Service Specification

IT Equipment Disposal

Secure Data Destruction

Contents:

Section 1 –

1.1 Client Engagement

In the absence of a client specific service contract, our Service Specification will act as an underlying guide as to what service Revive IT will provide.

1.2 Customer Service

Each client can expect to receive our highest levels of customer service at each step of the process.

We endeavour to make the entire process as simple and hassle free as possible for each client.

Client accounts are generated for each of our customer allowing Revive IT to provide its services effectively.

Our customer service team will be available between 8am and 5pm each working day via the communication methods stated on our website (www.reviveit.co.uk).

1.3 Service Pricing

Revive IT generate revenue by refurbishing equipment for re-use / sale or through materials recovery.

Our service provision costs are usually covered through these means allowing our clients to enjoy cost neutral IT disposal / data destruction.

In the event our costs can't be covered through these means or you wish for a more specific service such as onsite destruction, extensive reporting etc. there may be an associated cost. We'll always do our best to minimise this cost and you'll be made well aware of this during the collection booking process.

1.4 Compliance

Revive IT conform to and are UKAS audited to the following standards:

- ISO 9001 Quality Management
- ISO 14001 Environmental Management
- ISO 27001 Information Security Management
- OHSAS 18001 Health and Safety Management
- ISO 23001 Business Continuity Management
- ISO 50001 Energy Management
- BS 7858 Staff Vetting
- BS EN 15713 Secure Destruction

Revive IT are registered waste carriers, are permitted to store waste and are permitted to repair / refurbish waste electrical & electronic equipment (WEEE).

Waste records are maintained for a minimum of 3 years to comply with environmental legislation.

Our service is fully insured:

- Employer's Liability Insurance
- Public Liability Insurance
- Products Liability Insurance
- Professional Indemnity Insurance

Revive IT do not use third parties to complete our service.

Section 2 –

2.1 What we Recycle

Revive IT are able to recycle all IT / Telecoms / Computer related hardware.

Equipment can be in any condition – broken / working / incomplete etc.

- Computer Towers
- Laptops
- Servers
- All-in-Ones (AiOs)
- Uninterruptible Power Supplies (UPSs)
- Printers
- Apple Hardware
- Monitors
- Thin Clients
- Hard Drive Arrays
- Point of Sale (PoS) Hardware

- Whiteboards
- Photocopiers
- Credit Card Terminals
- Mobile Phones
- Tablets
- Data Bearing Devices
- Hard Disk Drives (HDDs)
- Solid State Drives (SSDs)
- Network Switches
- Routers
- Projectors
- Telephone Systems
- Telephones
- Toners
- Peripherals
- Scanners
- AV Hardware
- Networking Equipment
- Plotters
- Cables
- Accessories
- Etc.

2.2 Collections

Each collection Revive IT completes is assigned a unique identifier.

Revive IT will require the following information to complete a collection:

- Organisation name
- Full collection address
- Member of staff onsite and contact details

- Details of what needs collecting for recycling
- Details of any specific data destruction requirements
- If a full item specific inventory report is required
- Parking / access instructions
- Location of the equipment
- Any other requirements

All equipment Revive IT collects and processes is treated as waste.

A Collection Booking & Waste Transfer Form is completed and issued for each collection / service.

If we collect any waste under the European Waste Code (EWC) 20:01:35, a Hazardous Waste Consignment Note Code will be applied to the pickup.

COLLECTION BOOKING & WASTE TRANSFER FORM

Version 7 - 18.02.2020

www.reviveit.co.uk

SECTION A - Description of waste:

Computers	Printers	Peripherals
Servers	Networking	Other IT related

How is the waste contained?	Loose	**Physical form:**	Solid	**EWC Code:**	20:01:36

Quantities of each data bearing device type of which the approximate weight comprises will be indicated on your Data Destruction Certificate.		**Approximate weight (kg):**	
SECTION B - Current holder of the waste - Transferor			
Organisation name:		**Asset report required?**	
Address:		**Items to be collected?**	
Contact name:		**Parking / instructions:**	
Telephone number:		**Location of equipment (stairs / lifts / help available):**	
Email address:		**Onsite destruction? (power / location)**	
SIC code (2007):	43.21	**Available times:**	
Consignment note code - EWC 20:01:35 (if applicable):		**Booking completed by:**	
Collection charge:		**Other details:**	

SECTION C - Transferee (Revive IT)

Revive IT Recycling Ltd
7-8 Buslingthorpe Green
Leeds
LS7 2HG

T11 Exemption - NC2/061261/2018

Waste Carriers - CBDU179528

SECTION D - The transfer

Date of transfer:

Vehicle reg:

Revive IT Recycling -	Customer (Section B) -
Name:	**Name:**
Transferee's signature:	**Signature:**

***By signing above I confirm:**

1. **Acceptance of our Service Specification (displayed on our website).**
2. **Custody of all equipment has been transferred immediately to Revive IT.**
3. **I am legally allowed to transfer custody of the inventory.**
4. **I have fulfilled my duty to apply the waste hierarchy.**

SECTION E - Data Sanitization:

Guaranteed data destruction in accordance with our Data Sanitization Capability Statement.

