

Library Services and ICT Usage Policy and Procedure

Table of Contents

Policy Statement 3
1. Policy Principles 3
2. Library and ICT Services 3
3. Procedures 5
4. Responsibilities 5
5. Learning Management System (LMS) Training and Support 6
6. Conditions of Borrowing 7
7. Acceptable Use of ICT Resources 7
8. Cyber Security and ICT Protection 7
9. Monitoring and Privacy 8
10. Review of the Library and ICT Resources 8
11. Review and Evaluation 9
Version Control 10

Policy Statement	
Purpose	Glencoe Institute of Higher Education ('the Institute') *Library Services and ICT Usage Policy and Procedure* ('the Policy') outlines guidelines and procedures for the effective management and use of library services and Information and Communication Technology (ICT) resources at the Institute. This Policy aims to ensure seamless access to information, enhance operational efficiency, and promote a conducive learning and teaching environment for all stakeholders.
Scope	This Policy applies to all students, staff, and individuals utilising the Institute's library services and ICT resources.
Definitions	For definitions, please refer to the *Dictionary of Terms.*

1. Policy Principles

The Institute aims to provide a positive teaching and learning environment that enhances academic success. The Institute upholds the following principles:

a) Ensure alignment with relevant Commonwealth and Western Australian legislation, including the *Higher Education Standards Framework (Threshold Standards) 2021 (HESF 2021), Tertiary Education Quality and Standards Agency Act 2011 (TEQSA Act), Education Services for Overseas Students Act 2000 (ESOS Act)*, the *National Code of Practice for Providers of Education and Training to Overseas Students 2018 (National Code)*, to support the compliant, secure, and ethical use of library services and ICT resources;
b) Ensure equitable access to library resources and ICT facilities for all members of the Institute, regardless of background or status;
c) Access to learning resources does not present unexpected barriers, costs or technology requirements for students, including for students with special needs;
d) Promote responsible and ethical use of ICT resources and library materials, adhering to this Policy, the Institute's code of conduct and legal standards;
e) Safeguard the confidentiality, integrity, and availability of information and data stored within the library and ICT systems;
f) Provide high-quality library services, including collection development, information literacy programs, and responsive ICT support to meet academic needs;
g) Regularly review and update library and ICT services to adapt to technological advancements, educational trends, and regulatory requirements;
h) Educate and empower users to effectively navigate and utilise library resources and *ICT* tools through training and informational sessions;
i) Foster collaboration between library, ICT, administrative and academic departments to enhance service delivery and resource management;
j) Ensure compliance with relevant laws, regulations, and industry standards governing library operations, information management, and ICT security;

2. Library and ICT Services

The Institute library will operate from 8:30 to 17:30 on weekdays and weekends (subject to class schedules). The access to online library resources will be available for 24/7, seven days a week for all authorised users. The Institute provides comprehensive library and ICT services to support the academic needs of students and staff as listed below:

a) Library Services

i. Access to a wide range of academic materials, including prescribed and recommended books, journals, e-books, and databases, covering various fields of study;
ii. User-friendly digital catalogues and search tools to help users find and access resources efficiently;
iii. Assistance from the Academic Success Coordinator in finding and utilising resources for academic projects and research;
iv. Workshops and learning support sessions to develop academic skills;
v. Borrowing of materials from the library;
vi. Quiet study areas and computer workstations to accommodate different study preferences and needs;
vii. Access to online databases, e-books, and academic journals that can be accessed both on-campus and remotely;
viii. Orientation sessions for new users to familiarise them with library services and resources;
ix. Ongoing training sessions to enhance users' information literacy skills;
x. Facilities for printing, scanning, and photocopying documents;
xi. Online and in-person systems to reserve books in advance;
xii. Systems in place for users to provide feedback and seek assistance from library staff.

b) ICT Services

i. Availability of computers, printers, and other essential hardware for student and staff use;
ii. Access to a range of software applications needed for academic and administrative tasks;
iii. Reliable and high-speed internet connectivity throughout the campus;
iv. Technical support provided by the IT Coordinator and student support staff to assist users with any technical issues or concerns;
v. Access to online *Learning Management Systems (LMS)* for course materials, assignments, and communication with lecturers;
vi. Institute-provided email accounts and other communication tools to facilitate collaboration and information sharing;
vii. Secure Wi-Fi networks to ensure safe and reliable access to the Institute's digital resources;
viii. Regular training sessions and workshops to help users become proficient with ICT tools and systems;
ix. Access to platforms and software that support collaboration, such as Microsoft Teams, zoom, google drive and other virtual meeting software;
x. Implementation of security protocols to protect the Institute's digital infrastructure and user data.

c) Learning Management System (LMS) Access and Availability

i. Availability of a Learning Management System (LMS) to support teaching, learning, assessment submission, and communication between students and academic staff;
ii. Access to subject outlines, learning materials, assessment information, announcements, discussion forums, and feedback on assessments through the LMS;
iii. Access to the LMS provided to all enrolled students and relevant staff prior to the commencement of each teaching period;
iv. LMS subject sites normally made available to students at least one week prior to the commencement of the teaching period, allowing students to review subject outlines, learning resources, and assessment requirements in advance;

v. Uploading of subject materials, learning resources, and assessment information by academic staff prior to the commencement of teaching;
vi. Guidance on the use of the LMS provided to students through Student Orientation and academic support services.

