An Daras Multi Academy Trust

Information Security

Password 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 authentication mechanisms for information technology systems used by its staff and subcontractors.

2. Responsibilities

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

An Daras Trust always changes default credentials. Default credentials are changed as a matter of priority upon receiving a new device, factory resetting a device, or commissioning a new service. Accounts and devices are never exposed to the internet before first having their default credentials changed.

4. Strong Passwords

An Daras Trust follows the following principles when creating a new password. A Password Vault or Management portal will be used to support An Daras staff with password security.

- Are never obvious (easy for an attacker to guess)
- Are never commonly used passwords
- Have never been disclosed in a breach (validated using the HaveIBeenPwned service (haveibeenpwned.com)
- Are never re-used when a password expires
- Are never re-used across different accounts

5. Password Disclosure

An Daras employees and contracted staff will never:

- Write down their passwords or encryption keys
- Disclose their password to others

An Daras's IT service provider - currently ICT4 - will never ask employees or contracted staff for their password.

6. Multi-Factor Authentication

All employees and contracted staff at An Daras Trust will ensure that multi-factor authentication is enabled for all devices and services that support this technology.

7. Training

All employees and contracted staff at An Daras are encouraged to remain conversant with password advice from the UK's National Cyber Security Centre.