PO-58 USI CREATION AND PRIVACY RISK MANAGEMENT POLICY

1. Purpose

This Policy outlines the IAME RTO No. 90409 Board of Directors' formal resolution to prohibit the creation of Unique Student Identifiers (USIs) by any RTO personnel, including the CEO or any High Managerial Agent (HMA), on behalf of students. This Policy prioritises the protection of personal information and compliance with the Privacy Act and Student Identifiers Act.
Legislative Alignment:

- *Student Identifiers Act 2014 (Cth)*
- *Privacy Act 1988 (Cth)*
- *Standards for RTOs 2025*
- *Office of the Student Identifiers Registrar Guidance Notes*

2. Scope

This policy applies to:

- All prospective and current students of IAME RTO No. 90409
- All staff, contractors, and volunteers including the RTO CEO and HMAs
- Any external parties acting on behalf of the RTO

3. Policy Statement

In accordance with the *Student Identifiers Act 2014* and the *Privacy Act 1988*, the IAME RTO Board of Directors recognises that the collection, handling, and storage of personal and identity information to create a USI presents an unacceptable risk to the privacy and data security of students and to the compliance status of the RTO.

Board Directive – No USI Creation by RTO

As resolved by the IAME Board, and in accordance with bespoke RTO governance frameworks and the RTO's legislative obligations: "The IAME RTO CEO, HMAs, Trainers, Assessors or other staff members must not create or offer to create a USI for any student. This position applies regardless of whether the student provides consent or requests assistance".

4. Rationale and Risk Considerations

4.1 Identity Document Retention Risk

Under section 11 of the *Student Identifiers Act 2014*, identity documents and personal data used for USI creation must not be retained, unless required by law. Storing such information - even temporarily - creates a high risk of non-compliance and security breaches.

4.2 Student Autonomy and Digital Capability

The USI system is designed for direct student access and use. All students are expected to have the basic digital capability to create or recover their own USI, supported by usi.gov.au guided portal and recovery services. Where digital support is needed, students should be referred to the portal rather than the RTO handling the process.

4.3 Misconduct, Privacy Breach and Legal Liability

Any failure to obtain appropriate consent, mishandling of ID documents, or storage of unauthorised personal information can result in:

- Misconduct allegations under the **PO-53 Misconduct Policy**
- Reportable privacy breaches under the Notifiable Data Breach scheme
- Reputational damage and regulator non-compliance

5. Student Guidance and Support Protocols

While the IAME RTO will not create a USI, it will provide support by:

- Guiding students to the USI Creation Portal
- Providing written instructions or supervised digital access (without handling personal data)
- Referring to the **PR-19 Digital Evidence and Photo Consent Procedure** - to inform students of digital risk mitigation

PO-58 USI CREATION AND PRIVACY RISK MANAGEMENT POLICY

6. Policy Exceptions

There are no exceptions to this policy.

Any staff member found to have created, attempted to create, or encouraged the creation of a USI on behalf of a student may be subject to disciplinary action under the **PO-53 Misconduct Policy**, and the matter may be referred to appropriate regulators.

7. Records and Compliance Management

While the IAME RTO may collect and store the USI itself (once created by the student), the following controls must be applied:

- The USI is stored within a secure student management system with access logging
- No identity documents (passports, licences, Medicare cards) are to be copied, emailed, scanned, or retained
- All USI records are managed under the terms of the **PO-10 Privacy Policy** and the **PO-44 Confidentiality Policy** and **PO-61 Non-Disclosure Policy**

8. Communication of Policy

This policy shall be:

- Clearly communicated to all staff during onboarding and annual compliance training
- Included in the Student Handbook and website
- Reaffirmed through any procedural documents or forms that reference USI

9. Related Documents and Frameworks

Document	Relevance
PO-10 Privacy Policy	Storage, handling, and consent of personal data
PO-44 Confidentiality Policy **PO-61 Non-Disclosure Policy**	Ensures appropriate use of sensitive student data
PR-19 Digital Evidence and Photo Consent Procedure	Covers digital privacy during RTO-administered support
PO-53 Misconduct Policy	Sets disciplinary parameters for breach of obligations
Standards for RTOs 2025	Clause 7.5 – USI Collection and Reporting

11. Monitoring and Review

This policy will be reviewed annually by the IAME Board of Directors or as required due to legislative or regulatory changes.

Document Control Information and History				
Version	**Date**	**Created / Modified**	**Created by**	**Approved by**
V1.0	31/07/2025	Created	Peter Blanshard Chief Executive Officer – IAME / RTO	Jeffrey Richards Chairperson: IAME Board of Directors