**Data and IT Destruction and Disposal Guide**

V1.0

**Contents**

[Introduction 2](#_Toc90497347)

[Which devices does this apply to? 2](#_Toc90497348)

[What do you want to do with the device? 3](#_Toc90497349)

[**Device Transfer (within the school)** 3](#_Toc90497350)

[**Device Transfer (externally)** 3](#_Toc90497351)

[**Device Disposal** 4](#_Toc90497352)

[Sanitisation methods 4](#_Toc90497353)

[**NCSC Certified Data Erasure (Sanitisation) Products:** 5](#_Toc90497354)

[**PCs / Computers** 5](#_Toc90497355)

[**Smartphones and tablets** 5](#_Toc90497356)

[**Device Destruction** 6](#_Toc90497357)

[Why you need to update policies 6](#_Toc90497358)

[Annexe 1 – Device Secure Wiping and Resetting 7](#_Toc90497359)

[Annexe 2 – Data and Device Sanitisation Decision Flowchart 8](#_Toc90497360)

[Annexe 3 - Relevant Legislation 9](#_Toc90497361)

[**The Data Protection Act (DPA) 2018 and UK GDPR** 9](#_Toc90497362)

[**Waste Electrical and Electronic Equipment Recycling** 9](#_Toc90497363)

[**Waste Carrier Licences** 9](#_Toc90497364)

[Annexe 4 - Further Guidance and Support 10](#_Toc90497365)

[**The National Cyber Security Centre (NCSC)** 10](#_Toc90497366)

[**Centre for the Protection of National Infrastructure (CPNI)** 10](#_Toc90497367)

[**Asset Disposal and Information Security Alliance (ADISA)** 10](#_Toc90497368)

# **Introduction**

School and setting devices may hold a lot of sensitive information, including images and emails. Removing access to this personal information from devices to ensure data protection compliance and maintain security is essential when the schools wants to reallocate or dispose of devices which may contain personal data.

Pressing delete and sending files to the recycling bin will not remove the data, and emptying the bin won’t help either. With freely available software tools it is possible to restore everything.

This guide aims to look at the key aspects of handling reallocated, retired, and redundant devices and storage media.

# **Which devices does this apply to?**

The obvious data sources, such as the hard drive on a computer, won’t cover the memory found on devices like printers and copiers. Smaller smart devices e.g. thermostats / bulbs etc., have caches of flash media storage.

Electronic devices which need to be considered for data sanitisation include, but are not limited to:

* Hard drives – may be external or internal
* Flash memory drives / USB sticks
* Solid state devices
* Complete devices - PCs, phones, and tablets
* Digital media - CDs / DVDs / magnetic tapes
* Photocopiers and printers (often these capture images and have a memory of scanned images)

**What is Data Sanitisation?**

Data sanitisation is the process of irreversibly deleting, or destroying, data stored on a device. This means that even utilising forensic methods the data cannot be recovered.

Deleting data from a device is not enough to meet the requirements of the DPA 2018/UK GDPR. All devices, whether they are transferred to a new user, new owner or disposed of, should be subject to data sanitisation.

Before you sanitise or destroy your devices, back up any information on the device that you want to retain. Users should be reminded to sign out of all accounts. Some accounts will prevent another log on if other device IPs are registered as being logged on. It is also advisable to unpair your computer from external Bluetooth devices like mice and keyboards.

# **What do you want to do with the device?**

The need for sanitisation and the type of action taken will depend on what the ultimate intentions for the device are:

**Re-use:** When devices are to be repurposed and allocated to a different user.

**Repair:**  You may need to return a faulty device to the vendor for repair or replacement, giving them access to anything stored on the device.

**Disposal:**  Donating old devices to charities or re-selling unwanted equipment.

**Destruction:** On site, if appropriate, or may be carried out by licensed third-parties.

## **Device Transfer (within the school)**

Often, as newer devices are purchased, existing devices may be reallocated to other staff. If the original system owner and the new recipient have the same access, it may not be necessary to fully reset devices, but there may be saved user profiles and credentials which need wiping.

Transfers of devices between teachers, teaching assistants, headteachers, or business officers/managers can lead to data breaches if the levels of access previously assigned and existing profiles are retained.

