An Daras Multi Academy Trust

Information Security

Secure Configuration 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	**July 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 ensures consistent secure configuration across all hardware and software applications.

2. Responsibilities

All users, inclusive of employees, subcontractors and suppliers with direct access to our school or Trust's information technology systems are expected to conform to this policy.

An Daras 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. Configuration Principles

An Daras's IT assets are regularly reviewed to keep them aligned to the school's dynamic functional requirements and any unnecessary or unused services are removed. All default credentials are changed to meet the standard detailed in the school's password policy. The Trust adheres to the 'least privilege' principle which ensures that users are granted the least possible privileges adequate enough to carry out work responsibilities. These principles aim to:

- Prevent unauthorised users from collecting, copying and modifying data.
- Prohibit the use of removable media (and other external peripheral devices) where possible, and to scan for malware where use is allowed.
- Prevent the execution of malicious code.

4. Unapproved Hardware and Software

An Daras maintains an asset register which contains a list of approved software applications and hardware. All new software and hardware installations and modifications are approved and continuously monitored by An Daras's IT Service Provider - currently ICT4 and standard users are not permitted to perform any new installations.

5. Access to Systems

The Trust ensures least privilege access to standard users which prevents them from installing additional software or creating additional user accounts. Access to systems strictly requires a strong password as detailed in the password policy. All user accounts are reviewed as stipulated in the school's access control policy and unnecessary accounts are removed or disabled by the Trusts 's IT service provider.

6. Application Allow-listing and Execution Management

An Daras through its IT Service Provider implements application allow-listing for mobile and tablet devices, which explicitly permits only authorised software from the operating system vendor's 'app store' to be installed and executed on school devices where possible. Where allow-listing is not possible, the installation of new scripts and applications is prevented by restricting user privileges.

7. Auto-run/Auto-play

Automatic execution of code is prohibited. On Windows systems, auto-run is disabled using technical controls.