The Turing Trust Policy on Data Sanitisation and Destruction

The Turing Trust 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 The Turing Trust'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).

Secure Data Erasure

The Turing Trust's data erasure process gives donors a complete guarantee that no information remains on any donated hard drives, enabling them to be reused rather than physically destroyed. We process data-bearing assets from donating partners and sanitise using NCSC approved data-wiping software. 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. Drives which fail the wiping process will be physically destroyed.

In addition to individual hard drive certification, data wiping allows for drives 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. Software-based erasure done by The Turing Trust is also the most cost-effective method of data destruction as we generally do this process free-of-charge for donors in recognition of their support.

How we erase data

The Turing Trust 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 (the 'Enhanced Standard'). We use market-leading Blancco data erasure software. Blancco software is approved by the UK Government's National Cyber Security Centry (NCSC). Using Blancco'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 Blancco software which generates an individual, automatically produced data erasure report. This details 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
The Turing Trust provides secure physical data destruction in the event that hard drives are not in a working condition, or where a donor's requirements dictate physical destruction. To achieve this we use a solid steel punch that delivers four tonnes of hydraulic force to bend, mangle and pierce the drive's housing and platters. The conical punch of the unit causes catastrophic trauma to the hard drive's chassis whilst destroying its internal platters (the circular disks that store magnetic data). Following the hard drive crushing process with our pneumatic lever this renders the hard drive's platters as completely unreadable, ensuring complete data destruction.

This process is suitable for all kinds of hard drive formats and meets the DIN 66399 Standard security level H-3, guidelines for the physical damage of media. On request, we provide records detailing the crushed hard drive serial number, capacity and, where relevant, asset information.

Where on-site physical destruction or shredding of data-bearing assets is required we can provide this through our partners.

Data Sanitisation Method Alternatives
We are able to carry out a choice of accredited data destruction and data sanitisation options using Blancco's approved erasure software that is the most highly accredited and globally recognised wiping solution on the market. Therefore on request we can use alternative sanitisation methods specific to certain standards such as NIST 800-88 Purge or DoD 5220.22-M ECE from the United States in providing certified data erasure.

The majority of our donors opt for our default process using the HMG Infosec Standard 5, single-pass method. This is all that is required to certify the secure data destruction using the wipe process. Three pass methods, such as HMG Infosec Standard 5, Higher Standard, are available for clients whose security standards are particularly stringent - 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, The Turing Trust 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 within 28 working days which includes the completion of the data sanitisation / destruction process.

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

Data Type	Sanitisation Method	Result	Disposition
Hard Disk Drive	Blancco NCSC approved software, using a single-pass wipe.	Pass	Reuse
Hard Disk Drive	Blancco NCSC approved software, using a single-pass wipe.	Fail	Physical Destruction via Crushing – Pneumatic Punch / Leverage Shredding available - Price On Application (POA)
Hard Disk Drive -Contained within network devices or printers	Factory reset within unit	Pass	Reuse
Hard Disk Drive -Contained within network devices or printers	Factory reset within unit	Fail	Physical Destruction at The Turing Trust's discretion. Shredding available - Price On Application
Solid State Drive	A periodic Random Overwrite using Blancco NCSC Approved Software	Pass	Reuse
Solid State Drive	A periodic Random Overwrite using Blancco NCSC Approved Software	Fail	Physical Destruction via Crushing – Pneumatic Punch / Leverage Shredding available - Price On Application
Flash Drive Includes: -Mobile Phones -USB Media -Tablets	A periodic Random Overwrite using Blancco NCSC Approved Software	Pass	Reuse
Flash Drive Includes: -Mobile Phones -USB Media -Tablets	A periodic Random Overwrite using Blancco NCSC Approved Software	Fail	Physical Destruction at The Turing Trust's discretion. Shredding available - Price On Application

Networking Device, including but not limited to: -Switch -Router	Factory reset within unit	Pass	Reuse
Networking Device, including but not limited to: -Switch -Router	Factory reset within unit	Fail	Physical Destruction at The Turing Trust's discretion. Shredding available - Price On Application