



Title	Secure Disposal Policy
Process Owner	MD
Date Created	16/06/2020
Publish Date	03/10/2022
Approved By	Management Team
Summary	Policy detailing the requirements for securely disposing of both hardcopy and electronic information.
Classification	Public
Standard	All
Version	3.2

Change Record

Enter any changes to the document within the tag below...

New logo added to document header.

Data Capability Statement added to show how different data is destroyed.

Overwrite the content of the tag, this will create each change you have made to the document and record it in ISOportal



Secure Disposal Policy

Introduction

This policy is to ensure all information is securely disposed of and cannot be accessed by unauthorised parties.

Our Waste provider is detailed within the Control Details document on ISOportal

Applicable Legislation

- ❖ WEEE Waste Regulations
- ❖ Data Protection Act

Detail

Electronic media that have exceeded the maximum storage requirement must be securely disposed of. These are disposed of in a secure and compliant with WEEE waste regulations.

Paper materials

- ❖ All printed copy media is shredded using the shredders provided in each office
- ❖ This includes all paper and notebooks as well as written notes

Hardware

- ❖ When equipment is being donated or recycled data will be wiped (several times) and restore to factory default before the hardware is removed.
- ❖ The item of hardware will be removed from the asset register where appropriate or marked as decommissioned within the asset register.
- ❖ The following table acts as a guideline for disposal of certain devices, this is in conjunction with the Information Classification Policy;
- ❖ A certificate of destruction will be retained when equipment has been sent to our Waste supplier to confirm it has been destroyed



Hardware Classification

Classification	Role	Device	Disposal Method
Restricted	Restricted by the permissions on the system	❖ Data Server	❖ Software wiped ❖ Degaussed ❖ Physically destroyed
Company Confidential	Restricted by the permissions on the system	❖ PC's ❖ Laptops ❖ Data Servers ❖ Servers ❖ Tablets	❖ Software wiped ❖ Degaussed ❖ Physically destroyed
Internal	None required	❖ PC's ❖ Laptops ❖ Removable Hard drives	❖ Software wiped

Data Capability Statement



Data Capability Statement 2022

On client site		Media Type	At processing facility	
Reuse	Destruction		Reuse	Destruction
Magnetic HDD's are destroyed using overwriting software that has been approved by an independent Laboratory or by with Software that is NCSC/CPA Approved.	Magnetic HDD are physically impaired using HSM HDS Powerline 150 Shredder or physically impaired using a eDR crushing System. Shredding to less that 20mm capability is available where SLA requires	Magnetic Hard Disk Drives	Magnetic HDD's are destroyed using overwriting software that has been approved by an independent Laboratory or by with Software that is NCSC/CPA Approved.	Magnetic HDD are physically impaired using HSM HDS Powerline 150 Shredder or physically impaired using a eDR crushing System.
Solid State Drives are destroyed using overwriting software that has been approved by an independent Laboratory or by with Software that is NCSC/CPA Approved.	A Solid State Drive will be crushed onsite to physically impair the function before transporting to process facility.	Solid State Hard Drives	Solid State Drives are destroyed using overwriting software that has been approved by an independent Laboratory or by with Software that is NCSC/CPA Approved.	A Solid State Drive will be crushed to physically impair the function of the device.
Smart Devices are destroyed using overwriting software that has been approved by an independent Laboratory or by with Software that is NCSC/CPA Approved.	Smart Devices have batteries where possible, physically impaired using HSM HDS Powerline 150 Shredder or crushing system, transported back to the facility where it is manually stripped and the internal logic board is shredded to 6 mm	Smart Phones	Smart Devices are destroyed using overwriting software that has been approved by an independent Laboratory or by with Software that is NCSC/CPA Approved.	Smart Devices will be manually stripped to remove the battery and the internal logic board which is then shredded to 6 mm
Hybrid Disk Drives are destroyed using overwriting software that has been approved by an independent Laboratory or by with Software that is NCSC/CPA Approved.	Hybrid HDD are physically impaired using HSM HDS Powerline 150 Shredder or physically impaired using a eDR crushing System. Shredding to less that 20mm capability is available where SLA requires	Hybrid Disk Drives	Hybrid Disk Drives are destroyed using overwriting software that has been approved by an independent Laboratory or by with Software that is NCSC/CPA Approved.	Magnetic HDD are physically impaired using HSM HDS Powerline 150 Shredder or physically impaired using a eDR crushing System. Shredding to less that 20mm capability is available where SLA requires
Not Available	Not Available	Routers (Wired and Wireless)	Follow Manufacturers reset process and use independent testing program to erease data	Remove boards, drill FPGA chip - or shred to 6mm if needed.
Not Available	Not Available	Printers, Copiers and Multi-function devices	HDD is removed from device and is destroyed using overwriting software that has been approved by an independent Laboratory or by with Software that is NCSC/CPA Approved.	Hdd is removed from the machine. The HDD will be crushed to physically impair the function.
Not Available	Magnetic tape devices are shredded using HSM HDS POWERLINE 150 Shredder	Magnetic Tapes	Not Available	Magnetic tape devices are shredded using HSM HDS POWERLINE 150 Shredder
Not Available	Optical Disk are destroyed using HSM HDS POWERLINE 150 Shredder. OR HSM Classic 411.2 OMDD Shredder	Optical Disks	Not Available	Optical Disk are destroyed using HSM HDS POWERLINE 150 Shredder. OR HSM Classic 411.2 OMDD Shredder
Removal Media Device is destroyed using overwriting software that has been approved by an independent Laboratory or by with Software that is NCSC/CPA Approved.	Removable Media Device will be manually stripped to remove plastic and the internal logic board which is then shredded to 6 mm	Removable Media such as USB	Removal Media Device is destroyed using overwriting software that has been approved by an independent Laboratory or by with Software that is NCSC/CPA Approved.	Removable Media Device will be manually stripped to remove plastic and the internal logic board which is then shredded to 6 mm

Version 3.2
Classification Public

