BRIEFING NOTE · NON-TECHNICAL

Wiping laptops properly, and proving that we did

What the certification requirement actually asks for, what it costs, and what we need to put in place.

The requirement: evidence that data wiping is carried out securely in accordance with IEEE 2883 or NIST SP 800-88.
Applies to: every machine leaving our hands, whether sold, exchanged, donated or recycled.
Short answer: achievable. A day or two of setup, modest cost, and a written routine that everyone follows.
Prepared: September 2026

01 The problem in one paragraph

Deleting a file does not remove it. Neither does emptying the recycle bin, formatting the drive, or reinstalling Windows. All of these mark the space as available for reuse while leaving the actual data in place, where free software can recover it. If we pass a laptop on that way, we are handing the previous owner's files to a stranger.

The standards exist to close that gap. They require us to use a method that genuinely destroys the data, to pick the right method for the type of drive, and to keep a record for every single machine.

> **WHY THIS MATTERS TO US**
>
> A laptop passed on with recoverable personal data still on it is a personal data breach. It makes no difference whether it was sold, exchanged or given away. It is reportable to the Information Commissioner's Office, and it would damage the relationships that our supply of machines depends on. The whole point of the exercise is to make that outcome impossible rather than unlikely.

02 The two standards, and how they fit together

The requirement names two standards. They are not alternatives. They do different jobs and modern practice uses both.

NIST SP 800-88r2

The programme

Who is responsible
Which method we approve
What records we keep
How we prove it happened

Published 26 September 2025

defers to

IEEE 2883-2022

The technique

What to do to a hard disk
What to do to an SSD
What to do to an NVMe drive
How to confirm it worked

Published August 2022

Revision 2 of the NIST guidance deliberately dropped the step-by-step technical instructions that Revision 1 contained, and points to IEEE 2883 for them instead. That is why a policy citing only one of the two now looks incomplete.

DO NOT CITE THE OLD VERSION

NIST withdrew Revision 1 on the day Revision 2 was published. Any policy, application form or supplier questionnaire still referring to **SP 800-88 Rev. 1** is pointing at a withdrawn document. Ours should say **Rev. 2** and should name IEEE 2883 alongside it.

Three levels of erasure

Both standards use the same three levels. For any machine that will leave our hands and go to someone else, we use the middle one.

Clear

Basic overwrite of the space the system can see.

Stops everyday recovery software.

Not enough for handover

Purge

Uses the drive's own built-in erase commands.

Defeats laboratory recovery. Drive stays usable.

This is what we use

Destroy

Physically shred or destroy the drive.

Nothing recoverable, but nothing reusable either.

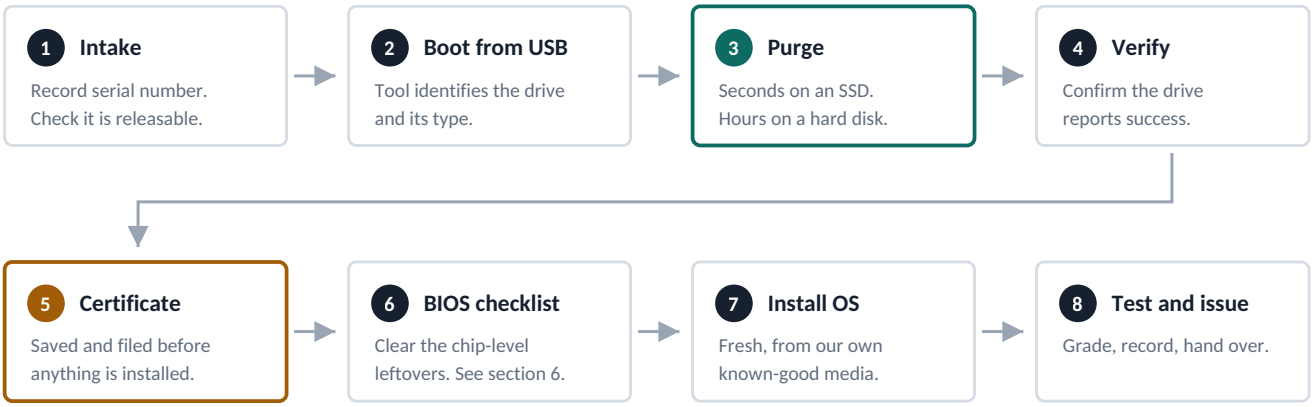
For drives that fail

Any drive that reports a failed erase goes down the Destroy route instead, with its own written record. That exception needs to be in the policy.