3. Procedures

The Institute's following procedures outline the steps and guidelines for effectively and responsibly utilising library and ICT resources, promoting a conducive environment for learning and teaching.

a) Students must present their student ID or account credentials to borrow books and access library facilities;
b) Staff or visitor must obtain appropriate credentials to access library services and ICT resources;
c) All users must note the loan period and any renewal options available for borrowed items and return borrowed materials to the designated location by the due date to avoid fines;
d) All users can access the online library services via the Institute's website logging into their library account to gain some access to a variety of online resources including e-books, journals, and additional library amenities;
e) Any authorised users who have forgotten the password for their library account must submit a request for their password changes via email or in person to the Academic Success Coordinator;
f) Users can connect to the Institute's network using their assigned credentials or guest access as applicable;
g) Users must use authorised software applications available on Institute-provided computers or personal devices connected to the network;
h) User must maintain the security and confidentiality of personal and institutional data while using ICT facilities;
i) All users must ensure compliance with software licensing agreements and copyright laws when using ICT resources.

4. Responsibilities

Following are the responsibilities for both the Institute and users in library services and ICT usage at the Institute.

Services	Institute	User
Library Services	*a)* Ensure a comprehensive collection of academic resources, including books, journals, e-books, and databases; *b)* Recruit Academic Success Coordinator to oversee the management and organisation of library services; *c)* Ensure library resources are accessible to all users;	*a)* Treat library materials and facilities with care and respect; *b)* Return borrowed items on time and in good condition; *c)* Use library resources ethically, respecting copyright and intellectual property laws; *d)* Actively utilise the library's resources and support services to enhance academic success; *e)* Provide constructive feedback to Academic Success Coordinator to help improve services; *f)* Report any issues or concerns with library services promptly.

	d) Regularly update and maintain library facilities and technologies; *e)* Continuously evaluate and acquire new resources to support academic courses; *f)* Handle user feedback and grievances promptly and effectively.	
ICT Services	*a)* Ensure the availability of necessary hardware, software, and internet access to support academic and administrative activities; *b)* Recruit IT Coordinator to oversee the management and organisation of ICT services; *c)* Provide training and support for users on ICT tools and services; *d)* Implement security measures to protect the Institute's digital infrastructure and data; *e)* Offer timely technical support to users experiencing issues with ICT resources; *f)* Regularly update and maintain ICT infrastructure to ensure optimal performance and reliability; *g)* Handle user feedback and grievances related to ICT services promptly and effectively.	*a)* Use ICT resources responsibly, avoiding any activities that may harm the Institute's infrastructure or violate laws and regulations; *b)* Adhere to guidelines for maintaining network security, such as using strong passwords and not sharing login credentials; *c)* Use only authorised software and refrain from installing unauthorised programs on Institute devices; *d)* Report any technical issues or security concerns to the IT Coordinator or support staff promptly; *e)* Use ICT resources ethically, respecting copyright and intellectual property laws.

5. Learning Management System (LMS) Training and Support

a) Orientation sessions for new students include guidance on accessing and using the LMS, including navigation of subject sites, accessing learning materials, and submission of assessments;

b) Training sessions and guidance materials provided to students to support effective use of the LMS and other digital learning tools;

c) Induction and onboarding processes for academic staff include guidance on the use of the LMS for uploading learning materials, managing assessments, and communicating with students;

d) Ongoing support and assistance available to staff and students through the IT Coordinator and student support services to address LMS access or technical issues.

6. Conditions of Borrowing

All users who borrow books or utilise library services are required to follow the Institute's guidelines for library services, as outlined below:

a) Student must present their ID when using library facilities and borrowing materials from the Institute's library;

b) In the event that a student ID card is lost, the user must notify the Academic Success Coordinator to obtain a replacement library ID card;

c) Users are required to return borrowed books and other resource items by the due date, Failure to comply will result in fines and penalties;

d) If an item borrowed from the library is damaged or lost and not returned in proper condition, following action will be taken:

i. The individual responsible must replace the lost or damaged item;

ii. Borrowing rights will be suspended for a period, with the duration of the suspension depending on the extent of damage caused.

7. Acceptable Use of ICT Resources

a) The Institute ICT resources should primarily be used for activities related to academic purposes. The Institute is not responsible for any loss or damages resulting from personal use;

b) Users must not send, view, download, or store any illicit, fraudulent, and obscene material that violates the law or Institute policies;

c) Users must not use the Institute's ICT resources to defame or slander any individual or organisation. Additionally, users must not engage in any behaviour that could be seen as harassing, abusive, or obscene;

d) Users must respect copyright laws and licenses for copyrighted materials. Users should also ensure confidentiality and adhere to any re-use obligations;

e) Users must follow the terms and conditions of online forums, including social media networks, mailing lists, chat rooms, wikis, and blogs;

f) Institute ICT resources should not be used for commercial purposes such as advertisements, solicitations, promotions, or other commercial messages, except as permitted by Institute policies.

