Provision and Acceptable Use of IT Policy (MPF1314)

1. Objectives

1.1. The objectives of this policy are to:

a) outline the principles that apply to the management and use of computing and network facilities across the University;
b) support efficient University processes and enhance staff and student experience with IT tools;
c) define the expectations of users of University computing and network facilities and restrictions on use; and
d) provide authority for the University to, where necessary in the performance of its functions or activities, monitor usage of University computing and network facilities to:

i. assist in the detection and investigation of actual or reasonably suspected unlawful behaviour or breach of University policy; and
ii. act on allegations of misuse of those facilities.

2. Scope

2.1. This policy applies to the provision of, and all users of, University computing and network facilities, including:

a) students;
b) staff;
c) honoraries;
d) contractors, consultants and external providers; and
e) approved visitors and other approved individuals or organisations.

2.2. This policy applies to all uses of University networks or connectivity services including using a user-owned device (Bring Your Own Device - BYOD) to connect to University systems.

3. Authority

3.1. This policy is made under the *University of Melbourne Act 2009* (Vic) and the Vice-Chancellor Regulation .

4. Policy

Provision of University information technology

4.1. University computing and network facilities support and enable research, learning and teaching, and engagement, through provision of cost-effective world class infrastructure and customer services.

4.2. Computing and network facilities and related services are responsive to the needs of users.

4.3. Environmental impact is a key consideration in selecting and deploying computing solutions for the University.

4.4. University computing and network facilities complement and inter-operate with other information technology in the lives of users.

Use of University information technology

4.5. All users of University computing and network facilities are required to use these facilities in an appropriate and responsible manner.

4.6. Users may be exempt from aspects of this policy where it is required for their role, studies or research. Prior written permission from the head of the relevant division and the Executive Director, Business Services and Chief Information Officer must be obtained.

4.7. Users who are alleged to have misused University computing and network facilities are subject to investigation and, if misuse is established, may have penalties applied, as detailed in this policy.

Compliance with law and policy

4.8. All users must use and manage University computing and network facilities in accordance with relevant law, applicable terms and conditions of use and other University policies, including the Information Security Policy (MPF1270), Privacy Policy (MPF1104), Records Management Policy (MPF1106), Student Conduct Policy (MPF1324), Child Safety Policy (MPF1337) and Appropriate Workplace Behaviour Policy (MPF1328). All University policies can be located at https://policy.unimelb.edu.au.

4.9. To the extent allowed by law, the University is not liable for loss, damage, or consequential loss or damage incurred by users which arises directly or indirectly from:

a) use or misuse of any University computing and network facilities;
b) loss of data or interference with data stored on any University computing and network facilities;
c) interference with or damage to equipment used in conjunction with any University computing and network facilities; or
d) any acts taken or decisions made not in accordance with this or any other policy.

Usage monitoring and investigations

4.10. All actions and usage of University computing and network facilities may be logged, monitored, recorded and analysed by authorised University personnel to:

- substantiate an allegation of misuse of University computing and network facilities;
- facilitate the investigation of an activity that may be contrary to University policy and/or compliance obligations; or
- facilitate the investigation of misconduct allegations and investigations, including where the use of the University computing and network facilities is not the subject of the suspected misconduct.

Use of Wireless data

4.11. The wireless network may be monitored by the University for the following purposes:

- to ensure that use of the network is authorised;
- for the management of the network and related University systems and services;
- to investigate use or misuse of the network in connection with a breach of any law or University policy (including but not limited to misuse as described in 5.22 of this policy);
- to obtain analytical data relating to the use of the network and the physical University campus, for future planning and space/infrastructure management;
- to assist in the detection and investigation of any actual or suspected unlawful or antisocial behaviour or any breach of any University policy by a network user, including where no unauthorised use or misuse of the network is suspected; and
- to assist in the detection, identification, and investigation of network users, including by using network data to infer the location of an individual via their connected device.

In carrying out these activities, the University may collect, use, or disclose personal information associated with the network including (but not limited to): account usernames, IP addresses, MAC addresses and network activity.