03 What the tool is, and how it is used

This is the part that surprises people. Erasure tools are not programs we install into Windows. They are small operating systems that live on a USB stick.

We start the laptop from the stick instead of from its own hard drive. That is necessary because a drive cannot erase itself while the machine is running from it. The tool takes over the machine, erases the drive, writes a certificate, and we then install a fresh operating system.



Handy sanity check: after step 3 the laptop should refuse to start. If it still boots into Windows, it was not purged.

04 Why the choice of tool matters

Different kinds of drive need completely different erasure methods, and this is where an inexperienced operator can go wrong without ever knowing it.

Older laptop: spinning hard disk

Writing over the whole surface reaches everything. This works.

All of it overwritten — nothing left behind

Newer laptop: solid-state drive

The same overwrite method cannot reach the drive's hidden spare area.

Overwritten

Data survives here

Reserved spare capacity, invisible to the tool

Solid-state drives constantly shuffle data between cells and keep a pool of reserve capacity that the operating system cannot address. An overwrite never touches it. The fix is to send the drive its own built-in erase command, which the controller runs internally across the whole chip. This is the single most common audit failure in our sector.

> **THE PRACTICAL CONSEQUENCE**
>
> Run the wrong method on a modern laptop and the screen still says **complete**, the drive still looks empty, and some of the previous owner's data is still recoverable. Nothing warns you. This is the reason to care about which tool we buy.

05 Choosing a tool

All three options below can produce a compliant Purge and a certificate. They differ in how much technical judgement they demand from whoever is at the bench.

OPTION	COST	SKILL NEEDED	IN PRACTICE
ShredOS free, open source	Free	**High** command line	Excellent for older spinning hard disks and produces a detailed PDF certificate. Its own documentation states plainly that it cannot fully sanitise solid-state drives, so those must be done separately using typed commands. Two processes to maintain, and real scope for error.
Parted Magic small commercial tool	Low tens of pounds	**Medium** menus, some judgement	A graphical desktop covering hard disks, SSDs, NVMe and eMMC, with a signed PDF certificate per erase. Licence covers unlimited drives. The operator still chooses the method from a menu, so they need to understand the difference. Good value if one trained person does the work.
Blancco and comparable products	Per device quote needed	**Low** largely automatic	Detects the drive type and selects the correct method itself, so the operator cannot pick the wrong one. Independently validated, and certificates are signed and filed centrally without anyone remembering to save them. The safe option if volunteers rotate.

