Secure Configuration Policy

1. Purpose

This is an internal policy that defines how Aspire Federation ensures consistent secure configuration across all hardware and software applications.

2. Responsibilities

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 IT service provider are responsible for providing support to users 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. Configuration Principles

Aspire Federation's IT assets are regularly reviewed to keep them aligned to the school’s dynamic functional requirements and any unnecessary or unused services are removed. All default credentials are changed to meet the standard detailed in the school’s password policy.

Aspire Federation adheres to the ‘least privilege’ principle which ensures that users are granted the least possible privileges adequate enough to carry out work responsibilities. These principles aim to:

- Prevent unauthorised users from collecting, copying and modifying data.
- Prohibit the use of removable media (and other external peripheral devices) where possible, and to scan for malware where use is allowed.
- Prevent the execution of malicious code.

4. Unapproved Hardware and Software

Aspire Federation maintains an asset register which contains a list of approved software applications and hardware. All new software and hardware installations and modifications are approved and continuously monitored by Aspire Federation's Zulogic/ Cantium and standard users are not permitted to perform any new installations.

5. Access to Systems

Aspire Federation ensures least privilege access to standard users which prevents them from installing additional software or creating additional user accounts. Access to systems strictly requires a strong password as detailed in the password policy. All user accounts are reviewed as stipulated in the school’s access control policy and unnecessary accounts are removed or disabled by Aspire Federation 's Zulogic/ Cantium .

6. Application Allow-listing and Execution Management

Aspire Federation implements application allow-listing for mobile and tablet devices, which explicitly permits only authorised software from the operating system vendor's 'app store' to be installed and executed on school devices where possible. Where allow-listing is not possible, the installation of new scripts and applications is prevented by restricting user privileges.

7. Auto-run/Auto-play

Automatic execution of code is prohibited. On Windows systems, auto-run is disabled using technical controls.

Approved by	
Date Approved	
Date of Next Review	