Information and Communication Technology (ICT) Use Policy

1. Purpose

The purpose of this policy is to establish clear expectations for the ethical, responsible, and secure use of information and communication technology (ICT) systems at Illoura College**.** It aims to protect the integrity of the College's digital infrastructure, promote safe and appropriate use of technology, and support effective teaching, learning, and administration in a blended learning environment.

2. Key Definitions

- **ICT Systems:** Includes Illoura College's network, internet, Wi-Fi, Learning Management System (LMS), student management systems, email platforms, shared drives, and all associated hardware and software.
- **Users**: Any individual—student, trainer, staff member, contractor, or visitor—who accesses Illoura College's ICT systems or digital platforms.
- **Unauthorised Use:** Any activity that breaches this policy or relevant laws, including unauthorised access, data sharing, downloading prohibited materials, or using ICT systems for non-educational or unlawful purposes.
- **Digital Literacy:** The ability of users to confidently and responsibly use digital technologies for learning, communication, and problem-solving in an online environment.

3. Policy

3.1 Student Responsibilities

Students are expected to:

- Use Illoura College's ICT systems for educational purposes only and in accordance with this policy.
- Access the College's network, LMS, and email systems using their authorised login credentials only.
- Maintain the confidentiality of passwords and report any suspected unauthorised access immediately.
- Ensure personal devices connected to college systems have up-to-date antivirus protection and legal software.
- Communicate respectfully and professionally through all digital platforms, including email, LMS discussions, and social media.
- Report any technical issues, security concerns, or suspected breaches to the ICT support team or Student Services.
- Follow the College's instructions when saving, sharing, or submitting digital work and assessments.
- Avoid actions that may damage or disrupt ICT systems, data, or other users' access.
- Adhere to Australian copyright laws when using or sharing digital content.
- ICT systems are provided to support the educational, administrative, and operational functions of Illoura College. Users must ensure their use of ICT resources aligns with organisational policies and relevant legislation.

3.2 Illoura College Responsibilities

Illoura College will:

- Provide and maintain secure and reliable ICT systems to support learning, teaching, and administration.

- Protect users' personal information and uphold data privacy in accordance with relevant legislation.
- Implement appropriate cybersecurity measures and monitor systems to prevent unauthorised access or misuse.
- Provide induction, guidance, and support to help students and staff use ICT systems effectively and responsibly.
- Ensure access to the LMS, network, and digital tools is allocated based on approved user roles.
- Communicate planned maintenance, system updates, or outages that may affect users.
- Take reasonable steps to investigate and address reported misuse or technical concerns promptly.
- Provide ongoing training to staff to ensure ICT use aligns with compliance and digital best practice.

3.3 Contractor and Visitor Responsibilities

Contractors, guests, and visitors who access Illoura College's ICT systems must:

- Use the systems only for authorised business or training-related purposes.
- Comply with the same ethical and security standards outlined in this policy.
- Maintain confidentiality of any College data or information accessed during their engagement.
- Obtain approval before connecting external devices to the College network.
- Report any ICT-related incident, loss, or breach to their college contact person immediately.
- Cease system access upon completion of their contract or visit, ensuring no data or content is retained.

3.4 Unacceptable use of ICT

This section applies to all users of Illoura College's ICT systems, including students, staff, contractors, and visitors. Unacceptable use refers to any activity that breaches this policy, relevant laws, or ethical standards.

Unacceptable use of ICT systems includes, but is not limited to:

- Accessing, storing, or distributing offensive, obscene, discriminatory, or illegal material.
- Using College systems for personal financial gain, unauthorised commercial activity, or non-educational purposes.
- Harassing, threatening, or bullying others through digital communication or social platforms.
- Sharing, downloading, or reproducing copyrighted materials without permission.
- Attempting to bypass network security, firewalls, or content filters.
- Gaining unauthorised access to accounts, systems, or confidential information.
- Introducing malware, viruses, or other harmful software into the network.
- Using another person's login credentials or leaving systems open and unattended.
- Posting or sharing false, misleading, or defamatory information about the College or its community.

4. Procedure

4.1 Breach Managing Procedure

- Any user (student, staff, contractor, or visitor) who identifies or suspects misuse of Illoura College's ICT systems must report it as soon as possible.

- Reports of suspected misuse must be made to the Quality Assurance Manager or Student Support Officer. Reports may be submitted verbally or in writing and will be handled with confidentiality.
- Based on the outcome of the investigation, Illoura College will determine and implement appropriate action. This may include issuing a verbal or written warning, providing counselling, temporarily suspending or restricting ICT access, terminating enrolment, employment, or contractual arrangements, or referring the matter to law enforcement in cases of serious or unlawful conduct.
- Illoura College monitors its ICT systems to ensure compliance and may request the removal of inappropriate, defamatory, or offensive content. Regular reviews of reported breaches will help identify patterns and guide staff and student awareness programs.

Note: Serious offences such as hacking, defamation, harassment, or the sharing of offensive or pornographic content are considered major breaches and may result in immediate expulsion, termination, or legal action.

5. Related documents and forms

Related Policies

- Privacy Policy
- Complaints and Appeal Policy
- Student Conduct and Disciplinary Policy

Forms

- Complaints and appeals form

6. Policy Information

Policy area	Training and assessment
Policy Version	V1.0
Date of Effect	July 2025
Review Schedule	July 2026
Applicable Standards	Outcome Standards for RTOs 2025 – Standard 1.8 and 2.3
Responsibility	Director of Quality Assurance