

# **A Guide to Computer Data Security**

## **Corporate & Personal**

**This guide is specific to your computer  
Hard Drive Data Security**



## Contents

	Page
About this Guide	3
Why is Data Security so important?	4
What is a Hard Drive?	5
How is Data Retrieved?	6
How is Data Erased?	7
How do I ensure Data Security at work?	8
How do I ensure Data Security at home?	9
Compliance & Certification	10
Alternatives to Data Erasure	11
What are the legalities?	13
Understanding the Risks and who can help?	14
Who are EOL IT Services?	15
References	16





## About this Guide

[EOL IT Services](#) has produced this guide on computer hard drive data security due to feedback received from our clients, their staff and our own employees. There has been so much media coverage regarding the importance of commercial and personal data security and yet so many people are still getting it very wrong.

As a responsible service provider and employer, EOL is aiming to educate as many people as possible regarding the risks of insufficient or no data security.

**"99% security is no security at all!"**

There is so much confusion surrounding the measures that need to be taken to ensure complete data destruction. We hope this guide will answer your questions and help you make the right decision when its time to dispose of the data stored on your hard drive.

Although electronic data can be stored on many different types of equipment including printers, fax machines, PDA's and more, this guide will only focus on data stored on computer hard drives.



## Why is Data Security so important?

Whether you're storing work related data on your office PC or personal data at home, when it's time to dispose of your PC or Laptop, you must ensure that any redundant data is disposed of correctly.

We are all very aware of the threats surrounding losing our electronic data through viruses or hardware failure, or the risk of our data being shared without our consent due to spyware or hackers. Everyone is also cautious these days about shredding paper based information, but how much care do we take when disposing of redundant IT equipment?

We must now all pay attention to the risk of our data getting into the wrong hands when disposing of our IT equipment. Correct data erasure at the end of its life is as important as the protection of our data whilst in use. We have all seen the ever increasing stories in the press regarding identity theft and fraud.....



“Identity theft soars as gangs target wealthy”  
The Daily Mail – October 2007

“Identity theft is all too easy”  
The Financial Times – December 2007

“ID theft fears lead millions to change passwords”  
The Telegraph – December 2007

....let's not make it any easier for these people to obtain our confidential information.

Research carried out in 2007 from BT and the University of Glamorgan, Edith Cowan University in Australia and Longwood University in the USA<sup>1</sup>, revealed that a significant number of hard disks which are bought second-hand contain sensitive company and personal information. Amongst the information found on the analysed disks were salary details, financial company data, bank and credit account details, hospital/medical data, pornography, visa applications and online purchasing details.

The research found that just over 37 per cent of the hard disks still contained personal data. This shows little improvement on the same research carried out in 2005 and 2006.

I'm sure many people reading this will remember the more publicised data security blunders in recent years. Sir Paul McCartney's name has been in the media<sup>2</sup> when some of his personal information made it in to the public domain, as has leading banks and now the HMRC. A verified Paypal account with a balance can fetch between £25 and £250, depending on how much money the Paypal user has sitting in the account. The same is true for bank account details.

The next most valuable piece of information is your e-mail password. It can fetch £1 to £75 depending on whether your account has been used for spamming previously. E-mail passwords allow access to an e-mail account and are typically used for sending spam.

Data security is clearly a problem – lets work together to resolve this issue.

## What is a Hard Drive?

Your Hard Drive will usually be contained within the main unit or casing of your computer. This is normally easy to access by removing certain screws or clips and opening the unit. However, before doing this, ensure the unit is completely disconnected from any power supply source and that you are using the correct tools.

As the primary communication device to the rest of the computer, the hard drive is very important. The hard drive stores most of a computers information including the operating system and all programmes. All this information is stored on the Platters.

Having a fast CPU (Central Processing Unit) is not much use if you have a slow hard drive, because the CPU will be spending time waiting for the information from the hard drive. If you experience a problem with your hard drive it is possible that data could be lost or corrupted.

