Secure sanitisation and disposal of storage media

How to ensure data cannot be recovered from electronic storage media.

This guidance is for organisations who need to ensure that data held on electronic storage media can't be read by unauthorised parties after it has left organisational control.

It will help organisations to protect data from being read by standard users with access to commercially available data-recovery tools, or by using forensic services. This is based on the protections proportionate for OFFICIAL data, as described in the Government Security Classifications Policy's threat model.

> **Note**: This guidance will **not** protect data from being read by a skilled, well-funded laboratory.
>
> - If media has stored data with an HMG security classification of SECRET or above, separate guidance should be followed, which is available from your normal NCSC point of contact (PoC).
> - Media that has been used for OFFICIAL data should **not** be re-used to store data of SECRET or above, even after sanitisation processes have been followed.

What is electronic storage media?

This guidance defines electronic storage media (ESM) as 'data storage that requires electrical power to be read from and written to'. This includes media such as:

- hard disk drives (HDDs)
- solid state drives (SSDs)
- memory chips (such as SRAM, DRAM)

- flash-based media (such as USB drives and SD/microSD cards)
- magnetic media (such as tape and floppy disks)
- optical media (such as CDs, DVDs and Blu-rays)

Practically every electronic item now contains some form of ESM. A non-smart device may only have a small amount of memory as it buffers data that passes through it, whilst a laptop or server may contain several terabytes (TB) of data.

All connected devices, all computers and smartphones, 'internet of things' (IoT) devices, routers and switches, many peripherals (such as monitors, memory sticks and memory cards) whether in your network or in industrial control systems will contain ESM.

It is not easy to identify electronic devices that categorically contain no ESM, or to identify what *type* of ESM a device contains. There have even been examples where several gigabytes of sensitive documents have been retrieved from decommissioned photocopiers and printers. For these reasons:

- this guidance treats all types of ESM in the same way
- any device that you consider *might* contain ESM should be sanitised

The types of electronic equipment that are unlikely to contain any ESM may include power supply units and transformers, fans, simple headphones, mice, and antennae. Before sale or disposal of these items, remove all labels or markings that indicate ownership of the device.

What is sanitisation?

Sanitisation is the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction. Any media that has stored data which is sensitive to your business should be sanitised before the device leaves organisational control. Simply hitting the 'Delete' key isn't enough.

Some forms of sanitisation will allow you to re-use the media, while others are destructive in nature and render the media unusable.

When to sanitise media

There are a number of situations when you will need to sanitise storage media:

- **Re-use:** if you want to allocate a device to a different user, or repurpose equipment within your organisation.
- **Sell:** you might want to sell (or donate) equipment that no longer meets your organisation's needs.
- **Repair:** you may need to return a faulty device to the vendor for repair or replacement.
- **Disposal:** you may want to sanitise media that's no longer required by your organisation, especially if you have limited confidence in third parties that provide sanitisation services.

The risks of not sanitising

If media is not sanitised, sensitive data may remain on it. This could result in the following problems for your business if media is lost or stolen:

- critical data could be recovered and used by adversaries or competitors
- private or personal data about your customers or staff could be used to commit fraud or identity theft
- your intellectual property could be recovered and published openly, leading to loss of reputation and revenue
- personal information could be leaked, breaching GDPR

Before you sanitise

In all cases, the media containing your sensitive data will be outside its normal operating environment and is therefore subject to greater risk from a different set of users, from third parties, or from less-trusted organisations and individuals. In order to decide the best approach, you will need to:

- Understand your data, its value to you, and its potential value outside your organisation. The NCSC's guidance on Asset Management can help you to this.
- Know which of your assets contain (or should be assumed to contain) ESM and which of those assets have handled data of value to your organisation.
- Record the life cycle of your ESM (that is, what is it being used to store, where, and for how long).
- Have a re-use and disposals policy in place, with key roles understood by everyone in your business. We've included a sample policy at the end of this document.
- Ensure that you understand the eventual sanitisation requirements as part of your purchasing decisions.
- Ensure you have the manufacturer's documentation to hand so you know how to sanitise your media when you need to.

Preparing ESM for re-use

When preparing devices for re-deployment (or when returning a device for repair or replacement, or selling a device), then the required procedure will depend on the presence of encryption.

For devices with encryption

For devices with an encryption option (such as BitLocker on Windows and FileVault on macOS), the manufacturer normally provides a 'factory reset' which deletes the encryption keys, making the data unreadable. Once this has been done, the device can be re-used or released outside the organisation (that is, sold or donated) with minimal risk to sensitive data.