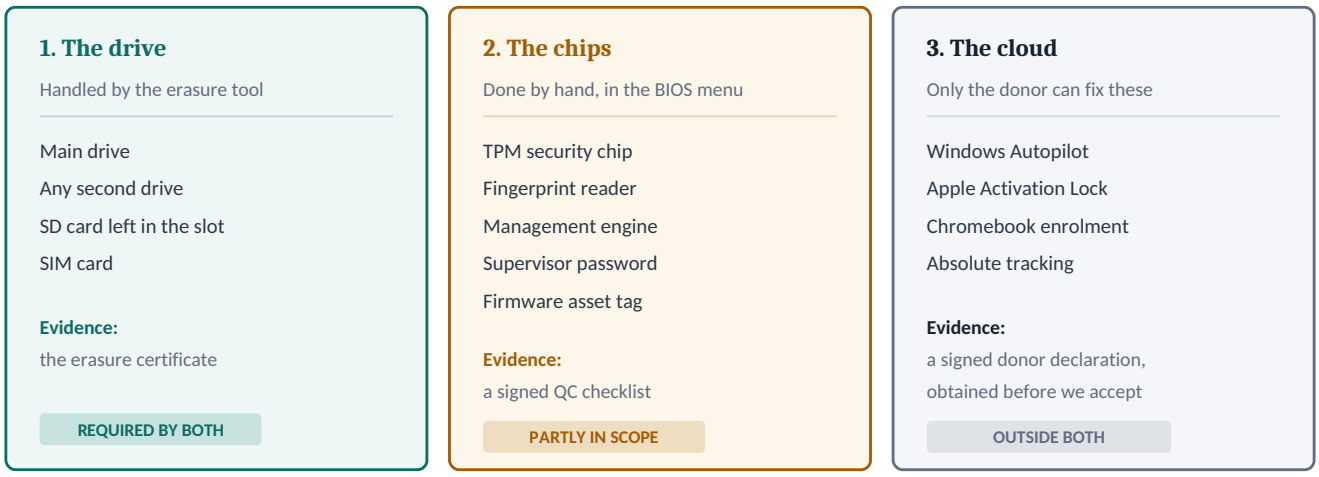
RECOMMENDATION

Blancco, or an equivalent validated product, if the budget allows. The argument is not that the cheaper tools are broken. It is that they let a well-meaning volunteer do the wrong thing while everything on screen looks correct. Paying removes that failure mode, produces certificates automatically, and gives us a third party's validation to point at when we are assessed. At a few pounds per machine against the cost of a single breach, it is a reasonable insurance premium. Ask about charity pricing.

A sensible fallback: start on Parted Magic while volumes are low and one trained person handles every machine, then move to a validated tool as soon as the work is shared out.

06 The parts a drive wipe does not reach

Erasing the drive is most of the job, not all of it. A laptop holds data in a few other places, and it can also stay tied to the previous owner in ways no wiping tool can undo.



Splitting the work into three like this is worth doing in the written policy. It shows an assessor that we understand where our control ends, which is a governance point the NIST guidance cares about. Only the first column is squarely a standards requirement — see section 07.

Two explanations that tend to land

The TPM. A small chip that acts as a built-in safe for passwords and encryption keys. Erasing the drive empties the filing cabinet but leaves the safe standing in the corner, still locked, still full. It has to be cleared separately.

Cloud enrolment. Some business laptops are registered to their old company's IT system. Wiping the drive changes nothing. The moment the machine connects to the internet it re-registers itself to them, rather like a phone still locked to a stranger's iCloud account. Only they can release it, so we have to ask before we take the machines.

> **MACHINES HANDED IN BY THE PUBLIC NEED A DIFFERENT INTAKE**
>
> The declaration route works when a business donates a batch: we ask their IT team to release the devices before we accept them. It does not work when an individual walks in with their own laptop. There is no IT team to ask, and people frequently cannot remember the password.
>
> For those machines the checks have to happen at the counter, while the person is still standing there: sign out of the Apple, Microsoft or Google account, remove any BitLocker or firmware password, and confirm they have taken a copy of anything they want to keep. Anything we cannot unlock at that point cannot be refurbished, and the intake form should say so plainly rather than leaving it to a conversation later.

> **RESETTING THE BIOS DOES NOT DO THIS FOR YOU**
>
> "Load setup defaults" resets ordinary configuration. It deliberately leaves the security items alone, because anything designed to stop a thief has to survive a reset too. Of the checks in the bench list below, it clears roughly one. Removing the small round battery does not help either. Modern laptops keep all of this in permanent storage.

Bench checklist, per laptop

Two or three minutes in the settings menu, while we are in there anyway to set the boot order. The tags show which items the standards actually call for — see section 07.

- [ ] Supervisor or BIOS password removed — if it is set and we do not have it, we cannot do any of the rest — EXTRA
- [ ] TPM cleared — STANDARD
- [ ] Fingerprint data cleared — GREY AREA
- [ ] Management engine unconfigured — business machines only — EXTRA
- [ ] Absolute tracking shows Disabled — EXTRA
- [ ] Secure Boot factory keys restored — EXTRA
- [ ] Old boot entries removed — EXTRA
- [ ] Firmware asset tag and owner name blanked — EXTRA
- [ ] Second drive checked for physically — do not trust the on-screen list — STANDARD
- [ ] SD card slot empty, SIM removed — STANDARD
- [ ] Asset stickers and property labels removed — EXTRA

07 What the standards require, and what we are adding

Not everything in this note is compliance. An assessor is checking us against NIST SP 800-88r2 and IEEE 2883, and a good deal of what follows sits outside both. It is still worth doing, but for different reasons, and we should not present it as though the standards demanded it.

