IT Resources and Usage Policy and Procedure

1 Background

Menzies Institute of Technology (hereinafter known as the ‘Institute’) is dedicated to management of Information and Technology (IT) infrastructure, usage, and reduction of related security risks.

2 Purpose

This policy deals with provision of IT resources by the Institute and the responsibility of authorized users when using the Institute’s IT resources. The *IT Resources and Usage Policy and Procedure* ensures appropriate measures are in place to protect the corporate data and IT systems, equipment, services and related infrastructure.

3 Audience

This policy and procedure applies to all students and staff of the Institute and any other individual who has any legitimate and authorized business purpose on the property of the Institute. It also applies to all databases, data sets and information that are held in computers owned or administered by the Institute and to all operating systems, applications and learning management systems owned by the Institute.

4 Definitions

Australian Copyright Law: This particular law is defined in the *Australian Copyright Act of 1968*. It includes any work of art that is written or thought of by someone else. If other people’s works are used, reference citation must be included.

Authorized user: refers to any individual who is authorized by the Institute supervisor to access any Institute’s IT system or facility, they will include but not limited to;

- Members of staff at the Institute
- Students

- Visitors
- Alumni
- A member of staff from an organisation or a company with which the Institute is pursuing a joint venture
- A member of staff from an organisation or a company that the Institute has an interest.

IT Resources: refers to all IT facilities that include computers, video conferencing room, computer laboratories, and lecture theatres across the Institute, as well as the use of all associated networks, hardware, internet access, data storage, software, computer accounts, voicemail, telephone services, and dial-in access.

Personal information: refers to any information or opinion that is recorded in any form about an individual (either true or false) whose identity is superficial and can be rationally ascertained from the information or opinion.

Institution supervisor: refers to the Principal Executive Officer (PEO), Head of Operations or any other members of the staff who have the authority (or has passed on or delegated the authority) to recommend a staff appointment.

Personal web page: refers to the pages produced by authorized users that are not directly related to work responsibilities. They do not include any commercial information and not use for business and related actions under any circumstances or situations. They are not to be placed on the official web-sites, and any server that hosts official and personal pages needs to maintain a clear and explicit distinction between the official site area and the personal page area.

5 Policy

5.1 Access to IT resources

5.1.1 The use of IT resources in the Institute must be lawful; any unlawful use will be a breach of *MITP26 IT Resources and Usage Policy and Procedure* and it will be dealt with as if it were a disciplined offence and in according to the disciplinary actions outlined in *MITP88 Staff Code of Conduct* and *MITP04 Student Code of Conduct.*

5.1.2 Unlawful use of the Institute's IT resources may lead to a legal action being taken against individuals or authorized users. Legal consequences such as damage, costs, and fines may be awarded against such users and in severe cases, imprisonment.

5.1.3 The Institute will distance itself from any authorized user who uses its IT resources unlawfully, and it will neither defend nor support such actions.

5.1.4 The access to the Institute's IT resources will be authorized by the appointed and relevant Institute Supervisor and provided by the established department.

5.1.5 The Institute will require all users to complete *MFAxx User Declaration Form* before authorization is granted for access to certain IT resources.

5.1.6 Any access to computers and emails will cease after the expiration of the contract on the date recorded on the relevant database. A thirty days extension will be provided for strictly professional reasons, but the approval must be granted by the Head of Operations.

5.1.7 All authorized users are prohibited from any authorized access to accounts, files or data on the Institute's IT resources. The IT Officer has the right to restrict access to an individual user if the user is in breach of this policy.

5.1.8 Students and staff must not share account details with anyone and must not disclose the password to anyone, including other employees or students of the Institute.

5.1.9 Other than the IT department, no other individual or entity is authorized to grant third party access to the communication and network infrastructure of the Institute. Any application for third party access should be forwarded in writing to the appropriate Institute Supervisor.

5.1.10 The Head of Operations will register all domain names for the Institute and all authorized users should note this requirement and that the Institute owns and controls the site and not the individual who registers the name.

5.1.11 Any user of patented software is subject to terms of the license as per the terms of the agreement between the Institute and the owner or licensor of the software.

5.2 Personal use of IT resources

5.2.1 All authorized users can use IT resources for limited and incidental personal purposes. The Institute allows the personal use of its IT resources provided that the use is lawful, and the actions do not have a negative impact, or damage the operations of the Institute.

5.2.2 The Institute's IT resources are not supposed to be used for private commercial purposes unless in an event where the paid work is conducted as per the regulations established by the Institute in relation to paid outside work activities.

5.2.3 The Head Operations is responsible for determining whether or not the use of the Institute's IT resources is reasonable.

5.2.4 The Institute will not accept any responsibility for any loss or damage from the use of its IT resources.

5.2.5 The Institute will not also take any responsibility for interference, disruption and loss of data or files that may arise due to the use of its IT resources.

