POLICY NAME:	Privacy and Information Security for Learners' Records	POLICY NO.	8.6A

DOCUMENT HISTORY:	EFFECTIVE DATE:	DATE OF LAST REVISION:
	8/30/2024	N/A
	DOCUMENT OWNER/ENFORCER:	LAST REVISED BY:
	Tim Oppenheim, Chief Information Officer	N/A
	APPROVED BY:	DATE OF APPROVAL
	Robin Essandoh, Chief Financial Officer	8/30/2024

PURPOSE:

This section outlines the purpose of the policy.

This policy outlines the measures taken by The Academy a NHSA to ensure the privacy and security of learners' records. It is designed to protect the confidentiality, integrity, and availability of learner information while facilitating appropriate access and use.

SCOPE:

This section outlines the scope of the policy, including the areas, departments, or sectors to which it applies

This policy applies to all learner records maintained by The Academy at NHSA, including but not limited to personal information, enrollment data, assessment results, certificates, and transcripts.

PRIVACY POLICY:

Security of Learner Information in Our Systems

Data Encryption

- The platforms NHSA uses to collect learner data (Canvas by Instructure and Litmos) are SOC2 compliant and follow the stringent requirements therein. SOC 2 reports focus on controls addressed by five semi-overlapping categories called Trust Service Criteria which also support the CIA triad of information security:

1. Security - information and systems are protected against unauthorized access and disclosure, and damage to the system that could compromise the availability, confidentiality, integrity and privacy of the system.
    - Firewalls
    - Intrusion detection
    - Multi-factor authentication

PRIVACY POLICY:

2. Availability - information and systems are available for operational use.
    - Performance monitoring
    - Disaster recovery
    - Incident handling
3. Confidentiality - information is protected and available on a legitimate need to know basis. Applies to various types of sensitive information.
    - Encryption
    - Access controls
    - Firewalls
4. Processing Integrity - system processing is complete, valid, accurate, timely and authorized.
    - Quality assurance
    - Process monitoring
    - Adherence to principle
5. Privacy - personal information is collected, used, retained, disclosed and disposed according to policy. Privacy applies only to personal information.
    - Access control
    - Multi-factor authentication
    - Encryption

Access Control

- Access to learner information within the NHSA system is restricted to authorized personnel only.
- Each staff member is assigned a unique user ID and strong password.
- Multi-factor authentication is required for accessing learner data within our system.

System Security

- SOC2 compliance requires secure systems and regular audits to ensure security is maintained over time. All 3rd party software NHSA uses is SOC2 compliant. See above for details.

Secure Maintenance of Learner Information

Data Retention

- Learner records will be retained only for as long as necessary, in accordance with legal and accreditation requirements.

Data Backup

- All 3rd party platforms are SOC2 compliant, and therefore, meet the stringent requirements therein related to data backup processes. See above for details.

Release of Learner Information

Learner Access

- Learners have the right to access their own records upon request.
- Identity verification procedures must be followed before releasing information to learners.

Third-Party Requests

- Learner information will not be released to third parties without explicit written consent from the learner, except where required by law.

PRIVACY POLICY:

Secure Release of Records

Certificate and Transcript Issuance

- Certificates and transcripts will be issued securely upon completion of a learning event.
- Digital certificates will be issued through a secure, blockchain based platform with verifiable authenticity.

Staff Training and Compliance

It is standard practice for all staff engaging with learner data to follow basic privacy policies.

Incident Response

- A data breach response plan is in place to address any potential security incidents.
- Any suspected or actual breaches of learner data must be reported immediately to the designated Data Protection Officer.

Policy Review

This policy will be reviewed annually and updated as necessary to ensure ongoing compliance with relevant laws and best practices.

TERMS AND DEFINITIONS:

TERM	DEFINITION

NONCOMPLIANCE STATEMENT:

Any violations of this policy must be reported promptly to the administrator responsible for policy oversight. The administrator will investigate all reported breaches. Consequences for non-compliance will be determined by senior management and may include disciplinary action depending on the severity and frequency of the violation.

RELATED POLICIES AND OTHER REFERENCES:

This sections provides links to related policies and other references.

8.5A SOP | Digital Portfolio Access and Certificate Management

REVISION HISTORY:

This section records changes made to the document, including the date, summary of changes, and names of approvers			
VERSION	**APPROVER** **Name/Position**	**REVISION DATE**	**SUMMARY OF CHANGES**