An Daras Trust
Igniting Curiosity Growing Capabilities

An Daras Multi Academy Trust

Information Security

Firewalling 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 manages firewalling technology and mechanisms for information technology systems used by its staff.

2. Responsibilities

Trust Operations Officer and Trust IT Service Provider - currently ICT4 - are ultimately responsible for organisational compliance to this policy.

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

An Daras Trust's IT service provider - currently ICT4 - are responsible for providing support 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 always changes default credentials on network boundary firewalls. 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 principles outlined in its Password Policy when changing network boundary firewall passwords.

5. Network Boundary Firewalls

The Trust requires that Network Boundary Firewalls have the following capabilities supported and enabled:

- HTTP and HTTPS proxy
- Gateway antivirus
- Multi-WAN with failover functionality (if multiple WANs are installed)
- Intrusion Prevention System
- Advanced Persistent Threat protection

6. Personal Firewalls (School Computers)

An Daras requires that the school or Trust's firewall software host-based firewall is enabled on all network connected endpoints that have such ability.

7. Personal Firewalls (Home-based and Bring-your-own-device Computers)

An Daras requires that the school or Trust's Firewall Software host-based firewall, or at least the built-in Windows or Mac OS host-based firewall is enabled on all network connected endpoints that have such ability.

8. Blocked Services

An Daras does not allow services that are identified by the NCSC, GCHQ or the Cyber Essentials scheme as vulnerable to be allowed to connect through firewalls. Services that are identified as vulnerable are as follows:

- SMB
- TELNET
- NetBIOS
- tFTP
- RPC
- rLogin
- RSH
- rExec
- HTTP

9. Internet Access

Access to the internet from the school or Trust Local Area Networks is granted only to devices that require access as an operational necessity. Restriction of access is implemented by a ‘Blanket Deny’.

10. Maintaining the Register

An Daras - via its current IT Service Provider - maintains a register of all approved firewall rules permitted on Boundary Firewalls using the built-in access control list on the device, adding clear justification in the description of each rule. Rules are approved only by the Trust Operations Officer based on guidance from the current IT Service Provider.