This matters in two directions. If we run short of time, the first group is the part that cannot slip. And if an assessor asks why we do something, we should be able to say honestly whether it is a requirement or a decision we made.

Required by the standards

- The Clear, Purge and Destroy levels, and choosing the right one
- Matching the method to the type of drive, and not overwriting solid-state media
- Verifying the result on every machine, not just issuing the command
- A record of sanitisation per device, carrying the fields the guidance sets out
- A written policy with named roles, approved methods and decision criteria
- Destroying any drive that fails, and recording that separately
- Covering every piece of storage in the machine: second drives, SD cards, SIMs, soldered flash
- Sanitising encryption keys wherever we rely on cryptographic erase, which is what brings the TPM into scope

In scope, but no method given

The guidance is clear that the whole device has to be considered rather than just the obvious drive, but it stops short of telling us how to handle these, because no general method exists.

- Clearing the TPM beyond key sanitisation
- The fingerprint reader's secure element, which holds biometric data on the sensor rather than on the drive
- Other firmware-resident storage on the mainboard

Why the fingerprint reader in particular. This is the one people query, so it is worth spelling out. The templates sit in permanent storage on the sensor and survive a drive wipe, and biometric data is special category under UK GDPR, so the case for covering it is strong. But IEEE 2883 is built around storage interfaces — SATA, NVMe, eMMC and so on — and a fingerprint sensor is not a storage device on any of them, so no erase command exists for it. Nor can we verify the result. We select "clear fingerprint data" in the settings menu and trust the firmware, with no way to read back and confirm. A framework built on evidence has nowhere to file that. Worth knowing too that some models keep the templates on the main drive or in the TPM instead, in which case the drive wipe and TPM clear have already dealt with it.

Our position: follow the manufacturer's own instructions and record what we did. That is a defensible answer and it is the one the standards point us towards. If we would rather be conservative, treating these as required costs one menu item per machine and no assessor has ever criticised an organisation for exceeding the standard.

Outside both standards

None of the following is data sanitisation. We do it anyway, for the reasons given.

- **Removing the supervisor or BIOS password.** Not a sanitisation step, but without it we cannot reach the menus to perform the other steps. A practical precondition.
- **Management engine, Secure Boot keys, boot entries, firmware asset tag.** Settings and identifiers rather than user data. We clear them so the machine does not arrive carrying the last organisation's fingerprints.
- **Autopilot, Activation Lock, Chromebook enrolment, Absolute.** Nothing to do with wiping. The data sits in someone else's account, not on the machine. We check because an enrolled laptop is unusable however well we erase it. This is a commercial problem, not a compliance one.
- **The donor declaration.** Our own form. It documents where our responsibility starts, which supports the governance thinking in the guidance even though no standard asks for the form itself.
- **The asset register.** The standards want records; tracking every machine by serial from arrival to handover is simply how we produce them, and it goes further than the minimum.
- **Removing stickers and property labels.** Presentation, plus not advertising which organisation a machine came from.
- **The counter script for machines handed in by the public.** Entirely ours, and the right answer to a problem the standards were not written for.

> **ONE THAT IS CLOSER THAN IT LOOKS**
>
> Neither standard names a product, so no tool choice is ever mandated. But Revision 2 added an explicit expectation that we establish trust in the vendor's implementation of whatever technique we use. Choosing a tool with independent validation is therefore not just a convenience — it is the most direct way to satisfy that expectation, and it is a fair point to make when the cost is questioned.

08 What counts as evidence

Revision 2 of the NIST guidance put the emphasis squarely here: policies, roles, decision criteria, records and evidence. An assessor wants four things.

