

IT & DATA SERVICES

Disk & Media Destruction

When your hardware reaches end of life, simply deleting files isn't enough. Our certified disk and media destruction service ensures your sensitive data is permanently, verifiably eliminated — protecting your business, your clients, and your compliance obligations. Whether you need a full audit trail for regulatory purposes or a straightforward one-off disposal, we have a solution to fit.

WHY IT MATTERS

Retired hard drives, SSDs, USB sticks, and tape media can hold recoverable data long after they've been "wiped" using standard tools. Proper end-of-life media handling is not just best practice — in many sectors it is a legal requirement under UK GDPR and the Data Protection Act 2018. Our service provides the documentation, chain-of-custody records, and certified destruction you need to demonstrate compliance.

DESTRUCTION OPTIONS

Data Wipe

Overwrites storage using DoD 5220.22-M and NIST 800-88 algorithms across multiple passes — rendering data unrecoverable while keeping the device functional and suitable for resale.

- Multi-pass overwrite
- HDD, SSD, USB, SD card support
- Certificate of erasure provided
- Suitable for device resale

Degaussing

A powerful electromagnetic process that permanently destroys magnetic fields on hard drives and tape media. The device is rendered completely inoperable and non-readable, even by specialist recovery tools.

- Effective on HDDs & magnetic tape
- Fast throughput for bulk media
- Certificate of degaussing provided

Physical Destruction

Media is shredded, crushed, or disintegrated using industrial equipment — the gold standard for highly sensitive, classified, or end-of-life material where no reconstruction risk can be tolerated.

- HDDs, SSDs, phones, tapes, optical
- Witnessed destruction available
- Certificate + waste transfer note

DID YOU KNOW?

- A standard "delete" or format only removes the file reference — data remains on disk and is recoverable with freely available tools.
- SSDs require secure erase commands or physical destruction — degaussing alone is ineffective on flash-based storage.
- UK GDPR requires organisations to have documented processes for secure data disposal at end of hardware life.
- Over 40% of second-hand hard drives purchased online still contain recoverable personal or business data.
- A single exposed drive can expose an organisation to ICO fines of up to £17.5 million or 4% of global turnover.
- Chain-of-custody documentation is often required by cyber insurance providers when making breach-related claims.

Not sure which option is right for your hardware or compliance requirements? Our team is happy to advise.

services@apexpointdata.com