Access to University-provided communication and collaboration services

4.12. Electronic communications and collaboration activities that use University computing and network facilities are records of the University. Examples include emails, video conferencing applications (including chat threads and meeting recordings and transcriptions), SharePoint sites and Learning Management System collaboration applications.

4.13. While the University recognises that some incidental, reasonable and lawful personal use of email, chat and other electronic communication channels will occur, users should note that the University may collect this personal information. The University reserves the right to access electronic communications without consent in circumstances where access to and review of the content of those electronic communications is considered necessary to support actions as described in 4.10.

Authorisation to access information

4.14. Access to personal information as outlined above will require authorisation from the Executive Director, Business Services and Chief Information Officer, and will be recorded.

4.15. Information collected as part of any preliminary enquiries or investigation as described in 4.10 will be managed in accordance with relevant law and other University policies, including the Information Security Policy (MPF1270), Privacy Policy (MPF1104), Records Management Policy (MPF1106), Child Safety Policy (MPF1337) and Appropriate Workplace Behaviour Policy (MPF1328).

Policy monitoring and exceptions

4.16. The Executive Director, Business Services and Chief Information Officer monitors compliance with this policy and supporting processes.

4.17. An authorised deviation from this policy may be granted if, following risk assessment, the impact of non-compliance is outweighed by the benefit of non-compliance. Users must ensure they do not deviate from this policy, unless the deviation has been approved by the Executive Director, Business Services and Chief Information Officer.

4.18. The Executive Director, Business Services and Chief Information Officer ensures that:

a) a register of policy deviations is maintained;
b) remediation is tracked, and effectiveness reviewed;
c) assessment is performed to check if nonconformities similar to the registered deviation may exist or may potentially occur; and
d) changes are recommended based on identified nonconformities.

4.19. For all deviations from this policy, asset owners should ensure that:

a) a risk assessment is performed to understand the impact of nonconformity;
b) a remediation plan is documented, and is time bound;
c) the deviation, and the actions to be taken to control and correct it, are formally approved by all relevant asset owners, service owners and the Executive Director, Business Services and Chief Information Officer; and
d) advice is provided to the Executive Director, Business Services and Chief Information Officer or delegate to maintain the deviations register.

4.20. Any records created as a result of this policy must be managed in accordance with the Privacy Policy (MPF1104) and Records Management Policy (MPF1106).

5. Procedural principles

University provision of services

5.1. Business Services, in collaboration with stakeholder representatives including representatives of each division, develops and maintains appropriate IT Processes and Guidelines.

5.2. Business Services supports IT environments which are consistent with agreed standards.

5.3. Support for non-standard environments may be subject to additional charges.

5.4. The University does not necessarily provide user support or funding for software licensing for a proposed non-standard use.

5.5. Divisions should not make purchases or commitments which have the effect of hindering or preventing transition to common IT products and services, and should seek advice from Business Services.

Service owner powers and responsibilities

5.6. Service owners are expected to offer their services in a professional manner with appropriate efficiency, reliability and security, considering the needs of their own users and wider user communities within and beyond the University. Service owners must be properly qualified and appropriately trained.

5.7. Service owners must impose appropriate security controls on access to facilities under their control.

5.8. Service owners must take reasonable steps to ensure that their staff and external providers use facilities only for authorised purposes and do not use facilities in a way that constitutes misuse.

5.9. Service owners and their staff and external providers must not access information stored on or passing through facilities unless that information is required for the proper performance of their duties.

5.10. Service owners must maintain and retain for at least six months a record of users who have used facilities under their control and may use those records for purposes such as monitoring and managing the performance of facilities, cost recovery and load management.

5.11. Service owners may, without prior notice, suspend or withdraw any service or the access of any user to facilities, for:

a) maintenance and upgrading of facilities;
b) preventing misuse of facilities;
c) preserving files or data;
d) the purpose of meeting regulatory or compliance obligations mandated by a government authority; or
e) other purposes that the service owner considers necessary to maintain or improve the operation, integrity or security of any facilities.

5.12. Service owners may impose and collect proper charges for the use of facilities under their control or the provision of related services.