Your Data Destruction Certicate will be provided within 7 working days.

Both parties are required to sign this document at the point of the collection. A copy will be issued to the client at that moment in time and one will be kept on the client's account for future reference.

As part of the transfer the client signs to confirm:

- Custody of all equipment has been transferred immediately to Revive IT.
- The transferor (client) is legally allowed to transfer custody of the inventory.
- The waste hierarchy has been complied with.

Any specific requirements / agreements relating to the collection, data destruction, data security or the service will be noted on this form.

2.3 Logistics

We operate our own fleet of vehicles to complete all collections and onsite services.

2.4 Transportation Security

Revive IT adhere to a carefully undertaken risk assessment and control plan with the key objective of minimising risk during transportation.

Our collection operatives have undergone extensive data security training addressing the risks associated with transporting data sensitive hardware to our collection vehicles and our processing facility.

Key control measures applied:

- GPS tracked vehicles

- Hardware transported directly to our processing facility
- BS 7858 security vetted staff
- Vehicles fitted with snap locks
- Vehicles with solid sides and solid bulkheads
- Segregation of collections
  If deemed necessary:
- Provision of SIA badged staff who have undergone Cash & Valuables in Transit training
- Use of multiple collection operatives
- Vehicles fitted with CCTV systems
- Inventory report & itemised tracking completed prior to loading

Revive IT do not use hubs or any storage other than our main processing facility.

Section 3 –

3.1 Processing Facility

All customer collections return directly to our processing facility on the same day – Located at: Unit 7-8 Buslingthorpe Green, Leeds, LS7 2HG.

This facility is specifically designed, solely owned and operated by Revive IT.

3.2 Physical Security

Customer collections are brought directly back to our processing facility where they are unloaded into a secure processing area behind 5 layers of physical security which includes site fencing, security shutters and multiple security grilles.

Customer collections deemed as high security are processed behind additional layers of security.

Customer collections are only exposed and unloaded once secure and locked within our perimeter fencing. These are then kept clearly marked and segregated.

Extensive security systems are in place which includes CCTV, number plate recognition, biometric access systems, 24hr monitoring & alert systems – all with redundancy.

3.3 Internal Security

Internal security measures include:

- Strict segregation and identification
- Restricted access to data processing areas via authorised staff only
- Use of biometric access systems
- CCTV
- BS 7858 staff security screening
- Strict procedures for new starters / visitors / contractors
- Insider risk minimised by a blend of physical and procedural checks

3.4 Internal Process

Customer collections are processed within 7 working days.

At the point of unloading, collections are deposited into their own secure, segregated location to wait processing.

Once initial logging has been completed, any assets which retain residual value go to be securely data sanitised and tested for re-use.

Any devices which are faulty or obsolete are data sanitised and are broken down for materials recovery and recycling.

All internal processes are physically segregated with assets clearly marked to prevent cross contamination.

Section 4 –

4.1 Data Sanitisation

Revive IT guarantee the destruction of all data held on the equipment we process.

In the absence of any specific requirements / agreements the destruction will be completed in accordance with our data sanitisation statement below.

Every data carrying device, which is received for data processing, will undergo the same process regardless of any assurances from the client that they have already destroyed the data.

Data Sanitisation Statement

Hardware:	Re-Use:	Destruction:
Devices registered on a cloud account	n/a	Storage device shredding, Physical destruction
Labels / References	n/a	Removal / Shredding
Computers	Drive erasure, Additional storage removal, System resets	Drive shredding, Additional storage removal, Physical destruction
All-In-Ones (AiO)	Drive erasure, Additional storage removal, System resets	Drive shredding, Additional storage removal, Physical destruction
Laptops	Drive erasure, Additional storage removal, System resets	Drive shredding, Additional storage removal, Physical destruction

