# University College Cork

# Guidelines on the disposal of devices containing confidential data

## Version 1


Information for the UCC community regarding the safe disposal of devices that may contain confidential information.

# Document Location

http://www.ucc.ie/en/it-policies/guidelines

# Revision History

| Date of this revision: 02/08/2013 | Date of next review: 2/08/2014 |
|---|---|

| Version Number/Revision Number | Revision Date | Summary of Changes |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |

# Consultation History

| Revision Number | Consultation Date | Names of Parties in Consultation | Summary of Changes |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

# Approval

This document requires the following approvals:

| Name | Title | Date |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |

# Guidelines on the disposal of devices containing confidential data - Technical Annexe

Data can now be found on wide variety of electronic storage data devices. These range from networked storage appliances, storage directly attached to (or contained in) desktops, laptops, pad/tablets, smartphones, through solid state storage in phones and USB drives, to more passive media such as CD and DVD. Because of the technological differences, the approach taken to sanitise the "disks" will vary according to the device type.

There is still controversy surrounding the effectiveness of magnetic microscopy to lift digital data via analogue means. This discussion does not seek to address "laboratory" attacks of this nature. (If there is data of a "top secret" nature then a combination of the techniques below combined with extreme destructive methods would probably be required. This would not be the norm in an education setting.)

## Device re-use:

**a)** The day-to-day methods for deleting files and directories and for re-formatting devices, usually do not delete the file contents but rather remove the pointers. This will deter a casual viewer but no more than that.

**b)** The next step up is to overwrite the file/disk contents themselves. There are a choice of utilities in this space.

However much of the portable media available today uses Flash (Solid State) technology. Solid State Disks (SSD) are now coming into the mainstream and replacing traditional Hard Disk Drives (HDD) in some computers. While HDDs have always hidden bad blocks and the like from the computer operating system, NAND Flash technology brings this to a whole new level. Because there is a limit to the number of rewrites in any particular block and because blocks are not updated in place, overwriting has limited effectiveness.

Additionally, overwriting usually involves multiple (typically triple) passes and tends to be very slow. While it would take a bit more work from the adversary, overwriting cannot ensure that at least some the data will be intact and readable.

**c)** Making files inaccessible using encryption is an option. This depends on the strength of the encryption and whether the encryption key is recoverable from the media. For encryption to be effective it must be applied BEFORE the disk is used to store data. For the reasons outlined in **b)** individual files cannot be safely encrypted and Flash devices will undermine retrospective encryption.

**d)** Most modern ATA disks support a built-in "secure erase" function (SE). This is both faster and more secure than repeated overwrites. This is the ideal where available. Some SCSI drives now support SE. It is now being seen more on often on SSDs (but not USB devices) too. Less well validated are the proprietary reset or clear functions provided on PDAs and the like.

### Device Destruction:

Optical media such as CDs and DVDs may not be rewritable and so shredding into suitable small pieces or melting/incinerating would be a straightforward practical approach. This approach can also be used for flash drives and SD cards.

Degaussing is a technique which uses a magnetic field to destroy the information on magnetic media (but not on optical media, of course). As a by-product, the device itself also becomes unusable.

## How to get the data wiped or the device destroyed.

UCC has contracted a third party service provider to ensure its electronic media devices are securely erased and destroyed. Details here.