# Donated computers

## Introduction

The COVID-19 pandemic has brought society's existing inequalities into sharp relief. Many pupils are living in households with severely limited access to computers and the internet either for financial reasons or because of where they live.

Over the last year, COVID-19 has meant that far more pupils being taught at home. Staff had to create online teaching resources while, at the same time, teaching the children of key workers at school. Where pupils do not have good internet access, online lessons cannot be "live" but need to be pre-recorded - which can be very time-consuming. Even where internet access is available, there are many families where access to a computer is very limited. There may only be one computer in a household of several children and working parents, for example.

These issues were partly addressed by the government in their laptop for disadvantaged pupils scheme, but there have been issues with schools' allocations, distribution and ongoing support. Charities (e.g. http://www.donatealaptop.co.uk/), business, and the BBC, with their Give-a-Laptop scheme, have also stepped in to provide computers for schools to distribute to pupils who need them.

Computers received from the Government scheme are new and can be set up in the usual manner.

Computers donated from elsewhere need to be treated more carefully. In particular, each one will need to be "cleaned" so that any personal or sensitive data is securely removed from it before a new operating system and any desired software are installed. Ideally, this will be done before reaching the school but certainly before being distributed to pupils.

This NEN guidance note addresses issues around the acceptance of donated devices.

**Where has the donation come from?**

Leaving aside new computers through the Government scheme, donations may come directly from the general public or businesses disposing of redundant computers. For example, a local business may offer a computer to a local school, or the school may invite donations from parents.

Charitable organisations have also been set up to facilitate the distribution of donated devices to schools and/or Local Authorities (LAs). The BBC have a list of organisations on their website that are able to accept donations. While some of the larger organisations will perform a full data clean and re-configuration before the donation is distributed, not all of them have the facilities to do this and rely on the donor deleting any personal information.

As a school or LA will ultimately be providing the donated computers to pupils for use at home, they have a responsibility to ensure that all sensitive data has been correctly

removed to avoid any liability. When receiving donations directly from a business or via a specialist intermediary, the expectation is that the device has been sanitised in accordance with guidance from the NCSC (National Cyber Security Centre). However, it would be prudent to have this confirmed before accepting the donation. If this assurance cannot be given, then the device will need to be sanitised and reconfigured by the recipient.

With a donation directly from the public or a local small business, it would be best to treat the device as if it has not been sanitised. In this case, the following outlines how to remove all sensitive information from the donated device.

**Data wiping**

The most valuable part of a computer is the data on the hard drive (or Solid State Drive [SSD]). For example, the computer drive may contain personal data which could be extracted and used for fraud or commercially sensitive data. Anyone donating old equipment (either privately or as a business) needs to securely remove all such data before donating it. In addition, any licensed software should be uninstalled, although this will often happen as a by-product of re-installing an operating system. Charities or schools which receive donations have a responsibility to ensure that they do not contain sensitive data before passing them to an end-user.

It is important to understand that just deleting a file (using ‘rm’, ‘del’, or emptying the trash or wastebasket) will not delete the file. These only make the file invisible to the user and mark the disk space as available for being overwritten: it DOES NOT delete the data on the disk itself. There are multiple software packages of varying levels of sophistication that can restore or view previously deleted data.

So, how do you securely delete the data?

There is a range of options depending on the type of device, operating system, and level of security required. We will consider two classes of device that may be donated: those with a mobile operating system (smartphones, tablets) and those with a desktop operating system (desktops and laptops).

**Mobile Devices**

The distinguishing feature of mobile devices is that their storage is, for all practical purposes, an integral part of the device rather than being an easily replaced element. However, data is, in most cases, automatically encrypted, so only a few relatively simple steps are required to securely "delete" it - what is actually deleted are the encryption keys which makes the data effectively unreadable.

Encryption and factory reset are generally secure enough for most devices, but it is not infallible. For iOS, "*While the basic encryption enabled by turning on passcodes protects all of the data on the device (including your apps), it can be bypassed by jailbreaking.*" (Source). So, where critical data is involved (a donation from an accounting firm, for example, then a fuller data wipe can be done by using, or example, this software. For Android devices, encryption is applied to the whole storage system and, as far as we are aware, cannot be bypassed once the keys are deleted by a factory reset.

