CDL provides an award winning, GDPR compliant, asset disposal service which helps eliminate the risks associated with data sanitisation for Data Controllers. CDL hold the following accreditations, awards and insurances which will ensure you comply to the GDPR ‘due diligence’ legal requirements...

- ADISA Accredited with Distinction
- Data Erase Company of the Year 2017, 2018 and 2019
- UK Government Cyber Essentials Plus
- ISO 9001, 14001 and 45001
- NHS DSPT compliant
- Halton Business of the year 2017 and 2018
- Cyber Security Insurance to £10,000,000
- GDPR Compliant
- Security Compliance Award 2018
- Security Company of the Year 2018
- Security Awards Editors Choice 2019

CDL can provide sanitisation standards expected by data controllers in the following ways:

**Non-Destructive** - Data on the media type is overwritten which then allows the device to be reused.

**Destructive** - The media type is physically destroyed making it unusable.

In House and On Site sanitisation is carried out with the following compliance methods:

**In House** - CDL will collect your equipment using our own satellite tracked vehicles and BPSS checked drivers. All CDL vans are fitted with a two camera CCTV system, one forward facing and one in the rear of the vehicle, overlooking the equipment.

Items are then processed at CDL facility which has one of the highest rated security systems available. The site perimeter is surrounded by 2.4 meter prison mesh fencing. The site is also covered by 30 x external and internal analytic, full colour night vision CCTV cameras and a further 35 x CCTV cameras with full PIR coverage, including 7 x PTZ cameras and an ANPR camera. Both the CCTV and alarm system are externally monitored 24/7 with a PA system and regular security patrols. During working hours, a security guard is present throughout the day to make regular perimeter checks and conduct employee searches. All site gates and internal doors are access controlled with relevant permissions.

