ITAD Compliance Pack

SECURE TRANSPORTATION SINCE 1996



A practical index of the documents, records, and checks a business should hold to show that redundant IT assets were disposed of securely and lawfully

1. Purpose:

This pack helps IT managers, InfoSec, Compliance, Procurement, and Facilities teams gather the evidence that an IT asset disposal (ITAD) project was handled properly, from the moment assets were released to their final outcome.

It helps to show:

- which assets left the business
- who handled them at each stage
- how data was destroyed or erased
- where the equipment went
- that the supplier was authorised to do the work

This pack is particularly useful for:

- **end-of-life hardware disposals**
- **office closures and IT refreshes**
- **data centre decommissioning**
- **regulated sectors with audit requirements**
- **GDPR accountability records**
- **supplier due diligence**

2. What This Pack Is For:

When a business disposes of IT equipment it remains responsible for the personal data on it and for the waste it produces. This pack sets out the records that show both responsibilities were met.

It does not replace legal advice or the supplier's own certificates. It is an index of what to ask for, what to check, and what to keep.

3. When to Use This Pack:

Use this pack when:

- appointing or reviewing an ITAD supplier
- planning a disposal project
- preparing for an internal or external audit
- answering a customer or regulator question about disposal
- closing down a site or a server room

Start it before the first asset is released, not after the last one has gone.

4. How to Use This Pack:

1. Confirm what your own policies and sector rules require
2. Use Part A before the supplier is appointed
3. Use Parts B to F during each disposal
4. Use the submission checklist before filing the record
5. Keep the finished pack with the project record

5. Part A: Supplier Due Diligence:

Purpose: shows the supplier was suitable before any asset was released.

- ☐ Company details and main contact
- ☐ Waste carrier registration evidence
- ☐ Treatment facility permit or details of the authorised downstream facility
- ☐ Quality, environmental, and information security certificates held, with expiry dates
- ☐ Insurance certificates
- ☐ Staff vetting statement
- ☐ Data destruction methods and the standard worked to
- ☐ Sample Certificate of Destruction and sample asset report
- ☐ Contract or data processing terms covering the service

6. Part B: Asset Register and Release:

Purpose: shows exactly what was released and who authorised it.

- ☐ Asset list with type, make, model, and serial number

- [ ] Data-bearing assets flagged
- [ ] Location of each asset before collection
- [ ] Release authorised by a named person
- [ ] Date and time of release
- [ ] Any asset not found or not released noted

7. Part C: Chain of Custody:

Purpose: shows continuous control from release to processing.

- [ ] Collection note signed by both parties
- [ ] Count checked at collection
- [ ] Container or cage references, with seal numbers where used
- [ ] Vehicle and crew details
- [ ] Receipt at the processing site
- [ ] Count and serial check on receipt
- [ ] Any discrepancy recorded and resolved

8. Part D: Data Destruction Evidence:

Purpose: shows that data was destroyed or erased and how.

- [ ] Method recorded for each asset type: erasure, degaussing, or physical destruction
- [ ] On-site or off-site destruction recorded
- [ ] Serial numbers of drives and media captured before destruction
- [ ] Erasure report for each wiped device
- [ ] Certificate of Destruction with date, quantities, method, and reference
- [ ] Witness details where destruction was witnessed
- [ ] Failed erasures recorded and sent for physical destruction

9. Part E: Waste and Environmental Records:

Purpose: shows the equipment was treated lawfully as waste.

- [ ] Waste transfer note for each collection
- [ ] Hazardous waste consignment note where required
- [ ] Weights by equipment category
- [ ] Reuse, recycling, and recovery outcome

- [ ] Environmental or WEEE report

10. Part F: Reuse and Resale Records:

Purpose: shows what happened to equipment that was not destroyed.

- [ ] Assets approved for reuse or resale listed
- [ ] Erasure confirmed before any asset left the processor
- [ ] Asset tags and company markings removed
- [ ] Final outcome for each asset recorded
- [ ] Any value returned to the business recorded

11. Suggested Submission Checklist:

- [ ] Supplier due diligence complete and in date
- [ ] Asset register complete
- [ ] Release authorisation signed
- [ ] Chain of custody complete, with no gaps
- [ ] Serial reconciliation complete
- [ ] Destruction or erasure evidence held for every data-bearing asset
- [ ] Waste documentation held for every collection
- [ ] Exceptions logged and closed
- [ ] Pack filed under one project reference

12. Common Compliance Gaps to Avoid:

- supplier certificates never checked or out of date
- asset list without serial numbers
- no signature at the point of release
- certificate issued for a quantity, with no serial list behind it
- data-bearing devices not separated from general WEEE
- no record of where reused equipment went
- waste paperwork and data paperwork filed in different places

13. Best Practice Guidance:

Decide the destruction method by data risk: the more sensitive the data, the stronger the case for on-site physical destruction.

Reconcile by serial number: a count is not proof. A matched serial list is.

Keep one reference: use the same project reference across every document in the pack.

Check the supplier each year: registrations and certificates expire.

Keep the pack: retain it for as long as your own policy and the regulations require.

14. Why this pack matters:

A complete **ITAD compliance pack** helps:

- show accountability for personal data
- answer audit and customer questions without delay
- reduce the risk of a data breach through disposed equipment
- prove the waste duty of care was met
- hold suppliers to a clear standard

With IT disposal, the equipment leaves the building but the responsibility stays. The record is what closes it.

15. Related Secure Transportation services:

- ITAD, Data Destruction and WEEE
- HDD Data Destruction
- WEEE Waste Disposal
- Secure Transport UK and Europe
- Programme Management and Compliance
- RAMS and Method Statements