5.13. Service owners must obtain approval from the Executive Director, Business Services and Chief Information Officer for any computer or network naming or numbering system, or management practice, which has an impact beyond the facilities under the control of the service owner.

Privileges and responsibilities of users

5.14. No user may engage in any act or practice, or omit to do any act or practice, which constitutes a misuse of any of the facilities.

5.15. Any user who becomes aware that facilities are being used by any person to infringe copyright or any intellectual property rights of another person or entity, or that the effect of any use of any facilities is to infringe such rights, must notify the University copyright officer immediately.

5.16. Any user who becomes aware that facilities are being used by any person to infringe the privacy rights of another person, or that the effect of any use of any facilities is to infringe such rights, must notify the University's Privacy and Data Protection Officer (PDPO) immediately.

5.17. All users must report any lost or stolen University owned or managed computing devices immediately to their Line Manager or the IT Service Centre.

5.18. Users are to log out or lock systems connected to the university network when not in use, including when unattended.

5.19. Users must exchange information only through University-supported channels and in line with the Information Security Policy (MPF1270) and Privacy Policy (MPF1104).

5.20. All users should use a secure and reliable internet connection and avoid using public Wi-Fi networks unless appropriate security safeguards are implemented.

5.21. All users must always safeguard sensitive information. This includes:

a) not discussing or displaying sensitive information in public spaces or with unauthorised people.
b) ensuring devices that store University data are physically secure and not leaving them unattended.

Misuse

5.22. Use of the facilities for any purpose other than an authorised purpose is considered to be misuse, for example:

a) use that causes or contributes to a breach of any provision of a law, statute, regulation, subordinate instrument, code of practice or conduct applying to the University or to which users are subject;
b) use that contravenes a University statute, regulation, rule or terms and conditions, policy or process;
c) creating, transmitting, storing, downloading or possessing illegal material;
d) the deliberate or reckless creation, transmission, storage, downloading, or display of any defamatory, pornographic, offensive or menacing images, data or other material, or any data capable of being resolved into such images or material. An exception can be made in the case of the appropriate use of facilities for properly supervised University work or study purposes, for which a prior written approval must be obtained in accordance with exception section 4.6;
e) use which constitutes an infringement of copyright or any intellectual property rights of another entity;
f) communications which would be actionable under the law of defamation;
g) communications which misrepresent a personal view as the view of the University, including unauthorised use of the University crest; and
h) deliberate or reckless undertaking of activities resulting in:

i. the imposition of an unreasonable burden or abuse of a University facility, for example:

- using applications or programs that abuse system resources, such as cryptocurrency miners and similar applications,
- using excessive capacity on shared infrastructure,
- unauthorised file-sharing;

ii. corruption of or disruption to data on a University facility, or to the data of another person;
iii. disruption to other users; and/or

iv. the use, distribution or introduction of hacking tools or malicious software (e.g., viruses, worms, trojan horses) within University IT environments. These tools will be regarded as malicious even if utilised in an approved course, unless they are confined to isolated testing networks.

i) creating, transmitting, storing, downloading or processing child exploitation material, for example child pornography and material that instructs on, promotes or incites child abuse.

Specifically prohibited activities

5.23. Users must not:

a) circumvent user authentication or access control measures, security or restrictions on the use of any facilities or account, including the use of tools that compromises security;
b) engage in gambling online, other than participation in approved football-tipping and like competitions, where the primary purpose is social rather than financial;
c) engage in unauthorised reserving of, or exclusion of others from using any facilities;
d) use any facilities for the purposes of any private business whether for profit or not, or for any business purpose other than University business, without prior approval from the division head;
e) make any use of the Computing and network facilities that contravenes the University's IT and Wireless terms of use, as approved and amended from time to time by the Executive Director, Business Services and Chief Information Officer; or
f) access information stored on or passing through facilities unless that information is required for the proper performance of their duties.

Removal of material

5.24. A service owner may at any time, without prior notice, remove or disable access to any material stored on or accessible via any facilities where it considers this may constitute, or be in furtherance of, the misuse or possible misuse of any facilities.

