1. Purpose

This policy outlines the standards for the acceptable use of information and communication technology (ICT) systems at Orange College (OC). It ensures that these systems are used ethically, legally, and safely in a manner that supports learning, teaching, and operational needs, and protects the wellbeing of all users. It aims to:

- Safeguard OC's systems and data from misuse and security threats.
- Promote responsible digital citizenship aligned with OC values.
- Maintain compliance with relevant legislation, including the Standards for RTOs 2025.
- Support learner digital literacy, engagement, and wellbeing across OC's learning environment

This policy contributes to OC's compliance with the Standards for Registered Training Organisations 2025 (SRTOs 2025) by ensuring all ICT-related activities uphold the values of quality training, student wellbeing, and digital literacy.

2. Scope

This policy applies to all individuals accessing OC-owned or provided ICT resources, including students, staff, trainers, contractors, and visitors, across both on-campus and remote environments. Responsibilities differ based on user role, but all are expected to comply with OC's values and relevant legislative and regulatory obligations, including the SRTOs 2025.

These ICT resources include, but are not limited to:

- Learning management systems (LMS), student portals, online tools
- Internet and network access, email systems
- College-issued and personal devices used on OC premises or networks

It covers all forms of digital communication and activity, both on and off campus, that involve OC ICT systems or relate to the College's learning and teaching or administrative functions.

3. Definitions

ICT Systems: Includes all hardware, software, communication tools, and internet-connected devices owned, managed, or accessed via OC systems.

Users: Anyone accessing OC systems, including students, employees, contractors, and visitors.

Unacceptable Use: Any use that breaches law, policy, or OC values, or that compromises system security, wellbeing, or educational integrity.

4. Responsibilities

Effective security is a team effort involving the participation and support of every OC employee, staff, trainers, contractors, students and visitors who utilise the facilities in our training centres. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

All users, including students, trainers, staff, contractors, and visitors, have the responsibility to:

- Use ICT systems in accordance with this and related policies
- Respect the rights, safety, and privacy of others

- Avoid engaging in conduct that may disrupt or compromise digital learning, wellbeing, or the security of OC systems
- Report breaches, suspicious activity, or misuse to the relevant College contact

OC will provide clear digital usage guidelines, ensure systems are monitored and secure, and respond promptly to concerns or breaches.

4.1 Student Responsibilities

To uphold a safe and inclusive learning environment, students must:

- Use OC platforms for educational purposes only
- Maintain password confidentiality and refrain from sharing login credentials
- Refrain from digital harassment, impersonation, or plagiarism
- Comply with the Student Code of Conduct and Social Media Policy

4.2 OC Staff and Trainer Responsibilities

OC staff and trainers have the responsibility to:

- Model ethical and professional ICT behaviour
- Protect student data and uphold privacy standards
- Use authorised platforms for communication and record-keeping
- Report and respond to breaches swiftly and appropriately

4.3 Contractor and Visitor Responsibilities

- Access ICT systems only for authorised purposes
- Maintain confidentiality of any OC information they encounter
- Adhere to all guidelines provided by OC regarding ICT use

OC reserves the right to monitor all computer-related activity and to assist authorities to our fullest extent should a breach of law occur.

5. Policy

All users must:

- Use ICT systems primarily for educational and administrative purposes.
- Respect OC's values of safety, responsibility, equity, and professionalism.
- Avoid any use that damages OC's reputation or causes harm to others.

The policy items listed below provide guidelines for activities which fall into the category of unacceptable use in OC.

5.1 Unacceptable Use of OC-Owned Resources

Under no circumstances is a student, employee or staff member to engage in any activity that is illegal under local, state, federal or law while utilising OC owned resources.

The following activities are, in general, *prohibited*:

1) Unauthorised copying of copyrighted material, including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources such as copyrighted music or movies.
2) Installation of any software on desktop or laptop computers.

3) Storage of personal files on computers. This includes personal photos and music files.

4) Intentional introduction of malicious programs into the network (e.g., viruses, worms, Trojan horses, etc.).

5) Use of OC computing assets to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

6) Affecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the student, employee or trainer is not an intended recipient, or logging into a device, server or account that the student is not expressly authorised to access.

7) Circumventing user authentication or security of any information technology device, network or account.

8) Using a login account that is allocated to another student or staff member.

9) Any form of harassment via email, telephone, social media or messaging, whether through language, frequency, or size of messages.

10) Video or audio recording of training sessions, or the trainer, or students in the classroom without prior permission from the Training and Operations Manager / CEO.

11) Using images of OC staff, students or images relating to OC's facilities without permission from the Training and Operations Manager / CEO.

12) Communicating on behalf of OC without permission from the Training and Operations Manager / CEO;

13) Any online activity such as denigrating OC through criticism of OC's policies, practices or personnel resulting in bringing OC into disrepute.

14) Removal of, tampering with, or damage to, any information technology hardware such as (but not limited to) computer mice, keyboards, screens, PCs, printers, projectors, memory devices, networking equipment, cameras, tablets, iPads or cables.

