An Daras Multi Academy Trust

Information Security 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

As part of An Daras Trust's responsibility to safeguard its information assets, this information security policy aims to preserve the confidentiality, integrity and availability of these assets. A rigorous information security policy sets a solid information security foundation, implementing industry standard controls for secure information asset management. This document provides an overview of the Trust's information security practices and the associated set of policies necessary to ensure adequate controls, processes are applied to safeguard the school's information assets.

2. Responsibilities

All employees with direct access to the An Daras Trust information technology system are expected to conform to this policy.

The Trust's IT Service Provider - currently ICT4 - are responsible for providing support in complying with this policy.

CEO and COO 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. Definitions

'Availability'
Readiness to access information resources when needed.

'Confidentiality'
Access controls to information assets to ensure that only authorised users with the right access privileges have access to the appropriate resources.

'Information Asset'
Any valuable resources or components in the interest of the school's strategic requirements.

'Integrity'
Information preservation to prevent any unauthorised modifications ensuring correctness and completeness.

4. Information Security Principles

To assure that systems are secure, three key information security principles must be guaranteed, namely confidentiality, integrity and availability. A violation of any of these principles compromises the security of a computer system and such may lead to severe unintended consequences. These principles aim to:

- make provision for the availability of information where there is a legitimate reason to do.
- ensure the integrity of information is always maintained.
- guide technical and non-technical controls and measures that ensure information is protected from unauthorised access using authentication and authorisation methods.

5. Sub-policies

Lower-level policies referred to by this policy provide granular details of the controls, procedures and processes implemented by An Daras Trust to support the aim of this policy. These include the:

- Anti-Malware Policy
- Access Control Policy
- Firewalling Policy
- Patch Management Policy
- Password Policy
- Secure Configuration Policy

6. Information Governance

An Daras Trust's CEO or Trust Operations Officer are responsible for the oversight in the production, maintenance and distribution of cybersecurity policies. This policy will undergo regular reviews and all significant changes are approved by the board to ensure internal consistency.

School Administration/Board responsibilities

- Ensuring that any changes made to this policy and any related policies are effectively communicated to all users.
- Ensuring staff understand and adhere to this policy and any related sub-policies.
- Reporting all instances of non-compliance.

Other users

Any person who uses, has access to or interacts with the school's information systems in any way possible should be responsible for:

- Conforming to the acceptable use of the school's information assets.
- Adhering to this information security policy and all related sub-polices.
- Reporting all suspected cyber security incidents through the approved procedure as stipulated in the school's cyber security incident management plan.

7. Incident Management and Response

An Daras Trusts' cyber security incident management and response plan provides guidance on what the school regards to be a cybersecurity incident, including methods of reporting. All suspected information security breaches need to be reported and investigated. All significant security recommendations must be incorporated into the risk action plan. In the case of a significant disruption to the school's information systems, the business continuity plan should be invoked to ensure a systematic, swift and effective recovery process in the best interest of the school.

8. Acceptable System Use

The use of the school's information assets and systems by authorised users must be in a lawful and safe manner. An Daras Trust information assets shall only be used for supporting learning activities, administration tasks and any other task that is directly or indirectly related to the school's interest. Any use of the school's information resources for personal gain or any other business might require the approval of the CEO.

9. Information Classification

An Daras Trust understands that not all information is equal, and thus the need for a sensitivity classification. This is important so as to adequately protect information based on value.

10. System Change Management

Changes to An Daras Trust's functional requirement that may call for modifications to existing information systems might affect the information security controls and processes and thus risk management controls may need to be implemented accordingly. Appropriate security provisions need to be considered before any significant changes are made to the school's network.

11. Breach of Policy

Any form of violation towards this policy may call for disciplinary measures the Trust's staff disciplinary procedure.