ICT ACCEPTABLE USE (DLI) POLICY

Section 1 - Preamble

(1) This Policy is effective from 1st December 2025.

(2) Additionally, staff members must adhere to the Navitas IT Acceptable Use Policy, which provides detailed guidance specifically applicable to staff ICT use.

Section 2 - Purpose

(3) This policy outlines the acceptable use of ICT resources at DLI, ensuring compliance with laws, ethical standards, and institutional regulations. It supports academic, administrative, and operational activities while protecting ICT resources from misuse. The policy aims to safeguard data integrity, prevent unauthorized access, and promote responsible digital practices within the DLI community.

Section 3 - Scope

(4) This policy applies to all DLI students, staff, associates, contractors, and any other authorized users who access ICT resources, including university-owned and personal devices (BYOD) used on DLI networks. It covers all hardware, software, cloud services, and data storage systems used within the DLI network.

(5) During the establishment of DLI, all policy, procedures and supporting processes will be regularly reviewed. In the establishment phase, defined as the first two years from when students commence DLI programs, any issues arising from the implementation of current policy, procedure or process will be referred to a jointly-convened Policy and Procedure Review Panel (PPRP). The PPRP will comprise designated academic and professional service representatives from the University Partners and the Office of the Rector. The PPRP will recommend an outcome best aligned with relevant principles and the best interests of any student(s) concerned, and will advise DLI on the future development of policy, procedure and supporting processes. During the establishment phase, the PPRP may make recommendations to vary any given policy only with endorsement from relevant University Partner governance processes. All policy and procedure will be subject to a full review at the end of the two-year establishment phase.

Section 4 - Policy

Principles of Acceptable Use

Primary Purpose:

(6) ICT resources must be used for learning, teaching, research, and operational activities.

a. Limited personal use is permitted if it does not interfere with responsibilities or violate security protocols.

Legal & Ethical Compliance:

(7) Users must follow all applicable laws, policies, and regulations regarding data protection, privacy, copyright, and cybersecurity.

Authorized Use Only:

(8) ICT access is granted based on academic or work-related needs.

a. Unauthorized access, sharing of credentials, or system modifications are prohibited.

Limited Personal Use

(9) Occasional personal use is allowed but must not impact system performance.

a. Users must not violate institutional policies or engage in activities such as cryptocurrency mining, personal business operations, or excessive bandwidth consumption.

Use of library electronic resources

(10) Publisher licences and PDFs

(11) Printing and photocopying material

(12) Use of electronic resources on Moodle

Access and Security

User Responsibilities:

(13) Users must protect their accounts, passwords, and devices.

(14) Sharing credentials or unauthorized access to systems is strictly prohibited.

Access Control:

(15) ICT access is role-based and revoked when a user’s affiliation with DLI ends.

(16) Users must not attempt to extend or gain additional access beyond their assigned permissions.

Authentication:

(17) Strong passwords and multi-factor authentication (MFA) are required where applicable.

(18) Users must regularly update passwords and avoid using the same credentials across multiple platforms.

Device Security:

(19) All devices connecting to DLI networks must have security patches and antivirus protection.

(20) Unauthorized software installations, network disruptions, or tampering with security settings are not permitted.

Incident Reporting:

(21) Security breaches, lost/stolen devices, unauthorized access, or cyber threats must be reported to the ICT Services team immediately.

Data Protection:

(22) Users must store and handle sensitive institutional data responsibly, using encryption where necessary.

(23) Sharing or transmitting confidential data without authorization is prohibited.

Prohibited Use

(24) Engaging in illegal activities, including hacking, identity theft, fraud, or data breaches.

(25) Accessing, distributing, or storing offensive, obscene, or discriminatory content.

(26) Unauthorized commercial activities, solicitation, or use of ICT resources for personal financial gain.

(27) Bypassing security controls, introducing malware, unauthorized software, or interfering with ICT operations.

(28) Use of anonymizing proxies, VPNs, or other tools to bypass network restrictions without prior approval.

(29) Cyberbullying, harassment, spamming, or misuse of communication tools.

(30) Unauthorized use of university branding, digital assets, or institutional email for personal gain.

Privacy and Monitoring

(31) DLI reserves the right to monitor ICT usage to ensure compliance and security. Logs and audits may be conducted for security reviews.

(32) Users should have no expectation of absolute privacy when using DLI ICT resources.

(33) Personal data collected through ICT systems will be managed according to the DLI Privacy Policy.

(34) Any detected misuse may result in access restrictions, investigation, or disciplinary action.

Intellectual Property and Copyright

(35) Users must respect intellectual property rights and licensing agreements.

(36) Unauthorized copying, distribution, or sharing of software, media, academic materials, or digital assets is strictly prohibited.

(37) Use of university resources to infringe copyright, including illegal streaming, downloading, or file-sharing, is not permitted.

Compliance and Enforcement

(38) Violations will be addressed per the DLI Student Code of Conduct and Staff Disciplinary Procedure.

(39) Consequences of policy violations may include warnings, loss of ICT access, disciplinary actions, or legal repercussions.

(40) ICT Services may suspend access to individuals or systems if misuse is detected to ensure operational integrity.

(41) Repeat offenders may face permanent restrictions or dismissal from university activities, depending on the severity of the breach.

Roles and Responsibilities

(42) Responsibilities for implementing this Policy are as follows:

Role/Decision/Action	Responsibility	Conditions and limitations
ICT Policy Governance	Chief Operating Officer	Ensure policy compliance and updates
ICT Access Management	ICT Services Team	Authorise and monitor access rights
User Compliance	All Users	Adhere to policy guidelines and report issues

Section 5 - Procedure

The following procedures document how to comply with this Policy:

a. ICT Acceptable Use (DLI) Procedure

b. The detailed procedural instructions for staff regarding acceptable use of ICT resources are provided in the Navitas IT Acceptable Use Policy

Section 6 - Definitions

(43) For the purpose of this Policy:

a. ICT Resources: Hardware, software, networks, and data storage facilities provided by DLI.

b. Users: Staff, students, and associates who access ICT resources.

c. Personal Use: Limited, non-commercial use of ICT resources outside of core duties.

ASSOCIATED DOCUMENTS

(44) Associated documents are available on the DLI Policy page.

POLICY DETAIL	
Name of policy	ICT Acceptable Use (DLI) Policy
Approved by	Yayasan Governing Board
Approval date	27th November 2025
Date of effect	1st December 2025
Version	V1.0
Date of review	1st December 2026
DLI Approval	Joint Management Committee 25th November 2025
Deakin University Approval	N/A
Lancaster University Approval	N/A
Responsible Executive	DLI Rector

Implementation Officer	DLI Chief Operating Officer
Policy/procedure superseded	N/A
Associated documents	ICT Acceptable Use (DLI) Procedure
Summary	This policy outlines the acceptable use of ICT resources at DLI, ensuring compliance with laws, ethical standards, and institutional regulations. It supports academic, administrative, and operational activities while protecting ICT resources from misuse. The policy aims to safeguard data integrity, prevent unauthorized access, and promote responsible digital practices within the DLI community.
Key words for online searching	Information, Computing, Technology, System, User, Access
Category	Administrative or University governance
Target audience	Students, staff, associates