15) Abuse of download limitations by excessive downloading of large files for personal use or continuous streaming of media from internet sources such as Internet Radio Stations.

16) Student use of social networking sites such as Facebook, Snapchat, Instagram and Kik whilst at OC is forbidden. OC's ICT resources are provided for teaching and learning.

17) Accessing or attempting to access inappropriate or blocked internet sites.

18) Creation or forwarding of texts, posts, messages or images that may be illegal, offensive, intimidating, defamatory, sexually explicit or aggressive

5.2 Unacceptable Use of Staff-, Contractor- and Student-Owned resources:

The following activities are, in general, *prohibited*:

1) Creation or forwarding of texts, posts, messages or images that may be illegal, offensive, intimidating, defamatory, sexually explicit or aggressive through OC platforms

2) Abuse of download limitations by excessive downloading of large files for personal use or continuous streaming of media from internet sources such as internet radio stations, while using OC internet/data

3) Communicating on behalf of OC without permission from the Training and Operations Manager / CEO;

4) Using images of OC staff, students or images relating to OC's facilities without permission from the Training and Operations Manager / CEO.

5) Using a login account allocated to another student or staff member, **unless assisting them in good faith to resolve a login issue or system error**.Any form of harassment via email, telephone, social media or messaging, whether through language, frequency, or size of messages.

6) Video or audio recording of training sessions, or the trainer, or students in the classroom without prior permission from the Training and Operations Manager / CEO.

7) Intentional introduction of malicious programs into the network (e.g., viruses, worms, Trojan horses, etc.).

8) Unauthorised copying of OC materials, resources and student/staff personal information.

Unacceptable use also includes ICT conduct that compromises the fairness, authenticity, or integrity of assessments, as defined under the Academic Misconduct and Plagiarism Policy.

6. Online Learning Environment

OC provides students, staff, trainers, and contractors with access to online learning resources via the internet and Learning Management System (LMS). In some instances, personal devices such as iPads/tablets/loan laptops are provided to students to enhance their learning experience.

It is the student's, staff's, trainer's or contractor's responsibility to ensure that portable devices assigned to them, such as iPads/tablets/loan laptops, are not damaged, lost or stolen. Any incidents relating to the mistreatment of portable devices must be reported to OC Staff immediately.

Students, staff, trainers, and contractors must secure their logins to learning systems with strong passwords and not share password information with other students, staff, trainers or contractors.

7. Enforcement

It is the responsibility of the person who witnesses or suspects a breach of this policy or experiences a breach of this policy to report it immediately. Any breach will be investigated and considered by the Training and Operations Manager / CEO. Each breach will be dealt with on a case-by-case basis.

This policy should be read in conjunction with the following:

- Student Code of Conduct
- Student Disciplinary Policy
- Access and Equity Policy
- Student Social Media Policy
- Privacy Policy
- Academic Misconduct and Plagiarism Policy

These documents collectively support OC's compliance with SRTOs 2025 and ensure a safe and inclusive learning environment.

7.1 Student Sanctions

Sanctions for breach by a student may include:

1) Providing a warning, counselling,

2) Withdrawal of certain privileges or opportunities,

3) Suspension, expulsion, refusal to re-enrol the student

4) Civil or criminal prosecution under applicable laws.

Serious breaches such as hacking, defamation, harassment, or distribution of offensive and pornographic content are automatically classified as being of a serious nature and may lead to expulsion or legal action.

7.2 Staff, Contractor, and Visitor Sanctions

Sanctions for breach by a staff member, employee, contractor or visitor may include:

1) Providing a warning, counselling,
2) Withdrawal of certain privileges or opportunities,
3) Suspension from duties, termination of employment
4) Civil or criminal prosecution under applicable laws.

Serious breaches such as hacking, defamation, harassment, or distribution of offensive and pornographic content are automatically classified as being of a serious nature and may lead to employment termination or legal action.

7.3 Records of Breaches and Privacy

Records of reported incidents of ICT misuse are maintained and analysed in order to identify persistent offenders and to implement targeted prevention strategies where appropriate.

OC reserves the right to request that certain subjects are avoided, defamatory posts are withdrawn, and inappropriate or offensive comments or images removed. OC has the right to monitor on an intermittent or continuous basis the information input or output, or other use of the network and any device attached to the network, including the sending and receipt of emails and the accessing of internet sites, and to check any material put on the network and in personal user accounts or on OC owned devices, in order to determine whether it is suitable for use in learning and complies with this policy. This includes files saved to personal network space and the content of emails.

Privacy will be respected when accounts are monitored.

8. Reporting and Complaints

Users concerned about a breach, misconduct, or potential risk must report it to:

- Their trainer or staff supervisor
- The Student Support Team (for technical breaches)
- The Training and Operations Manager (for educational or behavioural breaches)

Reports will be treated with confidentiality and managed in accordance with OC's Complaint and Appeals Policy and procedures.