**On Site** - Using our dedicated data destruction vehicle we can provide all our destructive services on site. The vehicle is equipped with our high level degausser, crypto cut shredder and hard drive crush box. The vehicle can be run on generator or can be mains powered for silent running. Alternatively the destruction equipment can be removed and used in our clients premises. The vehicle is also satellite tracked and has a two camera CCTV system, one forward facing and one in the rear of the vehicle overlooking the equipment being destroyed.
<table>
<thead>
<tr>
<th>MEDIA TYPE</th>
<th>Non-Destructive</th>
<th>Standard Level Destruction</th>
<th>Higher Level Destruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Magnetic Hard Drive</td>
<td>Erase using Whitecanyon Wipedrive V9 using HMG ISS Enhanced wipe method (NCSC Assured Standard)</td>
<td>Shred using Untha RS40 to 40mm</td>
<td>Shred using Untha RS40 to 20mm or 6mm</td>
</tr>
<tr>
<td>Solid State Drive</td>
<td>Erase using Whitecanyon Wipedrive V9 using NIST 800-88r1 wipe method (ADISA Claims Tested Standard)</td>
<td>Shred using Untha RS40 to 40mm</td>
<td>Shred using Untha RS40 to 20mm or 6mm</td>
</tr>
<tr>
<td>Back Up Tape and Floppy Disk</td>
<td>Not Available</td>
<td>Shred using Untha RS40 to 20mm</td>
<td>Shred using Untha RS40 to 20mm or 6mm</td>
</tr>
<tr>
<td>Mobile Device</td>
<td>Erase using BlackBelt Datawipe V4 (ADISA Claims Tested Standard)</td>
<td>Shred using Untha RS40 to 40mm</td>
<td>Shred using Untha RS40 to 20mm or 6mm</td>
</tr>
<tr>
<td>Flash Media / SD Card / CD-ROM</td>
<td>Not Available</td>
<td>Shred using Kobra 430 TS Shredder</td>
<td>Shred using Kobra 410 TS Shredder</td>
</tr>
<tr>
<td>Printer / Copier / MFD</td>
<td>Not Available</td>
<td>Remove hard drive and shred using Untha RS40 to 40mm</td>
<td>Remove hard drive and shred using Untha RS40 to 20mm or 6mm</td>
</tr>
<tr>
<td>Router and Switch</td>
<td>Reset to factory default following manufacturers instructions.</td>
<td>Remove boards and shred using Untha RS40 to 40mm</td>
<td>Remove boards and shred using Untha RS40 to 20mm or 6mm</td>
</tr>
<tr>
<td>Terminal / Thin Client</td>
<td>Erase using Whitecanyon Wipedrive V9 using HMG ISS Enhanced wipe method (NCSC Assured Standard)</td>
<td>Shred using Untha RS40 to 40mm</td>
<td>Shred using Untha RS40 to 20mm or 6mm</td>
</tr>
<tr>
<td>IP Phone</td>
<td>Reset to factory default following manufacturers instructions.</td>
<td>Shred using Untha RS40 to 40mm</td>
<td>Shred using Untha RS40 to 20mm or 6mm</td>
</tr>
<tr>
<td>MEDIA TYPE</td>
<td>Non-Destructive</td>
<td>Standard Level Destruction</td>
<td></td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>----------------------------</td>
<td></td>
</tr>
<tr>
<td>Magnetic Hard Drive</td>
<td>Erase using Whitecanyon Wipedrive V9 using HMG IS5 Enhanced wipe method (NCSC Assured Standard)</td>
<td>Destroy using eDR disk crusher</td>
<td></td>
</tr>
<tr>
<td>Solid State Drive</td>
<td>Erase using Whitecanyon Wipedrive V9 using NIST 800-88r1 wipe method (ADISA Claims Tested Standard)</td>
<td>Destroy using eDR disk crusher</td>
<td></td>
</tr>
<tr>
<td>Back Up Tape and Floppy Disk</td>
<td>Not Available</td>
<td>Degauss using Verity V880 Degausser or Proton T4</td>
<td></td>
</tr>
<tr>
<td>Mobile Device</td>
<td>Erase using BlackBelt Datawipe V4 (ADISA Claims Tested Standard)</td>
<td>Destroy using eDR disk crusher</td>
<td></td>
</tr>
<tr>
<td>Flash Media / SD Card / CD-ROM</td>
<td>Not Available</td>
<td>Shred using Kobra 410 TS Shredder</td>
<td></td>
</tr>
<tr>
<td>Printer / Copier / MFD</td>
<td>Not Available</td>
<td>Remove hard drive and destroy using eDR disk crusher</td>
<td></td>
</tr>
<tr>
<td>Router and Switch</td>
<td>Reset to factory default following manufacturers instructions.</td>
<td>Remove boards and drill FPGA memory</td>
<td></td>
</tr>
<tr>
<td>Terminal / Thin Client</td>
<td>Erase using Whitecanyon Wipedrive V9 using HMG IS5 Enhanced wipe method (NCSC Assured Standard)</td>
<td>Remove flash drive and shred using Kobra 410 TS shredder</td>
<td></td>
</tr>
<tr>
<td>IP Phone</td>
<td>Reset to factory default following manufacturers instructions.</td>
<td>Not Available</td>
<td></td>
</tr>
</tbody>
</table>

ON SITE DATA CAPABILITY
Data bearing and sanitisation restricting controls

It is the client’s responsibility to ensure the following controls are cleared prior to collection enabling CDL to sanitise the device successfully.

**BIOS PASSWORD**
A password preventing changes to the system BIOS

**APPLE PRAM PASSWORD**
A password preventing changes to apple PRAM

**COMPUTRACE / ABSOLUTE HOME & OFFICE**
A register of devices held by Absolute which locks a device and allows remote management

**APPLE DEVICE ENROLLMENT PROGRAM (DEP)**
A local register of devices held by a client which allows remote management and software deployment

**WINDOWS AUTOPILOT DEPLOYMENT PROGRAM**
A local register of devices held by a client which allows remote management and software deployment

**APPLE iCLOUD LOCK**
A user account lock which prevents the use of a device after sanitisation

**ANDROID FRP LOCK**
A user account lock which prevents the use of a device after sanitisation

The following controls will be cleared and/or factory reset as part of CDL’s standard procedure. If these controls can’t be accessed or the procedure fails then the device will be securely destroyed.

