Reusing IT Policy on Data Sanitisation and Destruction

Reusing IT refurbish used computers and assorted IT equipment for reuse in schools and charitable organisations. In processing donated IT equipment the charity has a duty of care to ensure that data is removed with an appropriate level of sanitisation commensurate with the sensitivity of the data stored on the media (hard disk, removable media, flash memory, etc.). The following document sets out Reusing IT's policy on data sanitisation and destruction and the stringent standards we follow to ensure the secure, full removal of confidential and sensitive data from redundant IT equipment ensuring compliance with General Data Protection Regulations (GDPR). We work to guidelines and with software accredited by ADISA

ADISA (Asset Disposal and Information Security Alliance) is an independent certification body that specialises in data protection and quality management within the IT asset disposal sector. They provide certifications and standards for organizations involved in the secure disposal and sanitization of IT equipment, ensuring data is properly erased and the environment is protected from e-waste.

Secure Data Erasure

Reusing IT's data erasure process gives donors complete assurance that no information remains on any donated devices, enabling them to be reused rather than physically destroyed.
We process data-bearing assets from donating partners and sanitise using trusted data-wiping software that is certified to ADISA global standards. Data wiping is the only truly assured method of data destruction, as each individual drive generates its own hard drive erasure report, certifying the date and method used. Devices that fail the wiping process will be physically destroyed.

In addition to individual device certification, data wiping allows for devices to be reused, creating significant environmental and social benefits. For example, just one classroom of 20 reused PCs enables 360 students to learn vital IT skills. It also saves 6 tonnes of CO_2e, the equivalent of planting 14 trees or nearly offsetting 1 person's annual carbon footprint in the UK.

How We Erase Data

Reusing IT takes data security extremely seriously and for this reason we only use industry-leading technology and techniques that have been approved to the highest standards including the UK Government's HMG Infosec Standard No. 5 and current best practice method IEEE-2883-2022. We use market-leading Cedar data erasure software which is certified to ADISA global standards. Using Cedar's latest, certified version of software we can always ensure erasure standards are maintained in line with technological advances.

The Reassurances You Receive
Each device we receive is wiped using Cedar's software, or shredded to <20mm particles by our certified e-waste recycling partner, as per the disposition table below. Cedar's ERASE IT generates a data erasure report for each device with information including: the hard drive serial number, hard drive capacity and erasure level of 100%. We provide these reports for each collection to a donor on request. This provides traceability required for a comprehensive data audit trail to meet GDPR standards.

Where required we can provide secure collection via GPS-tracked vehicles and DBS-cleared staff to transport equipment.

Secure Physical Data Destruction
Reusing IT provides secure physical data destruction in the event that devices are not in a usable condition, or where a donor's requirements dictate physical destruction. To achieve this we arrange for offsite shredding of the data-bearing asset, which reduces it to particles under 20mm in size. This renders the device as completely unreadable, ensuring complete data destruction.

On request, we provide records detailing the crushed hard drive serial number, capacity and, where relevant, asset information. Higher shredding grades are also available on request.

Where on-site wiping, or on-site physical destruction or shredding of data-bearing assets is required we can provide this through our partners. Where Reusing IT processes equipment via a third party partner we ensure that our partners meet or exceed our standards for data security. Typically we work with partners who meet ADISA ICT Asset Recovery Standard 8.0 or the R2v3 standard set by Sustainable Electronics Recycling International.

Default Data Sanitisation Methods
The table below outlines our default data sanitisation methods for various equipment types.

Data Device Type	Sanitisation Method	Disposition on Pass	Disposition on Fail
Hard Disk Drive	Single-pass wipe to IEEE 2883-2022 using Cedar's ADISA certified Software	Reuse	Offsite shredding to <20mm
Solid State Drive	Erase IT SSD Erasure		
Apple Mac (with Apple T2 chips)	Erase IT		
Networking Device, including but not limited to: -Switch	Factory reset within unit per NIST 800-88 Clear guidelines		Disassembly and downstream recycling by our e-waste recycling partner

Devices with solid state memory, including but not limited to: -Printers -Scanners -Cameras -Mobile Phones -Tablets -Flash Drives (USB media, SD Cards)	Offsite shredding of data-bearing components, to <20mm shred size	N/A

Data Sanitisation Method Alternatives

The majority of our donors opt for our default process. We are also able to carry out a choice of accredited data destruction and data sanitisation options using Erase IT's approved erasure software that is one of the most highly accredited wiping solutions on the market. Therefore on request we can use alternative sanitisation methods specific to certain standards such as IEEE 2883-2022, HMG Infosec Standard 5 Higher Standard, NIST 800-88 Purge or DoD 5220.22-M ECE from the United States. These methods may be chargeable so please check with our team for more details. For any questions regarding how to choose the most appropriate data sanitisation method please speak to our expert team who will be able to help you select the best option for your individual circumstances.

Service Timescales

Following a collection, Reusing IT follows internal processes whereby a processing 'Lot' is created within 24 hours of its arrival at our workshop. Equipment is processed and stored in our secure facility in a monitored and alarmed environment. We then aim to process equipment and complete data sanitisation or destruction within 45 working days.