



Privacy and Confidentiality Policy

Policy Name

Privacy and Confidentiality Policy

Version

3.0

Effective Date

1 July 2025

Review Date

1 July 2026

Policy Owner

Compliance Manager / CEO

Related Standards

Outcome Standards 1.6, 4.2, 4.3; Compliance Requirements 5, 6, 11, 16; Australian Privacy Principles (APPs 1–13)

1. Purpose

To ensure that NUA Learn complies with the Australian Privacy Principles (APPs) and RTO Standards by protecting the confidentiality, integrity and lawful use of personal information from learners, staff and stakeholders.

2. Scope

This policy applies to:

- All learners, staff, contractors and third-party partners
- All personal, sensitive and health information collected or held by NUA Learn
- All physical and electronic recordkeeping systems and communication methods

3. Definitions

- Personal Information: Data identifying an individual (e.g. name, address, USI)
- Sensitive Information: Health, disability, ethnicity or criminal history
- Confidentiality: Obligation to protect private information from unauthorised disclosure
- APP: Australian Privacy Principles from the Privacy Act 1988
- APP Entity: An organisation bound by the APPs

4. Policy Statement

NUA Learn ensures that:

- A clearly expressed and up-to-date APP Privacy Policy is available
- Individuals may use pseudonyms where lawful and practical (APP 2)
- Personal data is only collected when necessary and by lawful and fair means (APP 3–5)
- Unsolicited data is destroyed or de-identified (APP 4)

- Data is only used/disclosed for authorised purposes or legal obligations (APP 6)
- Individuals can opt out of direct marketing where applicable (APP 7)
- Overseas disclosures comply with security and consent obligations (APP 8)
- Government identifiers are only used under lawful provisions (APP 9)
- Data is accurate, complete and up to date (APP 10)
- Reasonable steps are taken to protect data from misuse/loss (APP 11)
- Individuals can request access to or correction of their information (APP 12–13)

5. Procedure

1. Collect data via secure authorised methods (e.g. enrolment forms, Teams/One Note, aXcelerate)
2. Provide APP-compliant Privacy Notifications at the point of collection
3. Securely store records using encrypted digital systems and password-protected files
4. Restrict data access based on defined roles and job function
5. Document and respond to suspected breaches using the Data Breach Response Plan
6. Allow individuals to access or request corrections to personal records

6. Responsibilities

Role	Responsibility
Compliance Manager	Ensure privacy compliance and manage breaches
CEO	Guarantee policies, contracts and systems uphold privacy standards
Trainers and Staff	Handle data lawfully, ethically and securely
IT/System Admin	Implement and maintain data protection systems

7. Monitoring and Review

- Data handling is audited as part of the annual internal audit schedule
- Breaches, complaints or near misses are investigated and reported
- Policy is reviewed annually or when legislative or operational changes occur
- Updates are version controlled in line with the Document Control Framework

8. Related Documents

- Records Management Policy
- Enrolment Form and Privacy Notice
- Data Breach Response Plan
- Complaints and Appeals Policy
- Staff Code of Conduct
- LMS/SMS Backup Policy
- IT Systems Access Matrix
- Secure File Naming Protocol
- Policy Review and Document Control Framework

9. References

- Australian Privacy Act 1988
- Australian Privacy Principles 1–13
- OAIC Guidance: www.oaic.gov.au