



ROYAL
INTERNATIONAL
COLLEGE

RTO Code: 46036 | CRICOS Code: 04153F

INFORMATION TECHNOLOGY POLICY AND PROCEDURE

☎ +61 0461414506 ☎ +61 491 138 564

🌐 www.royalinternational.edu.au

✉ support@royalinternational.edu.au

✉ admissions@royalinternational.edu.au

📍 **Melbourne** (Head Office)

Suite 2, Level 6, 341, Queen Street,
Melbourne VIC 3000 Australia

📍 **NSW** (2nd Campus)

406/2-8, Brookhollow Ave,
Norwest, NSW - 2153



Table of Contents

1.16. Information Technology Policy and Procedure	3
Policy Content	3
Purpose	3
Policy Statement	3
Objectives	4
Scope	4
General Principles and Compliance Requirements	4
Procedures	6
Continuous Improvement	7
Privacy and Confidentiality	8
Retention of Records	8

1.16. Information Technology Policy and Procedure

Policy Content

Aspect	Details
Regulator	Australian Skills Quality Authority (ASQA)
Standards Referenced	
Legislation / Requirements	

Purpose

The purpose of this policy is to establish and maintain a secure, ethical, and compliant framework for the use of information technology (IT) resources within the RTO. It ensures that all computing infrastructure, data, and systems are managed and used in a way that supports:

- The confidentiality, integrity, and availability of information.
- The delivery of training and assessment services.
- Compliance with the VET Quality Framework, National Code, and privacy legislation.
- The prevention of unauthorised use, disclosure, tampering, or destruction of information.

This policy applies to all users of RTO's IT resources, including staff, students, contractors, and third-party providers.

Policy Statement

The RTO is committed to:

- Implementing IT practices that ensure information security, reliability, and appropriate use.
- Ensuring IT systems support training, assessment, administration, communication, and data retention needs.
- Protecting the rights of individuals through lawful collection, handling, and storage of digital information.

- Ensuring all users are aware of their responsibilities and the consequences of policy breaches.
- Maintaining a governance structure to monitor and improve IT security and performance.

Failure to comply with this policy may result in disciplinary action, including suspension of access or termination of employment/enrolment.

Objectives

This policy and procedure aim to ensure the RTO:

- Provides a safe, ethical, and supportive IT environment for training and operations.
- Protects all personal, academic, operational, and corporate data from unauthorised access or loss.
- Promotes digital literacy and responsible use of IT across all stakeholder groups.
- Maintains up-to-date infrastructure that supports learning and business continuity.
- Ensures all users understand their responsibilities and comply with relevant legislation and standards.

Scope

This policy applies to:

- All RTO staff, trainers, assessors, contractors, and third-party service providers.
- All enrolled students using RTO technology services or platforms.
- All hardware, software, cloud-based systems, email systems, online learning portals, digital communication platforms, and data storage systems used within the RTO.

General Principles and Compliance Requirements

The following principles guide the responsible use, security, and governance of information technology within the RTO:

Policy Area	Implementation Requirements	Responsible Role
Authorised Use Only	Access to RTO computing systems is granted exclusively for authorised training, assessment, student support, administration, and business functions.	All Users / IT Manager
Appropriate Usage	Users must use RTO networks, internet access, email accounts, and digital systems only for RTO-related purposes. Personal or commercial use without prior written approval is prohibited.	All Users / IT Manager
Data Security	All digital data including student records, assessment files, enrolment data, and staff records must be stored securely with password protection and access restrictions.	IT Manager / RTO Manager
Confidentiality and Privacy	Users must protect confidential information. Any access, transfer, or disclosure of personal or sensitive data must comply with the <i>Privacy Act 1988</i> and the <i>Australian Privacy Principles</i>.	All Users / Compliance Officer
Monitoring and Auditing	The RTO reserves the right to monitor system usage, access logs, internet activity, and email traffic to ensure compliance.	IT Manager / PEO
User Responsibilities	All users must: – Keep login credentials confidential – Log out of systems when not in use – Report security breaches or suspicious activity	All Users

