information as a computer. They often store bank account details, emails, contact information and social media applications.

Many smart phones have a reset function built in to the system that will remove all data from the phone. However it may not securely format the drive. Much the same as a computer’s hard drive, the deleted files will be marked as available space but are still recoverable. The solution is to use the overwriting method by formatting the phone and repeatedly filling the hard drive with large files such as podcasts and movies. This has to be done manually and can be very time consuming. The more times this is repeated, the harder the data recovery will become.



Electronic Data Disposal

c-hq security services
Technical Consulting

> “The Gutmann Method is widely considered to be the most secure method by overwriting the data thirty five times.”

> “Physical destruction of a storage device is possibly the only way to completely remove the information.”

HOW TO PROTECT YOUR PRIVATE INFORMATION

There are several ways you can permanently remove data depending on the recording medium used:

Overwriting works by replacing your data with random text, it repeats this task many times. Each overwrite is known as a pass. It is a popular and relatively low-cost option; however the more times that the information is overwritten the more secure the deletion but also the more time consuming. A very time consuming technique is “The Gutmann Method”, which is widely considered to be the most secure method by overwriting the data thirty five times with carefully selected data patterns. However the United States Department of Defence recommends that data should be overwritten only seven times. This has a decreased level of security but is much faster than the Gutmann Method and therefore more efficient.

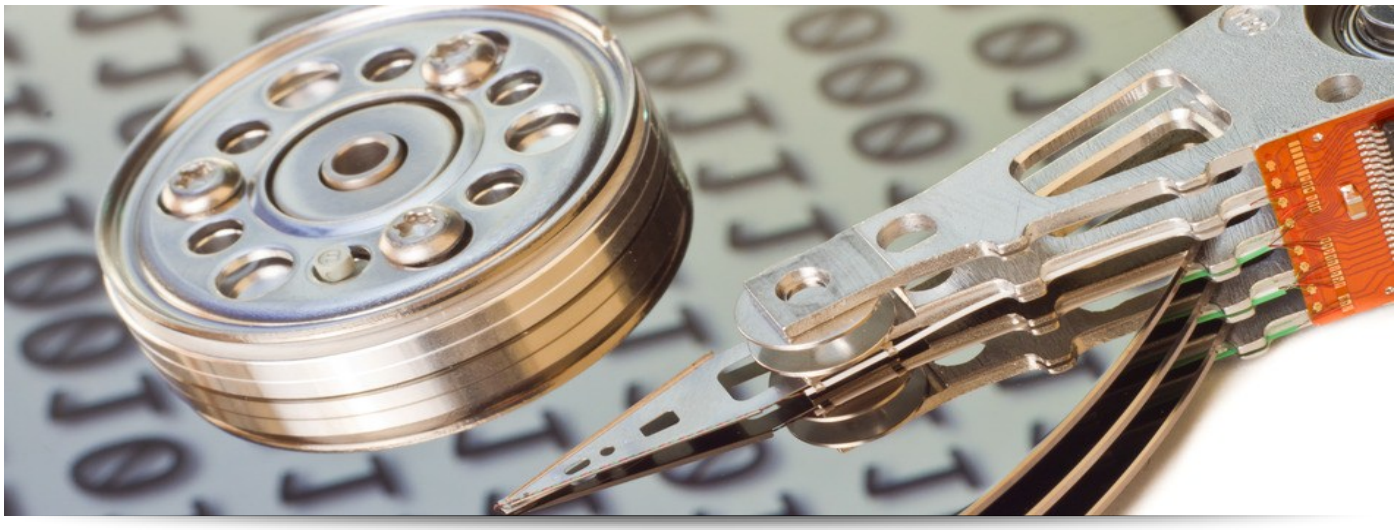
Degaussing is a method of removing the magnetic fields from a hard disk or any other magnetic storage device. This method removes all data and often renders the hard disk inoperable. This can become very costly to replace hard disks but it is a good solution for out of date computers that are being discarded. Solid state hard drives and optical media devices such as CDs and DVDs do not rely on magnetic fields to store data so degaussing will not have any effect on these.

Physical destruction is simply destroying the device that holds information through force. This is the best method for low cost storage devices especially CDs, DVDs and USB memory sticks.

Information stored and deleted on an encrypted disk remains unreadable as data is stored in characters that can only be read by having the correct password to decrypt the hard drive making the information readable again. Without this password, deleted files remain as secure as the encryption used.

CONCLUSION

Physical destruction of storage devices is possibly the only way to completely remove information, however this is often not a feasible solution. You should evaluate the sensitivity of the data and determine an appropriate destruction procedure dependant on the level of security, cost and time available. Whichever method you choose, please remember that once deleted, data may be able to be recovered.



c-hq security services
T. +44 (0) 1825 841261 | E. info@chqconsulting.co.uk | W. www.chqconsulting.co.uk