An Daras Trust
Igniting Curiosity Growing Capabilities

An Daras Multi Academy Trust

Information Security

IT Asset Disposal Policy

The An Daras Multi Academy Trust (ADMAT) Company
An Exempt Charity Limited by Guarantee
Company Number/08156955

Status: **Approved**	
Recommended	
Statutory	Yes
Version	v1.0
Adopted v1.0	**May 2022**
Reviewed/Approved	**25 June 2025**
Next Review	**June 2026**
Advisory Committee	Audit
Linked Documents and Policies	Cyber Security Essentials Accreditation Other ADMAT Cyber/IT/Information Security Policies

1. Purpose

This is an internal policy that defines how An Daras Trust manages the secure and responsible disposal of IT assets. This policy is part of An Daras's aim to ensure an effective IT Asset Management lifecycle.

2. Responsibilities

All users, inclusive of employees, subcontractors and suppliers with direct access to the An Daras information technology systems are expected to conform to this policy.

The An Daras external IT service provider - currently ICT4 - are responsible for providing support to users in complying with this policy.

The Trust Operations Officer is responsible for ensuring that this policy is annually reviewed and that changes are made in the event of legislation change or compliance frameworks such as the Cyber Essentials scheme are updated.

3. Asset Identification

This policy seeks to address the disposal of all of An Daras's information assets that have the capability to record or store data, including:

- PCs
- Laptops
- Servers
- Mobile Phones/Tablets
- Firewalls/Routers/Switches
- Printers/Scanners/Fax Machines
- External Hard Drives

4. Data Backup and Media Sanitisation

An Daras's IT assets should not be disposed of before ensuring that the required data backups and backup tests are done. All media with the capability to record or store data must be properly sanitised according to the sensitivity of the data.

5. Disposal Criteria

An Daras's administration should be notified if any IT equipment needs to be decommissioned. A decision should be made to either reuse/recycle or dispose based on the current Trust Disposal Policy. Before any IT equipment is disposed, a risk-based approach should be taken based on the type of asset and the sensitivity of the data potentially stored.

- **Restricted** - Assets used for the processing and storage of restricted and/or personal data should be identified as high risk because data loss could potentially have significantly detrimental effects. Such assets should be properly sanitised using approved technology or physically destroyed.

- **Confidential** - Assets used for the processing and storage of confidential data should identified as high risk as data loss could also potentially have significantly detrimental effects. Such assets should be properly sanitised using approved technology or physically destroyed.

- **Internal** - Assets used for the processing and storage of internal data should be identified as medium risk. Such assets should be sanitised using approved technology.

- **Public** - Assets used for the processing and storage of public data should be identified as low risk. Such assets should be sanitised and could potentially be reused somewhere else.

6. Third Party Service Providers

Where incapacitated, an approved licensed third-party service provider is contracted to undertake the IT disposal process on behalf of An Daras Trust. This will continue to be monitored to ensure that An Daras's IT disposal standards are met.

7. Environmental Responsibility

An Daras is fully aware of the hazardous impact of incorrectly discarding electronic equipment. Reasonable care should be taken to thoroughly separate and isolate toxic chemicals and components from all electronic equipment before shipment to a landfill.