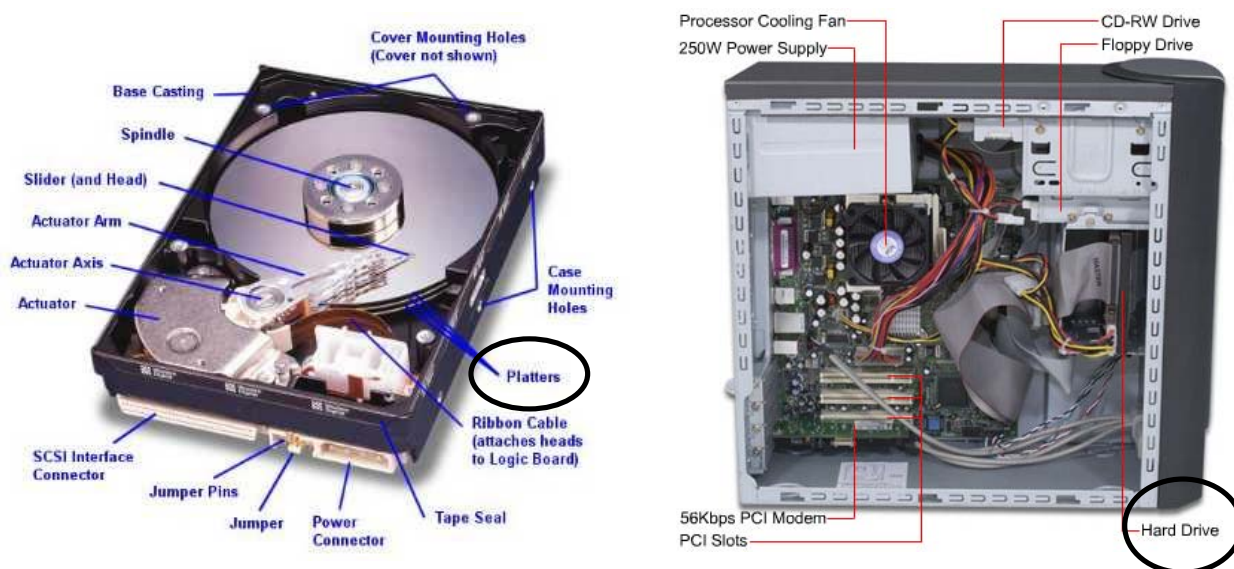
The hard drive stores data including text documents, pictures, programmes, video clips, etc. All this information is stored on the Platters.

Hard drives have become more and more reliable over the years as technology has progressed. They are however still one of the most likely components in your computer to fail as they are one of the few components with moving parts.

A hard drive, also known as a hard disk or disk drive, is really a set of aluminum disks with a magnetic oxide coating. Each of the disks has data recorded electromagnetically in concentric circles or tracks. Each track is also divided in to sectors (a set of which is known as a cluster).

Hard drives come in various sizes (the larger the drive, the more data can be stored) and with various rotation speeds

Hard drives store and read data in what is known as binary code – this means that information is stored very densely as 0's and 1's around the disc.



## How is Data Retrieved?

EOL once spoke to a prospective client – a large international bank – and asked if they would like us to take care of their data security in conjunction with carrying out their IT asset recycling. The bank explained that all data would be wiped from equipment before EOL collected it from their premises. When they explained that their data erasure processes was to 're-format' the drives we voiced our concerns. To add weight to our opinion we offered to collect a re-formatted hard drive and try to retrieve some data. We easily managed to retrieve 25,000 files! Needless to say, their processes soon changed.

Many people believe that re-formatting a hard drive will make data irretrievable – WRONG! Many free products are available to download from the Internet which can retrieve data from re-formatted drives. Re-formatting is NOT erasing. It simply prepares the drive for new data – but the old data is still there, even though it's slightly hidden. It's like putting a piece of underlay over an existing carpet – it does a great job of preparing for the new carpet, but the old layers are still underneath.

Even hard drives which have been physically destroyed can still contain retrievable data. A tiny piece of a hard drive Platter can contain 100's of Megabytes of data. However, you would need to be very determined and have access to sophisticated equipment to obtain the data.