ONE — THE WRITTEN POLICY

- Names both standards, current versions
- A table showing which method we use on which type of drive
- A step-by-step work instruction for the bench
- Named roles: who erases, who verifies, who signs off
- What happens when a drive fails: destruction, with its own record
- Training records, a retention period, and a dated annual review

TWO — A CERTIFICATE FOR EVERY MACHINE

Produced by the tool, carrying: our organisation's name; make, model, serial number and drive type; the method used; the tool name and version; how it was verified and the result; who did it and who checked it; the date; and what happened to the machine afterwards.

THREE — AN ASSET REGISTER

Every machine tracked by serial number from arrival to handover, with its certificate attached to the entry. A spreadsheet is perfectly adequate at our scale. This is our chain of custody.

FOUR — A PROCESS WE CAN DEMONSTRATE

Assessors often ask to watch one laptop go through from start to finish. Keep a sample pack of five completed certificates with their matching register entries ready to hand over.

> **THE REALISTIC RISK IS NOT TECHNICAL**
>
> An assessor finding four machines with no certificate is a worse failure than a slightly imperfect method. Gaps in the paperwork sink applications. Consistency matters more than sophistication, and consistency is exactly what slips when we are busy or short-handed. That is what the written instruction is for.

09 Questions we should expect

Can we not just reinstall Windows?

No. That leaves the old data in place and simply marks the space as available. Reinstalling over the top is one of the failure modes the standards exist to prevent.

How long does each laptop take?

Seconds on a modern drive, several hours on an older spinning one, but it runs unattended. Hands-on time is roughly five to ten minutes, most of it recording the serial number.

Do we need a technical person?

For setup, yes, a day or two. Day to day, no, provided it is written down. A volunteer can be trained on the routine in an afternoon.

What does it cost to start?

A few USB sticks and a drive dock, plus a modest software licence. Under a couple of hundred pounds to be operational, and a validated per-device tool can be added later.

What if we get it wrong?

Someone receives a laptop still carrying a stranger's personal data. That is a reportable breach whether the machine was sold, exchanged or donated, and it is what all of this is insuring against.

Is this achievable for an organisation our size?

Yes. Plenty of small charities and social enterprises already do it. The technical work is genuinely easy. The discipline of recording every machine, every time, is the part that needs real attention.

10 Where to read more

NIST SP 800-88 Rev. 2 — Guidelines for Media Sanitization

The current version. Free to download.
https://csrc.nist.gov/pubs/sp/800/88/r2/final

Summary of what changed in Revision 2

A short read explaining why Revision 1 was withdrawn.
https://csrc.nist.gov/News/2025/guidelines-for-media-sanitization-rev-2

IEEE 2883-2022 — Standard for Sanitizing Storage

The technical companion. Paid document.
https://standards.ieee.org/ieee/2883/10277/

Blancco

Validated commercial erasure software.
https://blancco.com/

Parted Magic

Low-cost bootable tool. Erasure detail on the linked page.
https://partedmagic.com/secure-erase/

ShredOS and nwipe

The free option. Note the SSD limitations set out in the nwipe documentation.
https://github.com/PartialVolume/shredos.x86_64
https://github.com/martijnvanbrummelen/nwipe

ADISA Certification

The UK certification body for IT asset disposal. Its research centre is currently the only laboratory verifying tools against both standards named in our requirement.
https://adisacertification.com/

ICO — ADISA ICT Asset Recovery Standard 8.0

The approved UK GDPR certification scheme, on the Information Commissioner's register.
https://ico.org.uk/for-organisations/advice-and-services/certification-schemes/certification-scheme-register/adisa-ict-asset-recovery-certification-80/

ICO — disposal and deletion guidance

The regulator's expectations for getting rid of equipment holding personal data.
https://ico.org.uk/for-organisations/advice-and-services/audits/data-protection-audit-framework/toolkits/records-management/disposal-and-deletion/

A note on pricing and product claims. Software prices and licence terms in this note come from the vendors' own published material and change often. Confirm current pricing directly, and ask each vendor about charity rates before deciding.