Factory resets may be appropriate (see Annexe 1)

## **Device Transfer (externally)**

If you are transferring to another school or donating devices (including donating to the PTA for sale\*) all [data](https://dataclass.stanford.edu/) stored on the device must be sanitised unless there is a documented justification for not doing so.

 *\* This needs to be handled carefully.*

Revoke all certificates / licences associated with the school and not pertaining directly to the device. Microsoft offers a device-based CAL (Device CAL) or a user-based CAL check licences, including those for operating systems.

Transfer of ownership forms should also be completed.

## **Device Disposal**

If a device is to be disposed of or transferred to a party outside of the setting/school, data must be sanitised.

This may involve physically destroying all device storage according to the NCSC guidelines. Most schools will use a third-party company for this process and will need to carry out appropriate due diligence. This means that you need to carry out checks on the suitability of providers. This guidance should help you to identify what you should look for in third-party companies.

As a minimum, it is recommended that companies are ISO 27001 / ISO 9001 certified and also certified by a suitable accreditation scheme, such as ADISA: [Search for a Certified Company (adisa.global)](https://adisa.global/search-for-a-certified-company/).

The Information Commissioner’s Office (ICO) have ‘Certified’ the ADISA Asset Recovery Standard as achieving suitable data protection standards for the organisations performing these services. ASISA certified providers offer some reassurance that you are using an appropriate provider.

Disposal companies need to hold a current, valid waste carrier licence, suitable insurance, and confirm their compliance with WEEE regulations. (see Annexe 2)

You should also ask the company what sanitisation method they use- see below.

# **Sanitisation methods**

Deleted data may appear to have been removed, but data remains on the storage media after a delete or format command is executed. Even emptying the recycle bin will not permanently erase the data.

1. **Secure erasure**

This is a set of commands in the firmware of most computer hard drives. If you select a program that runs the secure erase command set, it will erase the data by overwriting all areas of the hard drive.

1. **Disk wiping**

This is a utility that erases sensitive information on hard drives and securely wipes flash drives and secure digital cards.

1. **Overwriting**

Using random data instead of easily identifiable patterns makes it harder for attackers to discover the original data and so overwriting data with a string of 0s and 1s is another method of sanitisation.

Users should overwrite the entire hard disk and add multiple layers of new data (three to seven passes of new binary data) to prevent attackers from obtaining the original data.

Cipher.exe is a built-in command-line tool in Microsoft Windows operating systems that can be used to encrypt or decrypt data on New Technology File System drives. This tool also securely deletes data by overwriting it.

Use a disk cleaning software designed to permanently remove the data stored on a computer hard drive to prevent the possibility of recovery.

## **NCSC Certified Data Erasure (Sanitisation) Products:**

[Blanco Drive Eraser](https://www.ncsc.gov.uk/products/blancco-drive-eraser-6)

[YouWipe Data Erasure Tool (DET)](https://www.ncsc.gov.uk/products/youwipe-data-erasure-tool)

[WhiteCanyon WipeDrive 9.3.0.](https://www.ncsc.gov.uk/products/whitecanyon-wipedrive-9-3-0-cpa-configured)

## **Windows Computers**

**Using the Windows ‘Reset this PC’ or a clean Windows install will not necessarily delete all user data files. The resetting process allows for ‘resetting to default settings’ whilst still keeping data.**

**Common data recovery programs can also recover data from recently formatted drives.**

**Windows PC’s should be wiped before the Operating System is reloaded.**

## **Mac Computers**

**The Mac start-up disk also has two volumes, the read-only system one is separate to the read-write volume used for data. Reinstallation of the operating system will not delete the data.**

To securely erase free disk space formerly hosting sensitive information, Mac users should open Applications > Utilities > double-click Disk Utility.

Select the data volume then click the **Erase tab**.

**To ensure permanent secure destruction**

**Either overwrite the drives *(see above)* or for** PCs with a magnetic drive (PATA / SATA / SCSI) degauss. Solid-state (SSD) and Fusion drives will require physical destruction.

## **Smartphones and tablets**

Ensure that all data is removed from your device by performing a hard reset and returning it to factory settings (see Annexe 1)

In addition, physically remove any SIM cards and memory cards if your device has them.