Servers	Drive erasure, Additional storage removal, System resets	Drive shredding, Additional storage removal, Physical destruction
Hard Disk Drives (HDDs)	Erasure via Blancco / WhiteCanyon / Revive IT Wiping System 1.4 / OEM Utilities / Linux Secure Erase	Shredding / Crushing
Solid State Drives (SSDs)	Erasure via Blancco / WhiteCanyon / Revive IT Wiping System 1.4 / OEM Utilities / Linux Secure Erase	Shredding
Monitors	Label / Reference removal	Label / Reference removal
Point of Sale (PoS) Systems	Drive erasure, Additional storage removal, System resets	Drive shredding, Additional storage removal, Physical destruction
Printers / Multi-Functional Printers (MFPs) / Photocopiers	Reset electronically	Storage device shredding, Physical destruction
Apple Hardware	Drive erasure, Additional storage removal, System resets	Drive shredding, Additional storage removal, Physical destruction
Thin Clients	Factory reset / Storage device erasure	Storage device shredding, Physical destruction
Uninterruptible Power Supply (UPS)	Factory reset	Storage device shredding, Physical destruction
Mobile Phones	Blancco erasure / WhiteCanyon erasure / Factory reset / Security erase	Physical destruction, Additional storage removal, Shredding
Tablets	Blancco erasure / WhiteCanyon erasure / Factory reset / Security erase	Physical destruction, Additional storage removal, Shredding
Projectors	Factory reset	Physical destruction
Displays	Factory reset, Storage device erasure	Storage device shredding, Physical destruction

Televisions	Factory reset, Storage device erasure	Storage device shredding, Physical destruction
Telephones	Factory reset	Storage device shredding, Physical destruction
Telephone Systems	Factory reset, Storage device erasure	Storage device shredding, Physical destruction
Credit Card Terminals	Factory reset, Storage device erasure	Storage device shredding, Physical destruction
Wireless Access Points	Factory reset	Storage device shredding, Physical destruction
Network Switches	Factory reset, Re-flash, Secure erase	Storage device shredding, Physical destruction
Routers	Factory reset, Re-flash, Secure erase	Storage device shredding, Physical destruction
Firewalls	Factory reset, Re-flash, Secure erase	Storage device shredding, Physical destruction
Tape Drives / Autoloaders	Media tape removal, Factory reset	Storage device shredding, Physical destruction
Hard Drive Arrays	Drive erasure, Factory reset	Drive shredding, Additional storage removal, Physical destruction
Modules / Add-in Cards	Factory reset, Secure erasure	Storage device shredding, Physical destruction
Other Networking Hardware	Factory reset, Re-flash, Secure erasure	Storage device shredding, Physical destruction
CCTV Equipment	Drive erasure, Factory reset, Additional storage removal	Storage device shredding, Physical destruction

AV Hardware	Factory reset, Re-flash, Secure erasure	Storage device shredding, Physical destruction
Games Consoles	Factory reset, Re-flash, Secure erasure	Storage device shredding, Physical destruction
Digital Cameras	Factory reset, Secure erase, Storage device removal	Storage device shredding, Physical destruction
Media Tapes	n/a	Shredding
VHS Tapes	n/a	Shredding
CDs / DVDs	n/a	Shredding
Floppy Discs	n/a	Shredding
Memory Cards	Secure erasure	Shredding
USB Flash Drives	Secure erasure	Shredding
Security Code Generators	n/a	Shredding, Physical destruction
Confidential paperwork	n/a	Shredding
Other	Decided on a case by case basis	Decided on a case by case basis

4.2 Onsite Data Destruction

Any onsite data destruction must be requested at the time of booking.

If there is an associated cost this will be agreed before Revive IT complete the service.

Before we complete onsite destruction the following must be determined:

- If the destruction is to be completed in the vehicle or inside the client's premises
- What media is to be destroyed / erased, in what way and to what standard
- Does the media need asset reporting before destruction / erasure
- Is the area secure where destruction will take place
- If destruction is being completed in the vehicle, will the vehicle have a dedicated parking spot where it won't be interrupted
- Is CCTV footage of the destruction / erasure required

4.3 Quality Control

Revive IT have a documented quality control process, which checks a sample number of devices per month after the data sanitisation process has been completed.

Section 5 –

5.1 Product Re-Use

In accordance with the waste hierarchy, Revive IT prioritises re-use over any other output.

Providing assets can be securely data sanitised and it is commercially viable to do so Revive IT will refurbish hardware for re-use.

If it is possible and commercially viable to do so, Revive IT will repair devices to ensure maximum re-use potential. In the event a device can't be repaired the salvaging of parts will be considered before materials recycling.

Revive IT will confirm that any refurbished assets are safe to use as per their original design.

