An Daras Trust

Igniting Curiosity Growing Capabilities

An Daras Multi Academy Trust

Information Security

IT Acceptable Use 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	**5 July 2023**
Next Review	**July 2024**
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 that users understand the acceptable, and non-acceptable use of information technology assets, resources, and systems.

This policy seeks to provide guidance that promotes proper, legal and responsible use of An Daras Trust's information technology assets.

In addition, this policy supports the Trust and its school in ensuring that staff are aware of their responsibilities in using technology according to the following legislation:

- Communications Act
- Computer Misuse Act
- Computer, Copyright Software Amendment Act
- Copyright, Designs and Patents Act
- Criminal Justice and Public Order Act
- Data Protection Act
- Defamation Act
- Electronic Communications Act
- Freedom of Information Act
- General Data Protection Regulation (EU GDPR)
- Human Rights Act
- Malicious Communication Act
- Regulation of Investigatory Powers Act
- Trade Marks Act

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.

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

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

An Daras Board of Directors are responsible for the review and ratification of this policy.

3. General Principles

3.1 Keeping passwords secret

All users with access to An Daras IT systems, services and devices must keep credentials (usernames, passwords and encryption keys) secret in accordance with the Trust Password Policy.

3.2 Locking devices when leaving unattended

All users with access to An Daras IT systems, services and devices must 'lock' devices them when leaving the room or breaking line of sight.

3.3 Physically taking care of devices

All users with access to An Daras IT systems, services and devices must take all reasonable precautions to prevent loss, theft or damage to them.

3.4 Not using school/trust devices for inappropriate personal use

All users with access to An Daras IT systems, services and devices must do so without:

- Using inappropriate or offensive language, as defined within the Trust Staff Handbook and/or Code of Conduct
- Bullying or intimidating others.
- Disclosing secrets or personal data in accordance with the An Daras data protection policy.
- Using them for personal entertainment or activities not related to Trust or school business without prior consent.

3.5 Not using school/trust devices to break the law

All users with access to An Daras IT systems, services and devices must take all reasonable precautions to prevent infringement of legislation identified within the purpose of this policy.

3.6 Using IT in accordance with Safeguarding Policy

All users with access to An Daras IT systems, services and devices must use them to support the Trust Child Protection and Safeguarding Policy.

3.7 Using IT in accordance with Data Protection Policy

All users with access to An Daras IT systems, services and devices must use them to support the Trust Data Protection Policy.

3.8 Not avoiding technical controls designed to keep systems secure

All users with access to An Daras IT systems, services and devices must operate them in accordance with the way in which they were designed by the vendor and the Trust external IT Service Provider - ICT4. This includes, but is not limited to, the 'rooting' or 'jailbreaking' of devices.

3.9 Not using IT systems, services or devices that haven't been approved

All users with access to An Daras IT systems, services and devices must not use IT systems, services or devices that haven't been approved by An Daras Trust's external IT Service Provider - ICT4. We refer to this as 'shadow IT'.

3.10 Using IT in accordance with our Cyber Security Incident Management Plan

All users with access to An Daras IT systems, services and devices must use them to support the Trust and school Cyber Security Incident Management Plan which includes reporting suspicious activity and confirmed incidents to the Trust Operations Officer and them to the Trust external IT Service Provider - ICT4.

4. Internet Access

An Daras provides internet access to all staff and pupils for usage relating to school business or teaching and learning.

Internet access is filtered to prevent use that does not support school business or teaching and learning. This is done to reduce the risk of the An Daras devices becoming infected with malicious software (malware), in addition to supporting the An Daras Child Protection and Safeguarding Policy, and the Trust On-Line Safety Policy

An Daras expects all users to respect the web content filtering system, to not purposefully circumvent it, and to report any inappropriate websites to the Trust Operations Officer and the Trust external IT service provider - ICT4.

Where additional credentials (such as passwords) are required specifically to access the internet (this includes connecting devices to the Trust wireless network for internet access) they must be kept secret and in accordance with the An Daras Password Policy.

Intentional inappropriate use may result in further restriction or removal of internet access. Severe or continuous inappropriate use may result in disciplinary action.

5. Unapproved Software

Unapproved software has not been checked for malware, authenticity, compatibility and compliance.

Software that has not already been installed on An Daras devices are prohibited. This includes running software that doesn't require installation such as 'portable applications' that are able to be run from removable media or directly from download (for example, email attachments).

6. Bring Your Own Device (BYOD)

'BYOD' is the use of personally owned devices for work purposes. This includes mobile phones and tablets that are used for accessing any An Daras data, including emails.

An Daras allows BYOD, however personally owned devices must first be approved by the Trust.

When connecting personally owned devices to An Daras wireless network, they must always be connected only to the wireless network <<Wifi Network SSID (Name)>> which has been segregated from critical An Daras Trust or school networks. An Daras Trust and its external IT service provider - ICT4 will first assess the device for compliance with the Trust Information Security Policy and provide support in connecting it to the dedicated wireless network for internet access.

Only devices that meet the Trust security requirements will be approved for BYOD.

BYOD devices must not be used for:

- Contacting pupils or their families for any reason other than in professional capacity.
- Processing (this includes storing) images and videos of pupils or their families.
- Processing (this includes storing) any other personal data relating to colleagues, pupils or their families.

