IT Asset Disposal Audit Checklist

Identify every device within your organisation that requires secure disposal and chain-of-custody tracking.

PHASE 1: MULTI-DEPARTMENT HARDWARE DISCOVERY

- [ ] **Scan End-User Workspace Fleets**
  Compile physical inventories of remote-worker laptops, department desktops, and tablets currently designated for retirement.

- [ ] **Review Datacentre & Infrastructure Nodes**
  Identify rack-mounted production servers, storage area networks (SANs), standalone blades, and old firewall routers.

- [ ] **Check Shared Office Peripherals**
  Log networked multi-function printers, document scanners, smartboards, and enterprise VoIP hardware configurations.

PHASE 2: LOOSE STORAGE MEDIA IDENTIFICATION

- [ ] **Unearth Disconnected Drives**
  Audit IT support closets for loose solid-state drives (SSDs), magnetic platter HDDs, and hot-swap storage bays.

- [ ] **Log Encrypted Removable Volumes**
  Gather localized offsite flash drives, magnetic backup tapes, and external travel media containing historical data archives.

PHASE 3: CHAIN-OF-CUSTODY TRACKING & SIGN-OFF

- [ ] **Affix Tamper-Evident Security Seals**
  Apply numbered asset tags or locking tags to storage bins before transport to verify transit integrity.

- [ ] **Reconcile Post-Destruction Manifests**
  Cross-check the vendor's serialised destruction records against your initial discovery file to confirm complete reconciliation.

Phone: 0113 320 3344 **Email:** info@tmreuseleeds.co.uk tmreuseleeds.co.uk