Clicking 'delete' on a file won't do exactly what it says either. Most programmes move files to a 'holding area' rather than deleting them. Data is stored randomly on hard drives – the computer uses a File Allocation Table (FAT) to track the used and unused sections of the disk. Deleting data simply removes it from the file allocation table, freeing up those sectors to store new data when required. There are numerous software options available, as well as companies, which will provide access to data which was thought to be 'erased'.



## How is Data Erased?

### Overwriting

Data can be erased using a method known as 'overwriting'. Many erasure software options use a binary (ones and zeros) code to overwrite the existing data. This is often also referred to as 'wiping' or 'shredding' a file or disk.

The simplest overwrite technique writes the same data everywhere - usually a series of zeros. At a minimum, this will prevent the data from being retrieved simply by reading from the medium again, and is therefore often used for clearing data.

To overcome more advanced data recovery techniques, specific overwrite patterns are often utilised. These may be generic patterns intended to eradicate any trace signatures. For example, overwriting using a reoccurring pattern of ones and zeros may be more effective than zeros alone. Patterns based on the existing data may also be used, such as the complement, or bitwise inverse or NOT, of the existing data. For example, if the existing data is 1101 0110, its complement would be 0010 1001. Combinations of patterns are frequently specified.

One challenge with an overwrite is that some areas of the disk may be inaccessible, due to media degradation or other errors. Software overwrite may also be problematic in high-security environments where stronger controls on data are in place. The use of advanced storage technologies may also make file-based overwrite ineffective.

Overwriting is only secure providing a successful wipe is completed. If for any reason there is a fault with the hard drive, then physical destruction should be carried out. When using a software based erasure method, you should also be 100% sure that there aren't any hidden or disconnected hard drives within the computer which the software could miss.

### Degaussing

Another way to eliminate information on a hard drive is to degauss\erase the information. Degaussing is a magnetic field created using an alternating field of sufficient intensity to saturate the media. The magnetic field is then slowly withdrawn or reduced and the magnetic media is left in a magnetic neutral state, or erased. Part of the hard drive has a program called a servo, installed on the drive by the manufacturer, which also is erased. Degaussing the servo does render the drive useless and therefore this is not the most environmentally friendly option as the hard drive cannot be reused.



## How do I ensure Data Security at Work?

When it is time to dispose of your work PC or Laptop, securing the data stored on the hard drive needs to be properly managed. Most organisations have processes in place – whilst many of these are good, not all are sufficient.

You and your organisation should always consider the following factors when disposing of equipment:

### **The Seven Security Steps**

#### **1) What is most important – price or security?**

The cost of correct data security may be higher, but what will the costs be if data escapes from your organisation? Damage to your reputation can be 100 times worse than the actual data discovered.

#### **2) Have a plan**

It is crucial when dealing with commercial data that a detailed security plan is in place to ensure that the correct steps are followed.

#### **3) Be Pro-Active**

Make sure that your plan is in place and your staff are trained and aware of procedures before anything goes wrong.

#### **4) Be aware of your responsibilities**

Public companies must not only follow their internal procedures, but also adhere to regulations such as Sarbanes-Oxley, HIPAA and FACT Act. Although Private companies are not subject to the same laws, the consequences can be equally damaging if corners are cut.

#### **5) Limit the possibilities**

Now that most people have a USB stick in their handbag or attached to their car keys, limit the opportunities where data can be stored using other media.

#### **6) Know your equipment**

Keep up to date asset records and track your equipment throughout its lifecycle.

#### **7) Use a professional, accredited supplier to ensure correct disposal**

Not only can the correct supplier protect your data security, but by working with them and choosing the most suitable form of data erasure, you could also help to protect the environment by enabling your redundant equipment to be used again in complete or component form.



## How do I ensure Data Security at Home?

The average user probably does not realise the risks by selling their old computers on websites such as E-Bay. They may delete all their files, re-install the operating system and possibly re-format the drive, yet the data will probably reside on the disk, typically in unallocated space. Discarding computer equipment without due care, could lead to irreparable, financial and personal damage to the owner.

Many of us retain data such as bank details, medical records, online purchasing information, passwords and much more on our personal computers. To ensure complete data security, you must choose one of the following options:

### **1) Use a third party supplier to erase your data**

If you do decide to pass your retired computer to a professional organisation, make sure you do your homework and you are confident in their wiping or data destruction procedures.

