Secure Schools

Information Security Policy

Access Control Policy

1. Purpose

This is an internal policy that defines how Aspire Federation controls access to information assets. It is available, and mandatory to be read by all employees and service providers with access to Aspire Federation's information technology systems.

2. Responsibilities

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

All users, inclusive of suppliers with direct access to Aspire Federation's information technology systems will take all reasonable care to prevent their access to the system being hijacked by an unauthorised person. This includes ensuring that computers are locked or logged off when left unattended and conforming with the organisation’s Password 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.

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

3. Principles

Aspire Federation follows the following principles when designing, configuring, administering, and using information systems.

- **‘Least Privilege’**
  When determining who requires access to information and what they can do with it, Aspire Federation will only grant the privileges required to effectively carry out their job role.
- **‘Need to Know’**
  When determining who requires access to sensitive information, Aspire Federation will consider who needs access to the data; not who might at some point need access to the data, granting individuals access to highly sensitive documents, rather than groups.
- **‘Access by Job Function or Department’**
  Aspire Federation provides access to non-sensitive data by job function or department. This is to simplify the privileges structure and to limit the impact in the event of compromise.
- **‘Unique Digital Identities’**
  Where possible, Aspire Federation always issue unique digital identities to employees and service providers with access to its information technology systems. On most occasions, this is a unique username and password.
- **‘Regular Review of Access’**
  Aspire Federation will conduct an ‘Accounts and Privileges Review’ every 6 months.

4. Configuration and Administration

Accounts used to administrate Aspire Federation's information technology systems are, where possible, only used for administration purposes. Administrative accounts on operating systems and productivity services will not be used for daily operations.

5. Provisioning, Decommissioning, Promotion and Deletion

User accounts are provisioned, decommissioned, promoted and demoted by means of submitting a request to the Zulogic/ Cantium by Emma Hickling.

6. Special Privileges

Aspire Federation maintains a register of all users with special privileges to information systems. Special Privileges are digital identities with a level of access higher than any standard account. This register is known as the Special Privilege Register and is reviewed during the 'Accounts and Privileges Review' every 6 months. Maintaining the Special Privilege Register allows Aspire Federation to provide additional controls to higher risk digital identities.

Approved by	
Date Approved	
Date of Next Review	