8. Cyber Security and ICT Protection

To safeguard the confidentiality, integrity, and availability of the Institute's digital systems and information assets, all users must adhere to the Institute's cyber security requirements and responsible-use obligations. These provisions operate in conjunction with the *Records Management Policy and Procedure,* the *Staff and Student Codes of Conduct,* and the *Critical Incident and Emergency Management Policy and Procedure*.

a) User Responsibilities

All users are required to:

i. Use strong, unique passwords and protect login credentials, ensuring they are not shared, disclosed, or stored insecurely, consistent with the responsible-use obligations outlined in the *Staff* and *Student Codes of Conduct*;

ii. Immediately report suspected phishing, malware, unauthorised access, compromised accounts, or any cyber security incident to the IT Coordinator in accordance with this

Policy. Incidents posing significant operational, privacy, or security risks will be escalated under the *Critical Incident and Emergency Management Policy and Procedure*, where applicable.

iii. Use only authorised and licensed software on Institute devices or when accessing Institute systems, ensuring compliance with intellectual property, licensing, and copyright requirements;
iv. Avoid downloading unverified files, clicking unknown links, or engaging in unsafe online activities that may compromise the security of systems, devices, or personal data;
v. Store, transmit, and handle sensitive information securely, in compliance with the *Privacy Act 1988 (Cth), Records Management Policy and Procedure*, and all relevant institutional data-protection requirements;
vi. Comply with ICT security directives issued by the Institute, including mandatory system updates, authentication requirements, multi-factor authentication (MFA), password resets, and cyber-awareness training activities.

b) Institute Responsibilities

The Institute will:

i. Implement and maintain appropriate cyber security measures, including network protections, firewalls, secure authentication mechanisms, access controls, encryption, and monitoring solutions to protect against cyber threats;
ii. Monitor ICT systems for unusual, malicious, or unauthorised activity, consistent with the *Monitoring and Privacy* provisions of this Policy and the obligations outlined in the *Records Management Policy and Procedure*;
iii. Maintain incident response procedures to ensure timely mitigation, reporting, and recovery in the event of a cyber incident, including triggers for escalation under the *Critical Incident and Emergency Management Policy and Procedure*;
iv. Ensure regular system maintenance, updates, and vulnerability management, supporting secure and reliable access to digital resources;
v. Provide users with ongoing guidance, training, and awareness activities to support safe ICT practices and enhance organisational cyber resilience;
vi. Ensure cyber security practices align with *HESF 2021 Standard 7.2.1*, which requires secure, accurate, and reliable information systems and information management.

9. Monitoring and Privacy

While the Institute respects the privacy of users of ICT resources, it reserves the right to monitor user activity and take action if misuse is identified. The Institute reserves the right to inspect all Institute-owned ICT devices, including all files, email accounts, messages, and logs on those devices. The Institute may examine files and directories to determine the ownership or recipient of lost or misdirected files. The Institute reserves the right to examine files if there is a threat to system integrity, the security has been compromised, an activity adversely affects the quality of service for other users, the system is being used in violation of the Institute's Policy, or the system is being used for illegal activities.

10. Review of the Library and ICT Resources

The Institute is committed to the continuous improvement of its library and ICT resources to meet the evolving needs of students and staff. Regular reviews will be conducted to assess the effectiveness, accessibility, and relevance of these resources. Feedback from users will be actively sought and considered in these reviews to ensure that the services remain current and aligned with academic and technological advancements. The review process will involve evaluating the quality of materials, the performance of technological infrastructure, and the efficiency of support

services, ensuring that the Institute maintains a high standard of excellence in both library and ICT offerings.

11. Review and Evaluation

This Policy will be reviewed at least every two years, or earlier if required due to changes in legislation, regulatory requirements, technological developments within professional and industry sectors, or institutional priorities, to ensure its ongoing relevance, accuracy, and effectiveness.

Version Control

Version	Date of Approval	Approved By	Related Documents
1.1	7 August 2025	Governing Council	Records Management Policy and Procedure Staff Code of Conduct Student Code of Conduct Intellectual Property Policy and Procedure
Benchmarking Institutions			Melbourne Institute of Technology University of New South Wales The University of Queensland Australia Charles Sturt University Australian Catholic University The University of Southern Queensland
Policy Owner			Dean
Legislations			Tertiary Education Quality and Standards Agency (Cth) (TEQSA Act) Higher Education Standards Frameworks (Threshold Standards) 2021 (Cth) (HESF 2021) Education Services for Overseas Students Act 2000 (Cth) (ESOS Act) National Code of Practice for Providers of Education and Training to Overseas Students 2018 (Cth) (National Code) Copyright Act 1968 (Cth) Privacy Act 1988 (Cth) Privacy and Responsible Information Sharing Act 2024 (PRIS Act) Information Commissioner Act 2024 (IC Act) State Records Act 2000 (WA) WA Government Cyber Security Policy (2024)
Higher Education Standards Framework (Threshold Standards) 2021 (Cth)			Standard 2.2; Standard 2.3; Standard 3.2; Standard 3.3; Standard 7.2.1.