- Using software that hasn’t been approved by the Trust to process Trust or school level data.

7. Data Security and Privacy

Users of IT at An Daras must always do so in accordance with the Trust Data Protection Policy.

Removable media (such as USB drives, SD Cards and CDs/DVDs) are strongly discouraged and, where possible, have been prevented from being used with technical controls.

Users of IT at An Daras are granted access to data only on a ‘need to know’ basis in accordance with the Trust’s Access Control Policy.

Users of IT at the Trust have a responsibility for facilitating security updates on their devices. In practice, this means regularly restarting devices, especially when prompted to do so by the device.

Users of IT at An Daras have a responsibility for notifying the external IT Service Provider - ICT4 if they suspect a breach of data security, or the Trust Data Protection Officer if they suspect a breach involving personal data.

An Daras external IT Service provider - ICT4 ensures that the Trust IT networks use an appropriate level of encryption. Users of IT at An Daras have a responsibility for using the encryption tools made available to them to encrypt sensitive files leaving the Trust’s network by upload or email.

8. Unacceptable Use

An Daras information assets should not, under any circumstances be used for the acquisition, distribution, creation, processing, or storage of:

- any form of material that can potentially be used to promote discrimination based on but not limited to disability, race, sexual orientation or gender.
- any form of material that can be used to bully, victimise, or harass others.
- unlawful material that violates intellectual property and privacy rights.
- any form of material that directly or indirectly seek to promote unlawful actions that may be threatening, extremist, or defamatory.
- any form of material that may be regarded as obscene, indecent or offensive.

User Credentials and Password security

- All issued user credentials should be kept safe and secret in accordance with the Trust Password Policy, it is unacceptable to display passwords or store them in a location that is easily accessible, for example, writing down passwords and sticking them on a computer or desk.
- All users are required to change passwords when there is suspicion that they may have been involved in a data breach, or when requested by the Trust’s external IT Service Provider - ICT4.
- Unless explicitly authorised by An Daras external IT Service Provider - ICT4, user accounts should never be shared. A user should not log into a computer system to access resources or services using another user's credentials.

Email

- All users should be aware of the risks associated with using email as described in the An Daras cyber security awareness programme and should apply the techniques described within this training when handling emails.
- It is unacceptable to knowingly send or attempt to send an email with a malicious attachment or link with the intent of causing harm or disruption.
- As described in the cyber security awareness programme, all users should be careful to check received emails for suspicious links or attachments before clicking. All suspicious emails should be reported to An Daras Trust's phishing reporting email address using the method described in the cyber security awareness programme.

Internet

As previously explained in Section 4, the main purpose of An Daras internet connection is to support teaching, learning, and administrative operations, and any activity that might disrupt this is unacceptable.

- Accessing the internet for personal use or non-work-related purposes is acceptable but limited. All users shall be responsible for the websites they visit and the activities they conduct on the internet.
- It is unacceptable to indulge in any personal or non-work activity that consumes significant network bandwidth such as downloading very large files or live streaming.

School devices and networks

- It is unacceptable to attempt to bypass network security controls or filters.
- Where devices are shared, users should log out to prevent other users from using their credentials.
- Where the Trust issues a device intended to be used for remote working, only approved users should use such devices. If user-owned devices are permitted to externally access An Daras's data or services, only approved users should use this access.
- It is unacceptable to download, store, copy, distributed unlicensed material which may be subject to intellectual property and copyright laws.
- It is unacceptable to use tools that may degrade the network, scan ports, intercept network traffic, scan for vulnerabilities, reroute network traffic or alter the network configuration without approval.
- It is unacceptable to use devices in contravention of the Computer Misuse Act 1990, which makes the following an offence:
    - Unauthorised access to computer material. This refers to entering a computer system without permission (hacking).
    - Unauthorised access to computer materials with intent to commit a further crime. This refers to entering a computer system to steal data or destroy a device or network (such as planting a virus).
    - Unauthorised modification of data. This refers to modifying or deleting data, and also covers the introduction of malware or spyware onto a computer (electronic vandalism and theft of information).
    - Making, supplying or obtaining anything which can be used in computer misuse offences.

9. Monitoring

An Daras reserves the right to record and monitor the use of its IT network and facilities, subject to the Regulation of Investigatory Powers Act, for reasons including:

- Ensuring IT services and facilities remain effective and operational.
- The prevention, detection and investigation of a breach of the law, this policy or other Trust policies, procedures or standards.
- Investigation of suspected misconduct by users (inclusive of staff and pupils) such as plagiarism.
- Gathering information to respond to Data Subject Access Requests.
- Investigation of suspected cyber security incidents and data breaches.
- Conducting training exercises and preparing for information security incidents.

This includes, but is not limited to, monitoring (and, where appropriate, recording) of:

- Internet browsing data.
- Internet connection data.
- Communications (inclusive of email transactions and telephone calls).
- User device access and activity logs.
- User data access and activity logs.
- Bandwidth usage.

Only authorised personnel from An Daras's external IT Service provider - ICT4 may record and monitor the use of its IT network and facilities.

10. Breach of Policy

Any form of violation towards this policy may call for disciplinary measures under An Daras staff disciplinary policies.