**TRUSTED PLATFORM MODULE (TPM)**
A cryptoprocessor on a motherboard which stores data encryption keys

**INTEL ACTIVE MANAGEMENT TECHNOLOGY (AMT)**
A service processor on a motherboard which allows remote access at BIOS level

**SPLASH SCREEN**
An image displayed when booting showing the BIOS or manufacturer logo

**DELL OWNERSHIP / ASSET TAG**
Ownership and Asset information displayed when booting and in the BIOS

**HP INTEGRATED LIGHTS OUT (iLO)**
A service processor on a motherboard or expansion card which allows remote access

**DELL REMOTE ACCESS CONTROLLER (DRAC)**
A service processor on a motherboard or expansion card which allows remote access

**GENERIC REMOTE ACCESS CONTROLLER**
A service processor on a motherboard or expansion card which allows remote access
CDL's Untha RS40 shredder has a four shaft shredding system that achieves exacting output specifications and impressive throughputs. Hard-wearing cutters and integrated protection from unshreddables equate to an unrivalled data destruction method.

The Untha RS40 is a secure destruction solution for most data bearing items.

CDL shred items to the following sizes as a standard destruction method...

- Hard Drives - 40mm
- Switches and Hubs - 40mm
- Terminal / Thin Clients - 40mm
- IP Phones - 40mm
- Mobile Devices - 40mm
- Back up Tape and Floppy Disk - 20mm
- Data Bearing SMW - 40mm

We can also offer a higher level of destruction, shredding to 20mm or 6mm on request.
WipeDrive 9 is the only UK NCSC certified data sanitisation product which is also trusted by the US government with a client portfolio including the NSA, IBM, Microsoft, NASA, RBS, Fujitsu and Cisco.

WipeDrive 9 is has been NCSC approved and has been successfully evaluated to NIAP EAL 2+, HIPAA certified and claims tested by ADISA.

WipeDrive can sanitise data to the following standards:

- GB Infosec Enhanced Standard 5 - Higher Level
- US DoD 5220.22-M
- NATO NAPC
- NIST 800-88 Rev 1 Compliant
- FACTA Standards
- Sarbanes-Oxley
- US Army AR380-19
- US Air Force System Security Instruction 5020
- US Naval Staff Office Publication P-5329-26
- US National Computer Security Centre TG-025
- Australian Defence Signals ACSI-33 (X1-P-PD)
- Canadian RCMP TSSIT OPS-II Standard Wipe
- German VSITR
- CSEC ITSG-06
- HIPAA
While the approach for erasing magnetic hard drives is widely understood, solid state disks (SSD) require different techniques to achieve sufficient data security.

Because Solid State Disk (SSD) storage technology is inherently unique in the way data is stored, the assumption that the erasure techniques that work for traditional hard drives will also work for SSDs is problematic. This is due to wear leveling and redundant memory blocks that can't be accessed by most erasure solutions.

WhiteCanyon WipeDrive 9 passed claims testing up to risk level 4 by ADISA (ADPC00077) for sanitisation of data on solid state media using the NIST 800-88r1 algorithm. Subsequently, WipeDrive 9 has achieved ADISA PCT certification to test level 1 and 2.
The eDR Hard Disk Crusher ensures that your confidential information remains confidential by destroying it permanently. After being crushed by the Hard Disk Crusher, the data can never be recovered again.

The eDR Disk Crusher has been claims tested by ADISA (ADPC0042) for the destruction of magnetic and solid state hard drives.

The disk crusher punches through the hard disk's spindles and physically creates ripples in the platters making it impossible to recover the data. The disk crusher can also be used to destroy other data bearing items for transport before shredding.

Using an SSD cradle the disk crusher will destroy any memory chips on solid state drives, breaking them into several pieces making them unreadable.

- Crush around 100 disks an hour
- Visual verification of destruction
- Compact and Transportable
Blackbelt data erasing solution ensures that any handsets or tablets with confidential information attached, is wiped clear as effectively as possible. It means that all data is permanently removed from that device with three overwrites and a verification pass.

