Secure Schools

Information Security Policy

Firewall Policy

1. Purpose

This is an internal policy that defines how Aspire Federation manages firewalling technology and mechanisms for information technology systems used by its staff.

2. Responsibilities

Emma Hickling is ultimately responsible for organisational compliance to this policy.

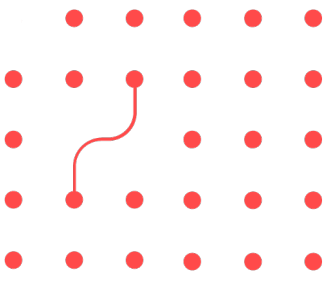
All users, inclusive of employees, subcontractors and suppliers with direct access to the Aspire Federation's information technology systems are expected to conform to this policy.

Aspire Federation's Cantium are responsible for providing support in complying with this policy.

Emma Hickling 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

Aspire Federation 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

Aspire Federation follows the principles outlined in its Password Policy when changing network boundary firewall passwords.

5. Network Boundary Firewalls

Aspire Federation 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)

Aspire Federation requires that the smooth wall 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)

Aspire Federation requires that the smooth wall 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

Aspire Federation 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 Aspire Federation 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

Aspire Federation 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 Emma Hickling.

Approved by	
Date Approved	
Date of Next Review	