**Digital cameras and media players**

Perform a standard factory reset, usually by a reset button on the device. Physically remove the hard drive or memory card.

**Photocopiers, printers, fax machines, and multifunction devices**

Remove any memory cards from the equipment. Perform a full manufacture reset to restore the equipment to its factory default. Refer to the manufacturer’s guidelines. If your devices are leased, check that data erasure obligations and data sanitisation are in your contract and what the terms of these are. You may be obliged to pay a fee to have the data wiped. You should consider this obligation at the start of any contractual relationship.

##

## **Device Destruction**

Physical destruction of a device is the most obvious way of preventing others from retrieving your information. These services are usually carried out at a specialised licenced facility that can disintegrate, burn, melt, or shred your computer drive and other devices. The destruction of data storage by crushing, shredding, or disintegration is called solid-state destruction.

It is not recommended that school staff attempt to physical destroy hard drives and devices in-house. Driving nails or drilling holes into the device will not achieve the recommended maximum size of 0.2mm for the pieces left behind and may still lead to data reconstruction.

Solid state drives require physical destruction with devices that are specifically engineered for this purpose.

CDs and DVDs can be destroyed by a shredder designed for this purpose (this is often on a label near the shredder teeth) or by incineration\*. There are also hardware devices available that erase CDs and DVDs by destroying their surface.

*\*Incineration requires a high degree of heat and may give rise to noxious fumes. This should not be attempted in-house.*

**Magnetic media degaussers** expose devices to strong magnetic fields that remove the data that is magnetically stored on traditional magnetic media. Once the media is degaussed, it can no longer be used. This method is suitable for tapes, floppy discs, and some hard drives (Solid state drives are not magnetic).

# **Why you need to update policies**

If expectations are not covered in school policy, then the liability for data loss will rest with the school for a lack of organisational measures.

Ensure that a data destruction policy exists which aligns with your data retention policy. It may be that one policy will cover both aspects, but policy should cover the expected controls for the sanitisation and disposal of data and equipment.

Implementing a data destruction policy is critical to ensuring that, regardless of whether information is in hardcopy or electronic form, it is safely and securely disposed of at the end of the lifecycle.

Don’t forget any CCTV equipment, and ensure data in cloud systems is also covered.

| **Device type** | **Recommended secure wipe** | **Recommended secure remote wipe** |
| --- | --- | --- |
| Android | [Erase all data (factory reset)](https://support.google.com/android/answer/6088915?hl=en)Select: **Settings > General > Reset > Erase All Content and Settings** menu. | [Android remote erase](https://support.google.com/accounts/answer/6160491?hl=en) or [MDM](https://www.ncsc.gov.uk/collection/device-security-guidance/getting-ready/mobile-device-management) |
| Chrome OS | [Reset to Factory Settings](https://support.google.com/chromebook/answer/183084?hl=en-GB) | [MDM](https://www.ncsc.gov.uk/collection/device-security-guidance/getting-ready/mobile-device-management) |
| iOS(Including iPhones and iPads) | [Erase all content and settings](https://support.apple.com/en-gb/HT201274)Select: **Settings > General > Reset > Erase All Content and Settings** menu.This will render all user data on the device cryptographically inaccessible.  | [Find my iPhone](https://support.apple.com/en-gb/HT201472) or [MDM](https://www.ncsc.gov.uk/collection/device-security-guidance/getting-ready/mobile-device-management) |
| macOS | [Manually erase your hard disk](https://support.apple.com/en-gb/HT208496), choosing the ***Secure erase*** option | [Find my iPhone](https://support.apple.com/en-gb/HT201472) or [MDM](https://www.ncsc.gov.uk/collection/device-security-guidance/getting-ready/mobile-device-management) |
| Windows | [Reset your PC](https://support.microsoft.com/en-gb/help/12415#section3), choosing the *Remove everything* option | Use [MDM](https://www.ncsc.gov.uk/collection/device-security-guidance/getting-ready/mobile-device-management) if using MDM-managed Windows |
| Windows Phone | [Reset your phone](https://support.microsoft.com/en-us/windows/reset-my-phone-04717aab-b858-8b37-523e-39143a6764d6) In the App list, tap Settings (gear/cog) iconTap **About**, and then tap **Reset your phone**. Reply **Yes** when the warnings appear. |  |

