An Daras Multi Academy Trust

Information Security

Access Control 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 controls access to information assets. It is available, and mandatory to be read by all employees and service providers with access to An Daras information technology systems.

2. Responsibilities

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

All users, inclusive of suppliers with direct access to An Daras information technology systems will take all reasonable care to prevent their access to the system being hijacked by an unauthorised person. This includes ensuring that computers are locked or logged off when left unattended and conforming with the organisation's Password Policy.

Trust Operations Officer and Data Officer are 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.

The Trust CEO is ultimately responsible for organisational compliance to this policy.

3. Principles

An Daras follows the following principles when designing, configuring, administering, and using information systems.

'Least Privilege'

When determining who requires access to information and what they can do with it, An Daras will only grant the privileges required to effectively carry out their job role.

'Need to Know'

When determining who requires access to sensitive information, An Daras will consider who needs access to the data; not who might at some point need access to the data, granting individuals access to highly sensitive documents, rather than groups.

'Access by Job Function or Department'

An Daras provides access to non-sensitive data by job function or department. This is to simplify the privileges structure and to limit the impact in the event of compromise.

'Unique Digital Identities'

Where possible, An Daras always issue unique digital identities to employees and service providers with access to its information technology systems. On most occasions, this is a unique username and password.

'Regular Review of Access'

An Daras will conduct an 'Accounts and Privileges Review' every 6 months.

4. Configuration and Administration

Accounts used to administrate An Daras information technology systems are, where possible, only used for administration purposes. Administrative accounts on operating systems and productivity services will not be used for daily operations.

5. Provisioning, Decommissioning, Promotion and Deletion

User accounts are provisioned, decommissioned, promoted and demoted by means of submitting a request to the Trust external IT service provider - currently ICT4 by the Trust Operations Officer.

6. Special Privileges

An Daras maintains a register of all users with special privileges to information systems. Special Privileges are digital identities with a level of access higher than any standard account. This register is known as the Special Privilege Register and is reviewed during the 'Accounts and Privileges Review' every 6 months. Maintaining the Special Privilege Register allows An Daras to provide additional controls to higher risk digital identities.