Finally, remember to remove any SIM or microSD cards!

Erase iPad/iPhone.

Erase Android device.

**Desktops/Laptops**

Desktop and laptop computers behave the same in terms of deleting personal data, so, in this section, "computer" will cover both.

The most secure way to remove data is to remove and physically destroy the drive. For a Hard-Disk (HD), degaussing and breaking the disk platter into several pieces will destroy the data. For a Solid State Drive (SSD), breaking data chips will destroy the data.

If you do not want to destroy the drive, then other, less dramatic options do exist. But be aware that data sanitation software designed for use on a HD will not work on a SSD.

For HDs, there are essentially two non-destructive methods for making sensitive data inaccessible: secure erasure and encryption. The advantage of encryption is that it does work on both HD data and data stored on a SSD.

**Secure Erasure (Hard Disk)**

For HDs, the tried and tested method to securely erase data is to do a Data Wipe - this involves a process of writing over the actual disk area used to store the file. Various algorithms are used to make the data unrecoverable, but all involve multiple rewrites to the disk. For example, DiskWipe on a PC or the “secure erase” option in MacOS's DiskUtility can be used to securely erase a disk.

**Secure Erasure (Solid State Disk)**

Things are a bit more complicated for SSDs because of the way data is stored. This article gives quite a good explanation of how a SSD (and other flash storage) works. For the major brands, there will, in all probability, be a special utility for erasing their particular SSD (see the links in the previously quoted article). PartedMagic also includes a tool for erasing SSDs.

**Encryption**

Another method of cleansing that can be used on both HDs and SSDs is encryption. Most modern operating systems allow you to encrypt either specific files/directories or the whole disk. Once the disk has been encrypted, a factory reset or re-installing the operating system will delete the keys making the data inaccessible.

**Hardware type and Specification**

For a donated phone or tablet, once a factory reset had been done and updates applied, it is ready to be configured and loaned to a pupil.

For desktop and laptop computers, there are more options. For example, an older computer that has been build for Windows8 may run very slowly, if at all, with a standard Windows10 installation. In this case, it could be reconfigured as either a Linux system or as a Chromebook using Neverware. This has proved to be a popular way to re-purpose older PCs

in such a way that they are consistent with the school's other hardware and have access to the most up-to-date software. It can even be installed on a range of Apple computers.

The key point is that even very old computers that cannot effectively run the newest operating system versions can be re-purposed and find a new use helping pupils access education.

**A word about licensing.**

Every refurbished computer needs an operating system to work - and a license for it. This should normally be installed by the donating organisation, but if you need to do this yourself, then there a several options.

- If you want to install Windows (given the caveats on performance noted above), then some Microsoft Authorised Refurbishers will sell the required Refurbished Windows licence at a minimal cost and provide support.
- Neverware pricing for Education is currently $20/year (or $38 for a one-time fee), and the software can be downloaded from their website.
- Linux is OpenSource and comes in various flavours, which can be downloaded and installed for free.

**Intended Audience**

*Senior Management, Staff with responsibility for Safeguarding policy, Heads of IT/Computing and other technical staff.*

**Summary**

Over the last year, the need for remote learning had exposed the inequalities that exist in access to digital resources. A child's access to a suitable device may be severely limited in many households, and internet access is very far from universally available or affordable.

In an effort to address these inequalities, the government set up a scheme to supply laptops with internet access. A range of charities also donate old computers: in most cases, these donations are directed to individual schools, which then distribute them to their pupils.

Before being loaned to pupils, it is essential that existing data is deleted by data-wiping or encryption and the keys removed. Ideally, this will be done either by the donor or an intermediary, but schools need to confirm that it has been done satisfactorily and, if it hasn't, be prepared to do it themselves.

The data on Android smartphones and tablets is already encrypted, and a factory reset will delete the keys rendering the data inaccessible. For iPads and iPhones, a factory reset does the same but can be bypassed by "jailbreaking" the phone. If the data is particularly sensitive, then a third-party application may be required to guarantee that the data is inaccessible.

An old computer may not perform very well if the latest o/s is installed. In these cases, installing either Linux or Neverwear – to make it into a Chromebook - may be a better option.