# **Annexe 1 – Device Secure Wiping and Resetting**

NCSC - Factory Resetting [Erasing devices - NCSC.GOV.UK](https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/erasing-devices)

# **Annexe 2 – Data and Device Sanitisation Decision Flowchart**

This flowchart is taken directly from NIST Guidelines for Media Sanitation – [full guidance available here.](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf)



# **Annexe 3 - Relevant Legislation**

## **The Data Protection Act (DPA) 2018 and UK GDPR**

A significant part of the data retained and processed by schools in personal information. Legislation covers all personal data, whether it is in hard copy or in electronic form, such as saved ‘in the cloud’, saved to a hard drive, sent in an email, or accessed via a smart phone.

Failure to safely dispose of personal data can lead to investigation and subsequent fines from the ICO.

There are no specific requirements around sanitisation in the UK GDPR or Data Protection Act, but legislation does state that an organisation must have suitable ‘technical and organisational methods’ to ensure that data is processed properly. The GDPR states that using a provider that is certified by the ICO is a good way to demonstrate compliance with the obligations under the UK GDPR.

**Waste Electrical and Electronic Equipment Recycling** [(WEEE) Regulations](https://www.hse.gov.uk/waste/waste-electrical.htm)

The Waste Electric and Electronic Equipment (WEEE) Regulations 2013 ([the Regulations](http://www.legislation.gov.uk/uksi/2013/3113/contents/made)) cover the requirements  for the recovery, reuse, recycling, and treatment of WEEE.

Further information on the WEEE Regulations 2013 can be found in the [Government Guidance Notes (PDF)](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/292632/bis-14-604-weee-regulations-2013-government-guidance-notes.pdf) produced by the Department for Innovation and Skills.

## **Waste Carrier Licences**

Department for Environmental Food and Rural Affairs (DEFRA) allow schools to search the register of licensed waste disposal carriers. If a third-party is collecting / transporting waste on behalf of the school, then they need to be included on [the register.](https://environment.data.gov.uk/public-register/view/search-waste-carriers-brokers)

# **Annexe 4 - Further Guidance and Support**

**The National Cyber Security Centre (NCSC)**

The NCSC has best practice guidance of secure methods of data sanitisation is available via their website:

Disposal guidance: <https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media>

Disposing of network devices: [Acquiring, managing, and disposing of network devices](https://www.ncsc.gov.uk/guidance/acquiring-managing-and-disposing-network-devices)

**Centre for the Protection of National Infrastructure (CPNI)**

[The Centre for the Protection of National Infrastructure (CPNI),](https://www.cpni.gov.uk/) sets the standard in the process of physical data destruction in the UK. The CPNI provides guidance on physical security, personnel security, and cybersecurity.

**Asset Disposal and Information Security Alliance** (ADISA)

[ADISA](http://adisa.global/) is a group of experts in IT asset disposal services. They have developed a standard that ensures data is managed throughout its lifecycle, and that personal data has been handled appropriately when IT equipment is re-used or destroyed.

Accreditation by ADISA confirms that an organisation is fully compliant with the accepted best practices of IT asset disposal and data destruction.

ADISA standards are ICO certified and their website allows you to check which disposal services / companies meet [the standards.](https://adisa.global/download-the-standard/)

**Higher level additional schemes referenced in NCSC guidance may not be as appropriate for schools procuring services, but are, nevertheless, secure:**

[Assured Service (Sanitisation) scheme (CAS(S))](https://www.ncsc.gov.uk/information/commodity-information-assurance-services): A scheme which the NCSC offers for companies wishing to provide sanitisation services to owners of highly classified Government data.

CAS-S accreditation confirms that the company in question is able to provide the highest possible levels of data destruction and sanitisation, officially graded as ‘secret’ by the UK government.

[CPNI's Secure Destruction of Sensitive Items](https://www.cpni.gov.uk/secure-destruction-0): A standard which CPNI applies to destruction companies which serve the Critical National Infrastructure (CNI). It majors on procedural and personnel safeguards.