

IT Asset Disposal and Data Destruction Record

Record of IT equipment leaving service: each item and serial number, how its data was erased or destroyed, verification, waste transfer and signed certificate.

1. Job details

Who authorised the work and where it is being done.

Project

Filled in from the project in SiteSurvey.

Certificate or job reference

Customer

Site *

Site address

Date *

Technician

Who at the customer authorised the disposal? *

Why is the equipment leaving service? (choose one)

- ☐ Reuse inside the organisation
- ☐ Sale or donation
- ☐ Return to a leasing company
- ☐ Return for repair
- ☐ End of life

The NCSC says storage media should be sanitised when it is reused, sold or donated, sent for repair, or disposed of. Otherwise sensitive data may remain on it.

Where is the data being erased or destroyed? * (choose one)

- ☐ On the customer's site ☐ At our premises ☐ At another company's premises

Name of the company (if applicable)

How is the equipment being moved, and by whom? (if applicable)

2. Items

One entry for each device or drive. Photograph the serial number label.

Clear, purge, destroy. NIST SP 800-88 Revision 2 (September 2025) describes three levels: clear (overwriting through the normal interface), purge (techniques that make recovery infeasible even in a laboratory, such as cryptographic erase) and destroy (the media cannot be used again). Choose the level to suit how sensitive the data is.

Items (copy this block for each one)

Type * (choose one)

- ☐ Laptop
- ☐ Desktop
- ☐ Server
- ☐ Hard disk drive
- ☐ Solid state drive
- ☐ Phone or tablet
- ☐ Backup tape
- ☐ Printer or copier with storage
- ☐ Network device
- ☐ USB stick or memory card
- ☐ Other: _____

Make and model

Serial number *

Asset tag

Was the storage encrypted in use?

- ☐ Yes ☐ No

Method * (choose one)

- ☐ Overwrite
- ☐ Cryptographic erase
- ☐ Secure erase command built into the drive
- ☐ Factory reset of an encrypted device
- ☐ Degauss
- ☐ Shred
- ☐ Crush or punch
- ☐ Other: _____

If applicable: Degaussing does not erase solid state or flash storage, which is not magnetic. Use a purge method the maker supports, or destroy it.

Software or tool and version (if applicable)

Verification * (choose one)

- ☐ Verified: passed ☐ Verification failed ☐ Not verified

If applicable: Do not release this item. Repeat with another method or destroy the media, and record what you did.

What happens to it next? (choose one)

- ☐ Reuse by the customer
- ☐ Resale or donation
- ☐ Returned to the leasing company
- ☐ Recycling as waste
- ☐ Returned to the customer

Photos: serial label, and the media after destruction (photos: attach, or note the file names)

Items recorded (worked out automatically in the app)

Verified (worked out automatically in the app)

Failed verification (worked out automatically in the app)

3. Waste and recycling

For anything leaving as waste.

Is any equipment leaving as waste?

☐ Yes ☐ No

Waste carrier (if applicable)

Waste carrier registration number (if applicable)

Waste transfer note reference (if applicable)

If applicable: Waste transfer notes. GOV.UK says each load of non-hazardous waste that leaves a business needs a waste transfer note or a document with the same information, and both businesses must keep a copy for 2 years. Some equipment counts as hazardous waste, which has its own consignment note rules: check with the carrier.

4. Certificate

The signed statement the customer keeps.

I confirm that the data on the items listed in this record was erased or destroyed by the methods shown, and that the result for each item is as recorded.

Technician name

Technician signature

Witnessed for the customer by

Position

Witness signature