5.3 The internet, messaging and email

5.3.1 All authorized users are allowed to access the internet for work associated purposes only.

5.3.2 The Institute permits personal use of its IT resources for personal purposes that are rational and lawful in terms of cost and time to the Institute. Examples of the allowed personal uses include; browsing, online banking, and travel booking.

5.3.3 The Head Operations of the Institute will determine whether the use of the Institute's IT resources is reasonable.

5.3.4 All authorized users are required to respect the privacy and the personal rights of others when using emails or messaging systems.

5.3.5 All authorized users are required to take reasonable care and not to defame another user, plagiarize other's work and not to copy or forward another user's personal email.

5.4 Security of IT resources and data

5.4.1 The responsibilities of all authorized users at all-times include;

a) Act lawfully.
b) Keep all Institute's IT resources secure and comply with the Institute's *MITP26 IT Resources and Usage Policy and Procedure.*
c) Not compromise or try to either compromise the security of any IT resource belonging to the Institute or exploit any security paucity.
d) Take rational steps that will ensure there is physical protection from damage from inappropriate use, drink spillage, power management, and protection from theft and anti-static measures.
e) Ensure that their personal computers are not left unattended prior to logging out or securing entrance to any work area; more so if the computer system they are using contains private, valuable and sensitive material.

5.4.2 Authorized users are asked at all times to:

a) Ensure that important data relating to the Institute is appropriately stored on the Institute's servers for backup and preservation.
b) Confirm that the course materials are posted or placed on the official Institute's servers and not on personal web pages
c) Respect appropriate Institute record keeping and management protocols.

5.4.3 Personal information about an individual will not be disclosed without written consent of the individual concerned and in accordance with *MITP33 Privacy Policy and Procedure*.

5.4.4 All authorized users are required to keep confidential Institute data except the information which has been sanctioned for external publication as well as all information that has been provided in confidence to the Institute by other parties.

5.4.5 The Institute will not accept any responsibility for any loss or damage from the use of its IT resources.

5.4.6 The Institute will not accept any responsibility for interference, disruption and loss of data or files that may arise due to the use of its IT resources.

5.5 Prohibited use of IT resources

5.5.1 The Institute's Name and Logo should not be used without prior approval from the Head of Operations and other Institute Supervisors. Any use of the Institute's Logo, Name or Crest should be in compliance with Institute regulations.

5.5.2 The Institute prohibits any paid advertisements on any of its website using the Institute domain name, personal website or any other website that has a substantial connection with the Institute except with written permission from the Head of Operations.

5.5.3 All authorized users are particularly prohibited from unauthorized access or any attempt to obtain unauthorized access to an IT resource from other organisations.

5.5.4 All authorized users at the Institute are particularly prohibited from engagement in any conduct that is described as an infringement of copyright. Any negligent or wilful infringement of copyright will attract disciplinary action, liability for damages and denial of access to the Institutes IT resources

5.5.5 The use of electronic resources such as online journals, databases and eBooks provided by the Institute will be monitored and governed by individual license agreements, and must be used for non-commercial research and study only.

5.5.6 The use of electronic resources in teaching should comply with the contractual agreement and terms and conditions of use from the material it is sourced from.

5.6 Privacy and surveillance

5.6.1 All files, stored data and accounts that belong to the authorized users at the Institute are secured and held private from any intervention by other users including the staff.

5.6.2 There will be cases when authorized staff will be required to intervene on user accounts and may temporarily suspend account access, disconnect computers from the network during the maintenance of the Institute's IT resources such as upgrading, repairing or restoring files servers.

5.6.3 All authorized users should be aware that IT staff can scrutinize the content of user directories and hard drives time to time in the normal operations of their work but they are bound to keep any information confidential.

5.6.4 Prior approval will be required and obtained from an authorized staff member prior to the access of user's files, data or emails. Any information that may be acquired from user's files will be taken as confidential and will only be disclosed to the relevant parties. Any access to this information will be granted stringently on a need to know basis.

5.6.5 The Institute does not generally monitor any files, emails or data stored in its IT resources or across the Institute's network. Nonetheless, the Institute has the right to monitor and access any device that is connecting to the Institute's network.

5.7 Theft of IT Resources

5.7.1 All theft of IT resources will be treated as a serious misconduct and dealt with the guidelines outlined in the *MITP88 Staff Code of Conduct Policy* and *MITP04 Student Code of Conduct Policy.*

6 Procedures

6.1 The Institute's IT resources shall be used only for a legitimate Institute purposes which the user is authorized to perform, just like any other infrastructure that is Institute property.

6.2 The Institute will only permit incidental personal use of the Institute's IT resources and such use must not be in violation of any of State or Commonwealth legislation.