All devices operate differently, so using these reset procedures cannot *guarantee* that all user data has been rendered unreadable. However for most devices, a 'factory reset' will provide a satisfactory level of assurance. Refer to the manufacturer's support site for detailed instructions on how to do this. Note that the NCSC also has separate guidance on the secure removal of data or malware from smartphones, tablets, laptops and desktop PCs.

For devices without encryption

For devices that **don't** use encryption, then the steps below should be followed. Commercial tools are available which can perform and verify the overwrite (and also check the metadata) for a number of types of ESM. It is particularly important that these steps are followed for devices that contain multiple types of ESM, such as hybrid drives or laptops.

1. Overwrite the entire user accessible memory space with a fixed data value, such as all zeros. In some cases manufacturers may provide instructions or tools to aid in this (for example, ATA or NVMe Sanitize commands).
2. Check the device metadata for information on remapping and bad sectors. If this information shows either remapping has taken place or bad sectors are present, then there is the possibility that data may remain on the device.
3. Power-off the device fully for a period of at least 15 minutes. This includes removing any batteries where practical. If batteries can't be removed, then there is the possibility that data may remain on the device.
4. The entire contents of user accessible memory should be read back, to verify that they do contain the fixed value that was written in the first step. If this verification fails, then there is the possibility that data may remain on the device.

For devices where data may remain

If the above steps could not be completed, or if there's no manufacturer-provided reset, it may not be possible to access all memory space in the device. This means that there is a residual risk that a skilled, well-funded data recovery laboratory could recover any data that persists on the device. In many cases this may not be a concern, however a risk owner needs to be comfortable with this.

Where the data needs to be protected to level higher than OFFICIAL, the data owner may choose to implement additional protections, for example not allowing re-use in an environment where the loss of PERSONAL (or other especially sensitive data) is more likely.

Disposing of ESM

For most devices and environments, the steps for **re-use** will also provide sufficient sanitisation prior to ESM being disposed. However, these steps may not be sufficient:

- where data may remain on the device (see above)
- if the device has stored more sensitive data (such as personally identifiable information, or data that has had additional handling caveats applied)
- if a heightened risk is present for another reason

In these circumstances the means of **accessing** the data should be removed. This is achieved by physically destroying the media to particles of 6mm or less. It is important that the resulting particle size is verified after destruction. Note that in these scenarios, the data should still be erased (in the same fashion as the re-use steps above) **prior** to destruction.

Commercially available shredders and grinders can destroy media, and there are also commercial sanitisation and destruction service providers. The NCSC run the Sanitisation Assurance (CAS-S) scheme for companies wishing to provide sanitisation services to central government (HMG) customers.

Degaussing can also be used to sanitise exclusively magnetic media, although it is important that a user understands that degaussers have specific strengths, so they must check that their degausser has sufficient capabilities to remove all data from the device. For example, not all degaussers work on all hard disk drive technologies.

For more information on secure destruction, refer to the National Protective Security Authority (NPSA) guidance.

Sample re-use and disposal policy

The following considerations can be used to shape your policy regarding the disposal of storage media:

- Do you understand the risks to your organisation if the equipment it uses is not appropriately sanitised before it is re-used or disposed of?
- Are there policy constraints around the donation or re-sale of certain equipment?
- Have you considered your obligations to comply with environmental policy (for example WEEE)?

- At the time of procurement, do you know how sanitisation will practically be achieved, and its impact on whole-life costs?
- Do your staff have the skills to dismantle some equipment onsite, to minimise how much waste must be sent for destruction rather than recycling?
- Do your staff have the skills to perform sanitisation on some types of equipment? Is this more cost effective than using a third party destruction provider?
- Are there available disposal companies that hold recognised certifications or work to recognised standards (such as CAS-S or ADISA Certification)?
- How much physical storage space do you have to store end-of-life equipment, and what are the security arrangements around storage? How long do you need to store end-of-life equipment before accumulating a volume which is economically viable to dispose of?
- Do you have any data held by third parties, for example in the cloud? You should always seek assurance from these third parties that your data will continue to be adequately protected from unauthorised users after a contract expires (that is, until remnants of the data are eventually overwritten or ESM is disposed of).

PUBLISHED

23 September 2016

REVIEWED

5 February 2025

VERSION

2.0

WRITTEN FOR

Small & medium sized organisations

Large organisations

Public sector

Cyber security professionals