**Nautilus Education – Access Control Policy**

**1. Purpose**

This policy defines the principles and procedures for controlling access to Nautilus Education systems and data. It ensures that only authorised individuals can access personal data and system functions, in line with legal, contractual, and operational requirements.

**2. Scope**

This policy applies to all staff, contractors, and users of the Nautilus Education platform, including access via desktops, laptops, tablets, and mobile devices.

**3. Access Principles**

* **Least Privilege**: Users are granted the minimum level of access required to perform their role.
* **Role-Based Access Control (RBAC)**: Permissions are assigned based on defined user roles (e.g. observer, administrator).
* **Need-to-Know Basis**: Access to personal data is restricted to those with a legitimate operational need.

**4. User Authentication**

* All users must authenticate using a valid work email address and secure password.
* Multi-factor authentication (MFA) is enforced for administrative accounts.
* Passwords must meet minimum complexity requirements and be changed periodically.

**5. Account Management**

* User accounts are created by authorised administrators using staff names and work email addresses.
* Accounts are reviewed regularly to ensure accuracy and relevance.
* Inactive or obsolete accounts are disabled or deleted in accordance with retention policies.
* Users must notify administrators of changes to their role or employment status.

**6. Access via Portable Devices**

* Access is permitted via secure mobile phones, tablets, and laptops.
* Devices must be protected by passwords, PINs, or biometric authentication.
* Users must not store personal data locally on devices.
* Public or shared devices must not be used to access the platform.
* Lost or stolen devices must be reported immediately for access revocation.

**7. Monitoring and Audit**

* All access to the platform is logged and monitored for security and compliance.
* Logs include login attempts, data access, and administrative actions.
* Audit trails are retained in accordance with data protection and operational policies.

**8. Access Revocation**

* Access is revoked immediately upon termination of employment, role change, or breach of policy.
* Administrators may suspend or restrict access where misuse or risk is identified.

**9. Third-Party Access**

* No third-party access to personal data is permitted.
* AWS, as the hosting provider, does not access customer data and operates under strict compliance controls.

**10. Policy Review and Governance**

* This policy is reviewed annually or upon significant system or regulatory changes.
* Compliance with this policy is mandatory for all users and enforced through system controls and administrative oversight.