Data Safe Solutions Ltd

ADOPTION BRIEFING

THE OUTCOME STANDARD · FOR ORGANISATIONS THAT HAVE ALREADY CHOSEN A SUPPLIER

Keep your supplier. Mandate the outcome.

You do not have to run the tender again, revisit the site audits, or recheck a single accreditation. **One line in the specification changes what your supplier has to prove.** Not which tool they use. What the result has to be, and who stands behind it.

START HERE

Your procurement was sound. It could not have asked for this.

Somebody ran that tender properly. Requirements written, suppliers scored, sites visited, accreditations checked, terms negotiated, sign-off obtained. That was months of work and **none of it was wrong.**

What the process could ask for

Accreditation held. Method stated. Certificate issued. Chain of custody documented. Insurance in place. References taken.

Every one of those is a fair question, and every credible supplier could answer it.

What it could not ask for

Evidence that the data on each individual device was rendered irrecoverable, warranted in writing, with a party liable if it was not.

No tender could have found that, because nobody in the market was offering it. Every erasure licence disclaimed the destruction outcome. The limitation was the market, not the process.

The gap is not in your procurement. It is in **what the market would agree to stand behind.**

THE MOVE YOU ALREADY MAKE

Changing the requirement is not new or unusual.

Disposal suppliers are told what to use all the time. Any ITAD will tell you the same thing, because they hear it from their clients constantly.

> "Our client says we have to use a named erasure product."
>
> **Routine instruction to an ITAD**

> "Our client says we have to use a specific overwrite standard."
>
> **Routine instruction to an ITAD**

> "Our client says everything must be physically destroyed."
>
> **Routine instruction to an ITAD**

So the mechanism already exists and your supplier already knows how to respond to it. The problem is **what is currently being mandated.** Named products are mandated on reputation. Overwrite standards are still mandated years after they were superseded, including HMG Infosec Standard 5, which NCSC guidance replaced. In each case the instruction specifies a **method**, and a method is a process.

You are already mandating. **Mandate the outcome instead of the method.**

WHAT TO MANDATE

The outcome standard.

Not a better eraser. A definition of what **destroyed** has to mean before anyone writes it on a certificate. Three parts, and a supplier meets all three or none.

Proven

A **device level record** that the data on that specific device was rendered irrecoverable. Not a record that a process ran.

Warranted

That outcome **warranted in the governing licence**, and not disclaimed or contradicted anywhere else in the agreement.

Insured

Cover that **responds when the outcome fails**, rather than a policy that excludes the one event that matters.

THE SAME THING, WORDED FOR A SPECIFICATION

For each device processed the supplier shall deliver **a device level record evidencing that the data has been rendered irrecoverable**; shall **warrant that outcome** in the governing licence, with liability for it not disclaimed elsewhere in the agreement; and shall hold **insurance that responds to failure of that outcome**.

Do not name us. Name the standard.

Nothing above mentions Data Safe Solutions, and it should not. **If another supplier can prove the outcome, warrant it and insure it, they have met the standard and your data is protected.** That is the point. It is a clause, not an accreditation scheme, and nobody administers it. Anyone can write it and anyone is free to meet it.

HOW TO TEST A SUPPLIER AGAINST IT

Four questions. Ask for the answers in writing.

A supplier who can answer all four on paper is giving you outcome evidence. One who cannot is giving you a process receipt. **This works on us as well as on anyone else.**

WHAT TO ASK ANY SUPPLIER, IN WRITING	WHAT A GOOD ANSWER LOOKS LIKE
How does your software select the correct destruction method for each individual drive?	The device is interrogated and the method determined per drive, not one method applied across a batch.
Does your certificate warrant that the data on that specific device is irretrievable, or only that a process completed?	A warranty of the outcome on the certificate, and the same warranty in the governing licence.
When the correct method is refused or unsupported, do you fall back to an overwrite and still certify?	Fallback is not permitted and the record says so. A failure is recorded as a failure.
What do you pay if data is later recovered from a device you certified?	A stated liability position with the clause number, and insurance that responds to the destruction having failed.

HOW IT GETS DELIVERED

Three routes. The requirement is identical in all three.

1

Mandate it to your existing supplier

Nothing about your arrangement changes. Your current ITAD keeps the contract, the collections and the chain of custody, and licenses the engine to meet the requirement you have set.

Enforced through the supplier terms you already have.

2

We deliver it on-site

DSS attends your premises and destruction completes before any device moves.

Suited to a decommission, a one-off clearance, or where assets cannot leave the building.

3

Run it yourself

You license the engine and operate it inside your own estate, with your own staff.

Suited to organisations already processing their own end-of-life equipment.

The engine outputs XML and integrates through OpenAPI, so it drops into existing asset management and workflow systems rather than replacing them. Live at NHS Royal Cornwall and across IT Health's Trust estate.

The method of delivery does not change the requirement. **Only the level of assurance.**

HOW WE MEET IT, AND HOW TO HOLD ANYONE ELSE TO THE SAME

Proven. Warranted. Insured.

In the contract

The contractual deliverable is the **Data Destruction Outcome**, achieved only where a Successful Execution Event is recorded.

Irrecoverability is warranted for each successful execution at **clause 5.1**.

Liability for that outcome is **uncapped at clause 17.1**, and is not qualified by a disclaimer elsewhere in the agreement.

No charge on a failure, and no false pass.

Behind the contract

£10 million Technology Professional Indemnity and **£10 million** Public and Products Liability, each on an each and every claim basis.

The **standard inefficacy exclusion is expressly removed by endorsement**, so the cover responds to the destruction itself having failed. An insurer does not strike that exclusion out for a product it expects to fail.

Independently certified to ADISA Product Assurance Level 5. Patent application GB2638704A published.

Put the four questions to your current supplier. Then put the same four to us.

We will answer in writing, so you can compare the two side by side.

hello@datasafe360.com | +44 151 440 3200

2nd Floor, Port of Liverpool Building, Mann Island, Liverpool L3 1BY

datasafe360.com · September 2026