



T&M REUSE YORKSHIRE LIMITED

10-Step Business Data Disposal Checklist

Phone: 0113 320 3344 | Email: info@tmreuseleeds.co.uk | Website: <https://tmreuseleeds.co.uk/>

CORE VALUE PROPOSITION

Ensure every IT asset leaving your business is securely tracked, sanitised and documented before disposal.

ORGANIZATION NAME:

AUDIT / BATCH REF:

INSPECTOR / LEAD:

DISPOSAL DATE:

PHASE 1: PLANNING, ASSET IDENTIFICATION & PREP (STEPS 1–5)



STEP 01

Complete Comprehensive Asset Inventory & Tagging

Log all decommissioned hardware into a central register prior to physical handling or transfer.

- Record Serial Numbers, Asset Tags, Device Types (Laptops, Desktops, Servers, Storage Media).
- Include removable media: external HDDs, flash drives, backup tapes, and smartphones.
- Verify physical location and confirm custody owner for every item listed.



STEP 02

Classify Stored Data & Define Sanitization Standard

Assess data sensitivity level to determine required regulatory erasure standard (e.g., NIST 800-88, HMG IS5).

- Identify presence of PII, GDPR-regulated customer data, intellectual property, or financial records.
- Assign clear sanitization standard: Logical Wipe (Clear) vs. Cryptographic Erase / Physical Destruction (Purge/Destroy).



STEP 03

Establish Physical Chain of Custody & Secure Storage

Prevent unauthorized access, theft, or data leakage while assets await sanitization.

- Transfer assets to lockable, access-controlled storage containers or secured rooms.
- Implement sign-in / sign-out logs for all technicians interacting with pending assets.



STEP 04

Unlink Accounts, Revoke MDM & Remove Security Locks

Remove cloud ties and firmware locks to enable full drive overwriting and hardware reuse.

- Deauthorize Mobile Device Management (MDM), Apple iCloud / Activation Locks, and Intune profiles.
- Disable BIOS / UEFI passwords, BitLocker / FileVault disk encryption keys, and firmware locks.



STEP 05

Verify Backups & Formalize Retention Sign-off

Ensure critical business data is safely archived in line with corporate compliance requirements before permanent erasure.

- Confirm successful data migration or backup completion with department heads.
- Obtain written authorization from Information Security Lead approving irreversible drive wiping.

PHASE 2: EXECUTION, DESTRUCTION & GOVERNANCE (STEPS 6–10)



STEP 06

Perform Certified Data Erasure (NIST 800-88 / Blancco)

Execute multi-pass software sanitization on functional magnetic drives and SSDs.

- Apply industry-standard software overwrite algorithms ensuring zero data recoverability.
- Generate tamper-proof erasure reports matching drive serial numbers to hardware chassis.



STEP 07

Physically Destroy Non-Erasable / Defective Media

Destroy media that fails software erasure or is physically damaged beyond software access.

- Utilize industrial shredding, degaussing, or crushing to DIN 66399 compliance.
- Maintain serial-tracked destruction logs for every crushed drive or tape.



STEP 08

Execute Environmentally Compliant WEEE E-Waste Disposal

Partner with authorized IT disposal specialists to promote circular economy and zero landfill goals.

- Engage certified environmental partners like T&M Reuse Yorkshire Ltd for ethical IT asset recovery.
- Obtain Hazardous Waste Transfer Notes (WTN) and Duty of Care compliance documents.



STEP 09

Collect & Archive Official Certificates of Data Destruction

Gather legal proof of data destruction for GDPR compliance, internal auditing, and legal protection.

- Store Certificate of Destruction (COD) mapped to exact device serial numbers in central audit vault.
- Ensure documents are retained in accordance with statutory corporate data retention periods.



STEP 10

Update Corporate Asset Register & Final Decommissioning

Formally close the asset lifecycle across IT, accounting, and insurance systems.

- Mark items as 'Disposed/Sanitized' in IT Service Management (ITSM) and financial ledger.
- Remove decommissioned hardware from active insurance coverage schedules and corporate liability.

Regulatory Compliance Standards

- **UK GDPR & Data Protection Act 2018:** Article 32 Security of Processing.
- **NIST SP 800-88 Rev 1:** Guidelines for Media Sanitization.
- **WEEE Regulations:** Waste Electrical & Electronic Equipment Directive.
- **ISO/IEC 27001:** Control A.8.10 Information Deletion.

Verification Summary

- [] Total Assets Accounted For: _____
- [] Erasure Certificates Received: _____
- [] Waste Transfer Notes Issued: _____
- [] Asset Register Reconciled: _____

Sign-off & Governance Authorization

IT / SECURITY OFFICER SIGNATURE:

DISPOSAL VENDOR / AUDITOR:

COMPLETION DATE & STAMP:

Need Professional, Secure IT Disposal & Certified Data Erasure in Yorkshire?

Call 0113 320 3344 | Email info@tmreuseleeds.co.uk | Visit <https://tmreuseleeds.co.uk/>