

Secure data destruction methods for electronic media

To prevent unauthorised access to data, it is important that the data must be rendered unreadable when the device on which it resides is disposed of or recycled, even within UCL. The appropriate method to use depends on the type of media. There are three main categories of media for these purposes: hard disks, CDs/DVDs and USB drives. Flash memory cards and floppy disks can be treated the same as USB drives. Techniques for destroying all data on these types of media are described below. There are also utilities for erasing individual sensitive files without wiping an entire disk.

Hard Disks

Simply deleting files from a computer's hard drive or other storage media is almost never sufficient, as 'delete' simply changes indexing information about a file and the data itself remains on the disk. Emptying the 'recycle bin' or the 'trash' folder of deleted files is also usually ineffective, as the pointers to the deleted files are removed but the data itself still remains on the storage media as unallocated space. There are many widely available programs that can restore data that has been deleted in this way. A plain "format" command is somewhat better, but a determined person could still access sensitive data.

UCL CST recommend that data should be overwritten several times using software tools prior to disposal or recycling of the media. The following free software tool satisfies UCL requirements for secure deletion:

- **Darik's Boot and Nuke (DBAN)** is a self-contained boot disk that securely wipes hard disks. It does not matter which operating system (eg: Windows, Mac OS, Linux) is on the hard disk to be wiped. To use DBAN, visit the site below, download the .iso file and burn it to CD/DVD as an image. Then boot the target machine from the CD/DVD and follow the prompts. DBAN will allow you to choose from a list of hard disks that it detects and will completely destroy the data on the drives you select. DBAN's default 'DoD short' method overwrites data 3 times and should be sufficient for all purposes. No private data recovery company claims to be able to reconstruct completely overwritten data.

<http://www.dban.org/>

CDs/DVDs

It is recommended that optical media such as CDs and DVDs are physically destroyed. Some shredders will shred CDs and DVDs but many will get stuck and the blades may get damaged, so you should check if your shredder is designed for this before attempting it. If no means of destruction is available, or for mass disposal of CDs and DVDs, contact Facilities Services on extension 37001.

USB Drives (including flash memory cards and floppy disks)

USB drives can be erased using DBAN in the same way as hard disks, but it is usually faster and more convenient to use a secure deletion utility specific to your operating system. Free or built-in products for the main operating systems are listed below. These are also recommended for erasing sensitive files from a hard disk without wiping the entire disk. An example of when this should be done is when sensitive data has been stored unencrypted on a laptop hard drive (note that it is no longer acceptable to store sensitive data unencrypted on mobile devices - see section 10 of the [UCL Data Protection Policy](#)).

• Windows

Eraser is a free file removal utility for all versions of Windows.

<http://eraser.heidi.ie/>

Once installed, Eraser adds an 'Erase' option to the right-click menu, so you can simply right-click on files or folders in Windows Explorer and select 'Erase'. If sensitive files have already been deleted in the normal way, you should run the Eraser program and use the 'Unused disk space' option on the drive in question to ensure all traces of the files are removed from the drive.

• Macintosh

Macintosh users have built-in options for secure deletion. For files you've deleted by dragging them to the Trash, use Secure Empty Trash from the Finder menu. It will overwrite and delete files in your Trash folder. For whole file systems, use the Disk Utility, which can be found in the /Applications/Utilities/ folder.

• Unix/Linux

Wipe is a secure file removal utility for Unix/Linux.

<http://wipe.sourceforge.net>

Inoperable Media

In the event that a hard disk or other device is inoperable and therefore cannot be wiped using software tools, the disk must be physically destroyed. Facilities Services should be contacted on extension 37001, and will arrange a suitable method of destruction.

05/08/2010