	– Avoid installing unauthorised apps	
Inappropriate Use	It is strictly prohibited to: – Access or distribute offensive material – Circumvent system controls – Engage in cyberbullying or harassment – Introduce malware or viruses	All Users / IT Manager
Incident Reporting	All actual or suspected data breaches, security incidents, or system malfunctions must be reported immediately to the IT Manager for investigation and resolution.	All Users / IT Manager
Access Termination	Access to IT systems is revoked upon termination of employment, end of course enrolment, or breach of usage terms. Final data backups or file transfers must be requested in advance.	HR / Student Support / IT Manager
Legal and Regulatory Compliance	All IT practices must comply with the following: – <i>Standards for RTOs 2025</i> – <i>ESOS National Code 2018</i> – <i>National VET Data Policy</i> – Privacy and Copyright legislation	Compliance Officer / IT Manager

Procedures

Step	Procedure
16.1.1	Ensure that all new staff and students receive an IT induction covering responsible use, login protocols, data privacy, cybersecurity practices, and reporting obligations.

16.1.2	Provide authorised login credentials and system access levels based on user roles. Revoke access when staff or students exit the organisation.
16.1.3	Conduct regular backups of all critical data (e.g. student records, enrolments, assessments) and store securely in encrypted, access-controlled environments.
16.1.4	Implement firewalls, anti-malware software, password protection, and automatic software updates across all systems and devices.
16.1.5	Monitor system access logs, internet activity, and file changes routinely to identify unauthorised or abnormal behaviour.
16.1.6	Investigate all reported incidents involving unauthorised access, breach of privacy, system failure, or misuse. Implement corrective actions as required.
16.1.7	Notify regulatory authorities (if applicable) of any major data breaches in accordance with the <i>Notifiable Data Breaches Scheme</i> or ESOS National Code breach reporting rules.
16.1.8	Maintain version-controlled documentation of all IT policies, security procedures, and incident logs in compliance with RTO's record retention obligations.
16.1.9	Provide regular training to staff and students on cyber safety, digital communication etiquette, use of cloud systems, and compliance with privacy obligations.
16.1.10	Review IT infrastructure annually to ensure it remains current, effective, and aligned with emerging regulatory and operational requirements.

Continuous Improvement

The RTO is committed to continuously enhancing its IT systems, digital security, and user practices to support compliant and effective operations.

- All IT-related incidents, improvement opportunities, and user feedback are documented and tabled at scheduled management meetings.
- The IT Manager coordinates an annual review of IT systems and processes to identify areas for enhancement and emerging risks.

- Corrective actions arising from audits, data breach reports, or student/staff feedback are tracked and reviewed through the Continuous Improvement Register.
- Where systemic issues are identified, changes to policy or system configurations will be implemented and documented in accordance with version control procedures.

Privacy and Confidentiality

The RTO upholds its obligations under the *Privacy Act 1988* and the *Australian Privacy Principles* to protect personal and sensitive information stored or transmitted through IT systems.

- Access to personal information is restricted to authorised personnel only and is granted based on role-based access controls.
- Information is stored securely using encryption, password protection, and system-level security protocols.
- Data must not be accessed, shared, or disclosed without proper authority or for any purpose outside the scope of the user's role.
- All users are trained in data handling protocols during orientation and are bound by the RTO's Privacy and Confidentiality Policy.
- Any unauthorised access, loss, or misuse of data must be reported immediately and investigated as per internal protocols.

Retention of Records

All IT records, including user access logs, system usage history, digital backups, incident reports, and version-controlled policy documents, are retained in accordance with regulatory requirements.

Record Type	Retention Period	Reference
System access logs and audit trails	Minimum of 2 years	SRT0 2025 -Standard 10(c)
Data breach or incident reports	Minimum of 2 years from investigation	Notifiable Data Breaches Scheme / RTO policy

Backup records of student data	As per enrolment record retention	RTO's Student Record Management Policy
IT policy version history	Minimum of 5 years	Version Control and Document Management Policy

All retention periods are monitored through the RTO's document control system and are subject to review based on changes in legislation or internal policy