### **2) Purchase data erasure software to wipe your own hard drive**

Once again, check, check and check again that you are buying the correct software. The cheapest option may not save you money in the long run!

### **3) Physical destruction**

If you would prefer to physically destroy your hard drive, ensure that you do it safely and where possible try to ensure that any remaining parts are as small as possible. Data can be retrieved from small sectors of a hard disk. Having the metal ground to a final powder state is the best ultimate solution. However, so long as the Platters are sufficiently damaged it should deter most determined criminal interest.



## Compliance & Certification

When it comes to compliance and certification, there are certainly lots of 'standards' out there. The most commonly mentioned standard is the US Department of Defense (DOD) Sanitizing standard DOD 5220.22-M. This standard is taken from the US DOD's National Industrial Security Program Operating Manual. The manual addresses how to prevent the unauthorised disclosure of classified information.

Other common standards are as follows:

- Air Force Systems Security Instructions 5020
- Bruce Schneier's algorithm
- BSI (German overwrite by Federal Office for Information Security/Bundesamt für Sicherheit in der Informationstechnik)
- German Standard VSITR
- CESG HMG Infosec Standard No 5 (baseline)
- CESG HMG Infosec Standard No 5 (enhanced)
- Navy Staff Office Publication (NAVSO P-5239-26) for RLL
- NSA (overwrite standard by National Security Agency)
- OPNAVINST 5239.1A
- Peter Gutmann's algorithm
- The National Computer Security Centre (NCSC-TG-025)
- US Army AR380-19

Probably the highest and certainly the most respected and well known level of certification is the CESG HMG Infosec Standard No 5 - enhanced level. It is approved to wipe UK Government Top Secret data and has also been approved by NATO.

Communications-Electronics Security Group ([CESG](#)) is the Information Assurance (IA) arm of Government Communications Headquarters (GCHQ). CESG are the UK Government's National Technical Authority for IA and are responsible for enabling secure and trusted knowledge sharing to help customers achieve their business aims.



## Alternatives to Data Erasure....



Physically destroying your hard drive should work, but it may not be safe to do so.



Drilling or punching your hard drive may deter someone from retrieving data, but the data will still be there – it could also be dangerous if not done using the correct tools and protective equipment.



Setting fire to your hard drive may work but it is dangerous and bad for the environment.





Putting a blow-torch to your hard drive may work but it is dangerous and bad for the environment.



Rubbing the hard drive with an eraser will definitely not work!



Hitting your hard drive with a bolt of lightning may work but it is a little difficult to predict where it will strike and highly risky to your personal well being.

There are clearly alternatives to using an external service provider but you need to consider the issues of Health & Safety and the Environment. You should ask yourself "Is it really worth the risk of a DIY solution?".

## What are the Legalities?

The Data Protection Act (DPA) is a UK Act of Parliament. The Act defines a legal basis for the handling of information in the UK which relates to living people. This includes names, birthday and anniversary dates, addresses, telephone numbers, fax numbers, e-mail addresses, etc. It only applies to that data which is held, or intended to be held, on computers or held in a 'relevant filing system'. The Office of the Information Commissioner (OIC), an independent government authority, oversees compliance with the Act.

Although the Act does not mention privacy, in practice it provides a way in which individuals can enforce the control of information about them. This Act is used by many UK companies & organisations. It is the main piece of legislation that governs protection of personal data within the UK and defines eight principles of information-handling practice, as listed below.

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-
  1. at least one of the conditions in Schedule 2 is met, and
  2. in the case of sensitive personal data, at least one of the conditions in schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.



## Understanding the Risks

There will always be risks – there will always be someone out there trying to develop new ways to retrieve or access others data. Do all that you can to ensure your work and personal data security by following the guidelines in this book.

If using an overwriting software solution - ensure the wipe is 100% successful and that there are no other drives present within the equipment.

If physically destroying your drive - ensure remaining fragments are as small as possible (ground to a powder state if possible).

If using a third party company to manage your data security – do your homework and make sure you trust a professional, accredited company with a good reputation.

