Students Computer and Internet usage Policy

1. Purpose

This policy outlines the appropriate use of RBIT's computer systems, network, and internet services by students.

It ensures that use of technology:

- supports learning and training outcomes
- protects students, staff, and RBIT systems
- complies with applicable legislation and regulatory requirements

This policy aligns with:

- Standards for Registered Training Organisations (RTOs) 2025
- National Code of Practice for Providers of Education and Training to Overseas Students 2018 (Student safety and wellbeing)

2. Scope

This policy applies to all students enrolled at RBIT, including:

- domestic students
- overseas students studying under CRICOS

2. Policy

2.1 Resource Utilisation

RBIT provides access to computers, networks, and internet services to support education and training.

Students must use these resources:

- primarily for academic and training purposes
- in a responsible, ethical, and lawful manner

2.2 Acceptable Use

Students are responsible for:

- complying with all RBIT policies and procedures

- using systems in a way that does not disrupt others
- maintaining the security of their login credentials

Students under 18 years of age must have appropriate parental/ guardian consent for internet use where required.

2.3 RBIT Rights and Monitoring

RBIT reserves the right to:

- monitor, log, and review network and system usage
- restrict or filter access to websites and services
- suspend or terminate access where misuse is identified

Monitoring will be conducted in accordance with privacy and legal obligations.

2.4 Unacceptable Use

Unacceptable use includes, but is not limited to:

Academic Misconduct

- cheating, plagiarism, or collusion

System Misuse

- unauthorised access to accounts or systems
- sharing passwords
- bypassing security controls
- downloading unauthorised software

Inappropriate Content and Behaviour

- accessing or distributing offensive, illegal, or harmful material
- harassment, bullying, intimidation, or stalking
- conducting private business activities

Non-academic Use

- excessive use of social media, games, or streaming unrelated to study

2.5 Unlawful Use

Students must comply with all applicable Commonwealth and State laws.

Illegal activities include:

- copyright infringement and unlicensed software use
- hacking or unauthorised system access
- fraud or misrepresentation
- creation, access, or distribution of illegal content
- defamation or unlawful communications

Serious breaches may be referred to relevant authorities.

2.6 Breach of Policy

Where a breach is identified, RBIT will:

- notify the student in writing
- provide the student an opportunity to respond
- determine appropriate action based on severity

Actions may include:

- warning
- restricted access to systems
- suspension of access
- disciplinary action under the Student Code of Conduct
- suspension or cancellation of enrolment (serious cases)

3. Procedures

3.1 First Breach

- Student issued a warning
- Access may be restricted or monitored
- Education provided on acceptable use

Serious breaches may escalate immediately.

3.2 Repeated or Serious Breaches

- Matter referred to the PEO or delegate
- Formal investigation conducted
- Outcome determined in line with Student Code of Conduct

Possible outcomes:

- continued monitoring
- suspension of access
- suspension or cancellation of enrolment

3.3 Appeals

Students may access RBIT's Complaints and Appeals Policy if they wish to challenge a decision.

3.4 Responsibilities

- **PEO / Delegate**
  - Determine outcomes for serious breaches
- **Academic / Compliance Team**
  - Investigate breaches
  - Ensure consistency and fairness
- **Administration / IT Support**
  - Monitor systems
  - Implement access controls
  - Maintain records

3.5. Related Documents and References

- Student Code of Conduct
- Complaints and Appeals Policy
- International Under 18 Welfare (CAAW) Procedure

External references:

- Australian Communications and Media Authority
- Esafety website

4. Record Keeping

RBIT will maintain records of:

- breaches and investigations
- actions taken
- correspondence

All records are securely stored and retained for a minimum of 2 years.