

Pre-Sale Device Checklist: Complete Data Sanitization Guide

Protect Your Personal Information Before Selling or Donating



Why This Matters

- ⚠️ **Factory resets & file deletion** don't actually remove data — they just hide it
- 🕒 Professional recovery tools can restore "deleted" files, credentials, financial records within minutes
- 🛡️ Proper sanitization ensures your personal information is **permanently destroyed**

❗ Data Exposure Risk

Selling without proper sanitization exposes: login credentials, financial records, personal photos, sensitive documents



Pre-Sanitization Preparation

Identify Your Storage Devices

- ☐ **SSD** (Solid State Drive): Standard in devices from 2015 onward
- ☐ **HDD** (Hard Disk Drive): Spinning magnetic disk, common in older devices
- ☐ External drives: USB-connected hard drives, flash drives, SD cards
- ☐ Check storage type: Windows (Device Manager) or Mac (About This Mac)

SSDs and HDDs require completely different sanitization methods

Remove Hardware Locks & Accounts

- ☐ Remove BIOS/UEFI passwords if set
- ☐ Remove firmware locks (especially Mac Activation Lock)
- ☐ Deregister device from manufacturer accounts
- ☐ Remove device from "Find My" services
- ☐ Clean device exterior and remove personal identifiers


Pre-Sanitization Preparation

Backup Important Data

- ☐ Back up files to **separate external drive or cloud service**
- ☐ Verify backup integrity by opening several files
- ☐ Store backup drive in secure location separate from device

Disconnect & Disable Services

- ☐ Disconnect from internet (disable WiFi, unplug Ethernet)
- ☐ Disable cloud sync services (OneDrive, iCloud, Google Drive)
- ☐ Temporarily disable antivirus and security software
- ☐ Log out of all accounts (Microsoft, Apple ID, Google, social media)
- ☐ Remove disk encryption recovery keys from cloud storage

 Sanitization **permanently destroys all data**.
There is no recovery after this process.

Cloud services may attempt to sync or recover data during sanitization, interfering with the process

Choose Your Sanitization Method

For SSD (Solid State Drive)

Manufacturer Utility

Easiest option with official tools

- Download from manufacturer (Samsung, Crucial, WD)
- Follow secure erase instructions
- Save verification report

 30 min - 2 hours

 Highest security

BIOS/UEFI Secure Erase

Advanced option built into system

- Enter BIOS/UEFI (Del, F2, F10, or Esc)
- Locate "Secure Erase" option
- Select SSD and confirm erasure

 30 min - 1 hour

 High security


Traditional file deletion and multi-pass overwriting **do not work properly** on SSDs due to wear-leveling algorithms

For HDD (Hard Disk Drive)

DBAN (Darik's Boot and Nuke)

Free option for multi-pass overwriting

- Download from dban.org
- Create bootable USB drive
- Select "DoD 5220.22-M" method (3-pass)
- Allow process to complete (3-12+ hours)


 3-12+ hours

 High security

Professional Software

Comprehensive option with verification

- Use Offignium (Windows) or MacGlacio (Mac)
- Select "Wiper Prime" algorithm
- Start Drive Erasure and wait for completion

 2-12+ hours

 Highest security

☑ Phase 3: Post-Sanitization Verification

- ☐ Internal SSD or HDD: Sanitized (Yes/No)
- ☐ External hard drive(s): Sanitized (Yes/No)
- ☐ USB flash drive(s): Sanitized (Yes/No)
- ☐ SD cards: Sanitized (Yes/No)

⚠ Common Mistakes to Avoid

❌ Factory Reset

Factory resets only delete file pointers, not actual data

✅ Secure Erase

Use hardware secure erase or multi-pass overwriting

❌ DBAN on SSDs

DBAN doesn't work properly on SSDs due to wear-leveling

✅ SSD-Specific Tools

Use manufacturer utilities or professional software

❌ Forgetting External Drives

External drives often contain years of backup data

✅ Complete Inventory

Sanitize every storage device connected to your computer

❌ Encryption ≠ Sanitization

Encryption protects data but doesn't erase it

✅ Always Sanitize

Perform secure erasure even on encrypted drives

Recommended software



Offigneum

Windows

- ✓ Supports **all device types**: SSDs, HDDs, external drives, USB
- ✓ **51 sanitization algorithms** including Wiper Prime
- ✓ Enterprise-grade verification reports

www.ambeteco.com/Offigneum



MacGlacio

Mac

- ✓ Professional-grade sanitization for **all Mac-compatible storage**
- ✓ Optimized for SSDs and HDDs with proper methods
- ✓ Supports USB sticks, SD cards, and external drives

www.ambeteco.com/MacGlacio

For Free Options



Manufacturer SSD Utilities

Samsung, Crucial, WD, Kingston

- ✓ **Samsung Magician**, **Crucial Storage Executive**, WD Dashboard
- ✓ Manufacturer-specific secure erase commands
- ✓ **Free** and optimized for specific SSD models



DBAN

HDD Only

- ✓ **DoD 5220.22-M** multi-pass overwriting method
- ✓ Bootable utility that works outside of OS
- ⚠ **Not suitable for SSDs** - only works on HDDs

Your personal data is your responsibility

- ⚠ One forgotten device can expose **financial records** and **personal photos**
- 🔒 Proper sanitization prevents **identity theft** and **privacy breaches**
- ✓ Follow this checklist to ensure **complete data destruction**

Data Sanitization is Not Optional—It's Essential