As an employer – ensure your organisation has the correct procedures in place to avoid data leakage. There's no retrieving the data once it's out there.....

Data breaches cost US companies an average of \$197 per record in 2007, according to a study by the Ponemon Institute - the average cost of a data breach was \$6.3 million, up from \$4.8 million in 2006<sup>3</sup>. In the UK, 37million items of personal data went missing in 2007<sup>4</sup>. The risks are very real!

Just as we now all shred our bank statements before putting them out for the dustman, secure your electronic data to the best of your ability before retiring your hard drive.

## Who can help?

There are a number of service providers out there who can help you with your data security requirements. When choosing a provider, please take the following into consideration...

- Can the supplier provide you with a certificate of data destruction?
- Can you observe the destruction of your data if you so choose?
- Is the service provider using environmentally friendly methods to destroy your data where possible? Do they have a zero landfill policy?
- Can your service provider give references from other professional or public sector organisations that have used its services?
- Which certificates does the service provider hold? ISO 9001, ISO 14001, etc.
- What insurances are in place in the event of data leakage?
- Are you able to track your equipment through their internal system – do they have a comprehensive asset tracking system?
- How secure is their building/s and transport? Are their staff security checked? Are their vehicles data tracked?
- Are you able to audit / inspect the facility where your equipment will be stored and your data will be wiped?
- Can you provider erase the data at your own site if so desired?

All of these aspects are worth considering and investigating before you hand your data over to someone else!



### Who are EOL IT Services?

[EOL IT Services](#) have been established since 1996 providing data security, managed IT services and IT asset recycling to businesses in banking, financial services, law, healthcare, the public sector and many more.

We understand the importance of complete data security and it is essential that our clients feel confident in our ability to deliver this service.

EOL has never allowed a single piece of data to escape its premises. Our 100% success rate further demonstrates our commitment to this crucial aspect of our business.

Personal and business data security really is so important to everyone and we hope you found this e-zine informative and useful, if so please pass this booklet on to anyone you think may find it of interest

### Your thoughts...

We would value your feedback and any ideas for improvement regarding this e-book. Let us know what you think by e-mailing us at [marketing@eolitservices.co.uk](mailto:marketing@eolitservices.co.uk) and we may incorporate some of your ideas in one of our future newsletters or other e-zines.



## References

- 1) University of Glamorgan website  
<http://www.news.glam.ac.uk>  
News Centre - Discarded Hard Disk Hold Sensitive Data  
September 2007
  
- 2) The Register website  
[www.theregister.co.uk](http://www.theregister.co.uk)  
Archive – 2000 – February  
February 2000
  
- 3) Network World website  
[www.networkworld.com](http://www.networkworld.com)  
Research Centre – Security  
January 2008
  
- 4) Public Technology website  
[www.publictechnology.net](http://www.publictechnology.net)  
News - Central Government  
January 2008



**Disclaimer**

EOL IT Services makes no warranty or representation that this E-Book will meet your requirements, that it will be of satisfactory quality, that it will be fit for a particular purpose, that it will not infringe the rights of third parties, that it will be compatible with all systems, that it will be secure and that all information provided will be accurate. We make no guarantee of any specific results from the use of our Services.

No part of this E-Book is intended to constitute advice and the Content of this E-Book should not be relied upon when making any decisions or taking any action of any kind. Whilst every reasonable endeavour has been made to ensure that all information provided in this E-Book will be accurate and up to date, EOL IT Services makes no warranty or representation that this is the case. We make no guarantee of any specific results from the use of our services.

No part of this E-Book is intended to constitute a contractual offer capable of acceptance. No goods and / or services are sold through this E-Book and product and / or service details are provided for information purposes only.

Whilst every effort has been made to ensure that all graphical representations of products and / or descriptions of services available from EOL IT Services correspond to the actual products and / or services, EOL IT Services is not responsible for any variations from these descriptions.

EOL IT Services does not represent or warrant that such products and / or services will be available from us or our Premises. For this reason, please contact us prior to visiting if you wish to enquire as to the availability of any products and / or services. Any such enquiry does not give rise to any express or implied warranty that the products and / or services forming the subject matter of your enquiry will be available upon your arrival at our Premises.