5.2 Waste Management

For any hardware that can't be re-used or salvaged for parts, data destruction will be completed and it will be broken down / segregated for materials recycling.

All material is sent for precious metal / material recovery which covers the cost of the environmentally friendly recycling of the less desirable materials such as plastic.

Full out-going waste records are kept and downstream duty of care auditing is completed.

Section 6 –

6.1 Reporting

Depending on customer's requirements, Revive IT is able to report back on varying levels.

Standard Data Destruction Certificate

Detailing what has been data sanitised and processed.

Juxon House
100 St Paul's Churchyard
London
EC4M 8BU

Phone: 020 3582 2578
Email: it@reviveit.co.uk
Web: www.reviveit.co.uk

Data Destruction Certificate

Client / Address:
Revive IT Recycling Ltd (LS7 2HG)
Unit 7-8
Buslingthorpe Green
Leeds
LS7 2HG

Collection Date:
May 06, 2020

Collection ID:
J2000698

Data Destruction Used: Standard Pro Data Destruction

ITEM ID	DESCRIPTION	DATA DESTRUCTION COMPLETE & PROCESSED
J2000698-00001	35 x Desktop Computers	✔ OJB
J2000698-00002	44 x LCD Monitors	✔ OJB
J2000698-00003	18 x Server	✔ OJB

J2000698-00004	52 x Laptops	✔ OJB
J2000698-00005	73 x Mobile Phones	✔ OJB
J2000698-00006	5 x UPS	✔ OJB
J2000698-00007	15 x Printers	✔ OJB
J2000698-00008	11 x Projectors	✔ OJB
J2000698-00009	2 x Box of Assorted Cables	✔ OJB
J2000698-00010	3 x Box of Keyboards / Mice	✔ OJB
J2000698-00011	28 x Loose Hard Drives	✔ OJB

Notes

Verified by HD

Data Destruction Certificate & Asset Inventory Report

Itemised list of what has been data sanitised and processed.

Juxon House
100 St Paul's Churchyard
London
EC4M 8BU

Phone: 020 3582 2578
Email: it@reviveit.co.uk
Web: www.reviveit.co.uk

Data Destruction Certificate & Asset Report

Client / Address:
Revive IT Recycling Ltd (LS7 2HG)
Unit 7-8
Buslingthorpe Green
Leeds
LS7 2HG

Collection Date:
May 06, 2020

Collection ID:
J2000698

Data Destruction Used: Standard Pro Data Destruction

ITEM ID	DESCRIPTION	MAKE / MODEL	SERIAL	ASSET TAG
J2000698-00001	Desktop PC	HP Elite 8300 SFF	CZC413367G	00206
J2000698-00002	Desktop PC	HP EliteDesk 800 G2 SFF	CZC6077FKZ	00310
J2000698-00003	Desktop PC	HP EliteDesk 800 G2 SFF	CZC6398FX2	00311
J2000698-00004	LCD Monitor	BENQ GL2450	ET5BF02754019	00296
J2000698-00005	LCD Monitor	BENQ GL2460	ET78F01297SL0	00295
J2000698-00006	Laser Printer	HP P2055dn	CNCHB98910	00245
J2000698-00007	Laser Printer	HP Pro 400 M401dn	VNH6710720	00251
J2000698-00008	Laser Printer	HP P3015	VBNQCBL03M	00259
J2000698-00009	Scanner	Fujitsu S1500	053822	00218
J2000698-00010	Scanner	Fujitsu S1500	057542	00219
J2000698-00011	Telephone	Grandstream GXP2130	20EYZJNE806C477C	00316
J2000698-00012	Telephone	Grandstream GXP2130	20EYZJNE806C46E9	00317

Notes

Verified by HD

Customised Reporting

We offer customised reporting to meet your exact security requirements.

- Each individual item scanned and tracked from the point of collection to completion giving full visibility
- Item description
- Make / model
- Serial number
- Your asset tags

- Data erasure certificate per device (Blancco / WhiteCanyon etc.)
- Weight by item / type
- Photographic evidence of physical destruction
- Inventory of data bearing components before physical destruction / erasure
- Final destination of each item / material type
- What has been re-used / repaired / recycled as materials

Section 7 –

7.1 GDPR Compliance

Revive IT has a complete GDPR Policy, GDPR Evaluation, Data Security Risk Assessment and Risk Treatment Plan in place which is regularly reviewed.

Revive IT will not view, store or collect any data on equipment we process. Data held on equipment is handled with the sole purpose of ensuring erasure / destruction.

Revive IT is registered with the Information Commissioners Office (ICO).