6.3 The Institute will be responsible in regard to Australian laws in all its policies and contracts between the Institute and other external agencies.

6.4 The Institute has well-established obligations and policies that relate to intellectual property, sexual harassment, gender based harassment and any form of racial discrimination as defined by the State laws and its own policies. The Institute expects that all of its authorized users will use the IT resources to exercise full responsibilities in this particular area.

6.5 All authorized users should acquaint themselves with the statutes, rules, and policies of the Institute that include but are not limited to those related policies acknowledged in this *MITP26 IT Resources and Usage Policy and Procedure*.

6.6 All authorized users are prohibited from using the Institute's IT resources to act deceitfully to commit fraud.

6.7 The Institute holds certain contractual and licensing obligations related to the use of its IT infrastructure that compel the way facilities are used. In case of doubt, the authorized users are required to familiarize themselves with any restrictions that are detailed in the license agreement. For further clarifications, the authorized user should contact the Head of Operations.

6.8 No authorized user shall, in any circumstance use the Institute's IT resources to transfer, access or store illicit material. IT resources are only available for use relating to the Institute's legitimate purposes.

6.9 The Institute recognizes that in order to achieve the purpose of this policy, all authorized users will;

6.9.1 Respect the rights, perception and beliefs of others.

6.9.2 Not at any time engage in any form of anti-social activities, including nuisance e-mail, chain letters, and obscene, harassing, or unwelcome behaviour.

6.9.3 Follow similar standards of behaviour while online as they would do in real life.

6.9.4 Respect and recognise the artistic works and ideas of others by following the copyright rules.

6.9.5 Always properly acknowledge the publisher or author of any information they access using the Institute's IT resources and not claim other people's work as their own.

6.9.6 Use IT resources within the Institute for training and assessment purposes only.

6.9.7 Seek advice from IT staff prior to responding to unfamiliar online prompts.

6.9.8 Eliminate and delete emails from unsecure and unknown sources without opening any of the attachments as it may contain a virus.

6.10 Access to the following content/purposes is specifically prohibited:

6.10.1 Pornography.

6.10.2 Unauthorized streaming video, music, internet radio, online games, file-sharing and recreational chat.

6.10.3 Gambling/Gaming.

6.10.4 Downloading movies and music.

6.11 All users should follow the below guidelines in using the Institute's computer laboratories.

6.11.1 Computer labs should be accessed for study or work purposes only.

6.11.2 Users are required to advise appropriate staff or supervisors of any security issues or breaches of which they become aware while using resources in the computer laboratory.

6.11.3 Installation of any software onto laboratory computers is prohibited unless the request was approved in advance by the Head of Operations.

6.11.4 Users accept that all actions and usage may be monitored or recorded.

6.11.5 All personal files need to be saved into users' removable media such as USB Flash Disk. Laboratory hard drives are cleaned once it is restarted.

6.11.6 Users will be respectful of others and will not make unnecessary noise and distraction. Low conversations that are not disturbing to others are permitted.

6.11.7 Food, drink and phone usage in computer laboratory is prohibited.

6.11.8 Users must not use any systems to attempt to gain unauthorized access to other systems within or outside the Institute.

6.11.9 Users must not use resources available at the computer laboratories for commercial purposes without explicit permission from the Head of Operations.

6.11.10 The Institute's information systems, networks and Learning Management System are not to be used for any unlawful activities, including violation of copyright, hacking and the deliberate spreading of viruses or malicious code.

6.11.11 When leaving the computer laboratory, users are expected to clean work areas by removing all papers, disks, books and any other items of personal property.

6.11.12 Users who violate clauses outlined in this policy may be asked to leave the computer laboratory.

6.12 Users should contact helpdesk@menzies.vic.edu au for advice on any issue or problems.

7 Review

This policy will be subjected to a review every three years from the approval date. Exceptions to frequency of review can be made if necessary. Any person who wishes to enter a complaint concerning this policy may do so in accordance with the appropriate policies.

RTO Code:	21834
CRICOS Code:	02815M
Document Title:	IT Resources and Usage Policy and Procedure
Document Number:	MITP26
Version:/	Version 01
Relevant Standards:	
Related Policies/Documents:	MITP88 Staff Code of Conduct MITP04 Student Code of Conduct MITP33 Privacy Policy and Procedure User Declaration Form
Responsibility:	IT Officer
Approved By:	PEO
Date Approved:	18/04/2018
Next Review Date:	April 2018

Version Control and Change History:

Version Number	**Approval Date**	**Amendment**
1	09/04/2010	Creation of policy
2	01/06/2012	Completed review and updated
3	01/06/2014	Completed review and updated
4	01/09/2016	Reviewed and updated the next review date
5	01/03/2017	Reviewed and updated the next review date
6	18/04/2018	Updated policy name and policy and procedure sections