



Asset Disposal Policy (ADP).

Copyright of Information and Documents

The copyright of this document is vested in [Company Name] and is issued in confidence only for the purpose for which it is supplied.

©[Company Name][Year]

Document Ownership

This document is the property of [Company Name] and is issued for the information of such persons who have a need to know its contents in the course of their official duties. Any person finding this document is requested to inform [Company Name] [Telephone Number] and return it safely to the following address stating the circumstances in which it was discovered:

[Company Name]
[Line 1 Address]
[Line 2 Address]
[Postcode]

Document Reference & Author Information

Document Reference : [Document Reference Number & Version]
Author : [Name & Position]
Owner : [Name & Position]
CDS Target Level : **CDS Level 1**

Table of Contents

- Copyright of Information and Documents 1
- Document Ownership..... 1
- Document Reference & Author Information 1
- Table of Contents..... 1
- Document Version Information..... 2
- Links & Dependencies 2
- Register of Applicable Legislation [UK Legislation supplied for information] 2
- Compliance with Corporate Policies..... 2
- Abbreviations 2
- Overview 3
- Purpose 3
- Scope 3
- Responsibilities 3
- Policy 3
- Secure and Controlled Disposal..... 4
- Asset Tracking and Management..... 4
- Physical Security of Assets 4
- Consequences for Non Compliance..... 4



Disciplinary Action.....4

Document Version Information

Version	Changes	Date
1.0	Initial Draft	

Links & Dependencies

Document Title	Reference	Date

Register of Applicable Legislation [UK Legislation supplied for information]

Document Title	Reference	Date
Waste Electrical and Electronic Equipment (WEEE)		Jan 07
The Environment Act		
Data Protection Act 1984		1984
Hazardous Waste Regulations		2005
Electrical Safety Regulations		1994
Basel Convention on Trans-Frontier Shipment of Waste		

Compliance with Corporate Policies

Document Title	Reference	Date

Abbreviations

Terms & Abbreviations	Explanation or Expansion
Asset	'Asset(s)', 'item(s)', 'equipment', throughout this policy and refers to an item with a useful life greater than 12 months, an original purchase value of more than £500 or a residual value of £50.

Overview

1. <Company Name> has many items of technology equipment and devices that store data that belong to both this organisation and potentially our customers. These devices include many types of media in CD-ROMs, DVD, hard drives, USB storage media that hold data that may be considered sensitive from a commercial and private perspective.
2. Before each asset is disposed of, whether to another department or physical destruction by whatever method, consideration should be taken on how the data will be securely erased. <Company Name> will also have to take considerations from a legal standpoint for protecting personal information as well as the proper disposal of electrical equipment.

Purpose

3. This policy has been developed to define the requirements for the proper disposal of surplus or redundant IT assets at <Company Name> and to ensure that data loss or breach of confidentiality does not occur.

Scope

4. This policy applies to all devices with a data storage capacity within <Company Name>.

Responsibilities

5. The Management board of <Company Name> are the owners of this policy and have the responsibility for ensuring that it is rigorously enforced, an asset register and disposal register is created and maintained with any decisions appropriately recorded.
6. Authority for the maintenance of the registers and disposal of assets may be delegated to IT security staff for items up to the value of £500.
7. The director of finance is to give initial authority for any sale of IT assets that exceed £500 market value.

Policy

8. When equipment and devices reach the end of their useful life or requirement and require disposal they are to be sent to the IT Security officer for processing and under no circumstances should disposal be conducted by any other department or staff member.
9. Equipment that has been successfully erased will be made available for employees to purchase with all sales final. No warranty or support will be provided with any equipment sold.
10. Any equipment not in working order or remaining from will be donated or disposed of according to current environmental guidelines.
11. <Company Name> has contracted with several organizations to donate or properly dispose of outdated technology assets. <Company Name> will ensure that each contracted party will be vetted (to an appropriate CDS level) to ensure that the assets will be erased / destroyed appropriately and securely.

Secure and Controlled Disposal

12. All assets that require special handling due to the sensitivity of the data held on the equipment or media are to be identified within the asset register (in red for example) as being subject to special handling procedures. Those assets subject to these procedures are to be erased on site by <Company Name> employees.

Options for Disposal of Assets

13. The following options should be considered for assets identified for disposal:
- a. Transfer to another department
 - b. Private sale
 - c. Destroyed or recycled.

Asset Tracking and Management

14. Each new asset introduced in to the organization is to be recorded in the asset register with all details being completed at the earliest opportunity. This register is to be held by the IT security section and should be checked on a regular basis to check its completeness and accuracy.
15. On the disposal of each asset, the register is to be updated and an appropriate certificate of disposal (if destroyed or moved out of the organisation) raised and filed securely. Any asset management tag should also be removed at this stage.
16. The process of managing assets from cradle to grave will reduce the risk to the organization from fraud and this policy aim to minimize that risk.

Physical Security of Assets

17. Once an asset has been identified for disposal it is to be removed from circulation and placed within a secure area with limited access to IT security personnel that will ensure unauthorized access or reuse.

Consequences for Non Compliance

18. The ramifications of <Company Name> not handling or disposing of data or equipment has both the legal issues surrounding any brought about by 3rd parties as well as customers perception of this organisation and a possible loss of credibility.

Disciplinary Action

19. Any employee found to be disregarding this policy may be subject to disciplinary action against them that may include the termination of their employment.