RTO Policy for Storing Third-Party Evidence

Purpose

This policy outlines the procedures for storing third-party evidence collected as part of the Recognition of Prior Learning (RPL) process. The purpose of this policy is to ensure the security, confidentiality, and integrity of learner information and evidence.

Scope

This policy applies to all staff involved in the RPL process, including assessors, trainers, and administrative staff.

Policy Statement

The RTO will:

1. **Secure Storage:**
- Store all third-party evidence in a secure, locked location, either physical or digital.
- Implement appropriate security measures to protect against unauthorised access, loss, or damage.
2. **Confidentiality:**
- Treat all third-party evidence as confidential and only disclose it to authorised personnel.
- Obtain consent from learners before sharing their personal information with third parties.
3. **Retention Period:**
- Retain third-party evidence for a minimum of **7 years** after the completion of the RPL process or the finalisation of any related legal proceedings.
- Comply with all relevant legislation and regulatory requirements regarding record-keeping.
4. **Access and Retrieval:**
- Establish clear procedures for accessing and retrieving third-party evidence.
- Limit access to authorised personnel only.
5. **Disposal:**
- Develop a secure and confidential method for disposing of third-party evidence, such as shredding or secure electronic deletion.
- Ensure that all personal information is permanently removed or destroyed.
6. **Regular Review:**
- Regularly review and update this policy to ensure its continued relevance and effectiveness.
- Conduct internal audits to monitor compliance with this policy.

Procedures

1. **Collection of Evidence:**
- Collect third-party evidence directly from learners or through secure electronic transfer.
- Verify the authenticity and relevance of the evidence.
2. **Storage of Evidence:**
- Store physical evidence in locked cabinets or safes.
- Store digital evidence on secure servers with appropriate access controls.
- Regularly back up digital evidence to prevent data loss.
3. **Retrieval of Evidence:**
- Implement a system for tracking and retrieving evidence when needed.
- Ensure that only authorised and relevant personnel can access the evidence.
4. **Disposal of Evidence:**
- Follow secure disposal procedures to protect learner privacy.
- Document the disposal of evidence.