Erasing mobile device data is an excellent way to protect customer data and avoid any unnecessary destruction or re-procurement costs. Not only that, but erasing mobile device data also allows recycler companies to redistribute used handsets quickly and effectively, safe in the knowledge that all previous data has been destroyed.

BlackBelt Datawipe 360 v4 has been claims tested by ADISA (ADPC0074) for use on iOS and Android mobile devices.

Blackbelt DataWipe can sanitise the following platforms:

- Apple iOS - All Versions
- Android 1.5 and later
- Windows Mobile - All Versions
- RIM BlackBerry OS4.3 and later
- Nokia Symbian 3rd Edition and later
The Proton T-4 deguasser is NSA approved which is recognised by the NCSC for meeting higher level degaussing standards as defined in HMG IS5. This is the highest level of data sanitisation offered in the UK. This approval applies to all magnetic media such as:

- Hard Drives
- DLT/LTO Tapes
- Other Magnetic Tapes
- Floppy Disks
- Audio Tapes

The Proton T-4 produces a bi-directional field which provides a 20,000 Gauss positive field and a 20,000 Gauss Negative field. The T-4 achieves this by using a unique, patented “Reverse Polarity”. Other degaussers may have either a positive or negative pulse, but only one. The T-4 has both and it is fully automatic. This ensures complete and permanent erasure of your data.

- Approved to erase all magnetic media available today and guaranteed on 8 TB hard drives
- Listed on the National Security Agency’s Evaluated Products List (NSA EPL-Degausser) and complies with DoD requirements for destroying classified information on magnetic media
- Internal software requires all parameters (capacitor voltage, switch, etc.) are present before degaussing. This software guarantees that each degauss cycle delivers sufficient strength and consistent performance
Kobra 410TS HS - High Security Crypto Cut Shredder

The Kobra 410TS is CPNI approved for high security shredding to meet standards as defined in HMG IS5.

The 410 TS is a High Security 0.8x9.5mm Crypto Cut shredder, suitable for shredding Top Secret and Crypto Paper documents as well as Optical Media including CD's/DVD's & Blu-Ray Discs, 80mm mini disks and credit cards.

The 410 TS has a security Level of P-6 and has been approved by the UK Government to meet the most stringent High Security requirements required and are recommended for all Military Bodies, Government Agencies or Security Commercial Organisations.

The 410 TS can shred up to 3000 pieces of Optical Media per hour and will turn a single sheet of paper into 10-15,000 individual pieces. The special 2.5x1.5mm OM cutting system has the highest security level available today and exceeds the Optical Media Destruction Devices guidelines and the ASIO T-4 standards for TOP SECRET level destruction of Optical Media.

- 0.8x9.5mm Crypto Cut
- Din Security Level P-6
- 410mm Entry Throat (A4, A3 and Printouts)
- CPNI Approved for Paper, Credit Cards, CD ROMS and Floppy Disks
The Kobra 430 TS Industrial Shredder is a very high performance, electric conveyor belt fed machine that is designed for large shredding requirements and continuous shredding operations, processing up to 300kg of waste per hour.

The 430 TS is supplied with new design of carbon hardened cutting knives which allow for up to 40% more efficiency in shredding capacity. Shredding up to 130 sheets of 70gsm paper documents with ease to tiny 5.8 x 50mm cross-cut pieces.

The Kobra 430 TS will shred the following items to DIN security level P-3:

- Paper
- Cardboard
- USB Media
- CD / DVD / BluRay
- Credit Cards
- Floppy Disks
The Verity V880 Automatic Metal Tape Degausser offers highly efficient erasure of high energy cassettes and cartridges in a compact conveyor degausser.

The cassettes are placed onto the moving conveyor belt and carried over two degaussing coils that are orientated at 90 degrees to one another in a "V" formation. The belt speed is fixed at 4 inches per second. This permits the machine to completely degauss media with "one pass" degaussing.

Security level - Standard Commercial Security
Technology - Dual V configured Degaussing Coils

Media Type - VHS/S-VHS, LTO, DLT, DAT as well as Computer cartridges, DC, TK 50/70/85, 3480/3490/3490e & 4/8mm