5.25. Without limiting, a service owner may at any time, without prior notice, remove or disable access to any material stored on or accessible via any facilities which it considers infringes or may infringe the privacy rights of any entity.

5.26. Where a person is aggrieved by a decision to remove or disable access to material under this section:

a) they may make a written submission to the Executive Director, Business Services and Chief Information Officer in response to the decision;
b) the Executive Director, Business Services and Chief Information Officer, or delegate must consider any such submission, investigate the matter, and decide as soon as practicable whether to uphold, revoke or alter the decision, and then advise the aggrieved person of the outcome; and
c) in making a decision, the Executive Director, Business Services and Chief Information Officer, or delegate, must have regard to the purpose of this policy and the interests of the University.

5.27. Any action taken under sections 5.25–5.27 must take into account any relevant requirements of the Privacy Policy (MPF1104) or Records Management Policy (MPF1106), or applicable regulatory or compliance obligations

Investigation

5.28. In this section, 'investigator' means an authorised representative of a service owner or the Executive Director, Business Services and Chief Information Officer, or delegate.

5.29. If an investigator considers that an allegation of misuse of the facilities which is brought to their attention would, if substantiated, constitute a significant and unacceptable abuse of any facilities, then they must do one of the following:

a) investigate the allegation under this section; or
b) if the investigator is a person other than the Executive Director, Business Services and Chief Information Officer, refer the allegation to the Executive Director, Business Services and Chief Information Officer for investigation under this section; or
c) if the user is a student, refer the allegation to be dealt with as an allegation of general misconduct under the Student Conduct Policy (MPF1324); or
d) if the user is a member of staff, recommend that the allegation be dealt with under the Appropriate Workplace Behaviour Policy (MPF1328) or other relevant procedures or policies; or
e) recommend that the allegation be dealt with under the provisions of any applicable contract.

5.30. An investigator may, at their discretion, investigate or refer any other allegation of misuse which is brought to their attention.

Outcomes of investigation - reporting

5.31. If, as a result of an investigation under section 5.30, an investigator is satisfied on the balance of probabilities that misuse of any facilities has taken place, they must:

a) prepare a written report setting out particulars of the misuse and of the investigation undertaken, and any action taken by the investigator;
b) if the investigator is a person other than the Executive Director, Business Services and Chief Information Officer, provide a copy of that report to the Executive Director, Business Services and Chief Information Officer;
c) if the investigation concerned alleged misuse of a facility, and the investigator does not have the role with responsibility for that facility, provide a copy of the report to that relevant role;
d) if the allegation of misuse was made against a member of staff or an honorary, provide a copy of that report to the Vice-President (Administration & Finance) and Chief Operating Officer; and
e) if the allegation of misuse was made against a student, provide a copy of that report to the Academic Registrar.

Outcomes of investigation - penalties

5.32. If, as a result of an investigation under section 5.31, an investigator is satisfied on the balance of probabilities that there has been misuse of any facilities , they may, at their discretion, do one or more of the following:

a) decide to take no further action on the alleged misuse;
b) counsel the user on appropriate use of the facilities;
c) if the user is a student, recommend that the allegation be dealt with as an allegation of general misconduct under the Student Conduct Policy (MPF1324);
d) if the user is a member of staff, recommend that the allegation be dealt with under the Appropriate Workplace Behaviour Policy (MPF1328) or other relevant procedures or policies;
e) if the user is an external user, recommend that the allegation be dealt with under applicable provisions of any contract or otherwise as determined by the Vice-President (Administration & Finance) and Chief Operating Officer, or Executive Director, Business Service and Chief Information Officer;
f) decide to suspend or withdraw any service, or the access of any user to any facilities, except where the user is a student and access to facilities is necessary for the student to continue their studies, in which case the decision can only be made with the approval of the Academic Registrar or delegate, or pursuant to the penalty provisions in the Academic Board Regulation following investigation of the allegation;

g) require the user to indemnify or compensate the University or a service owner for the reasonable loss and damage occasioned by reason of the misuse; or
h) if the misuse constitutes a potential breach of privacy, refer to and manage this in accordance with the University's Responding to a Privacy Incident process.

User responses and appeals

5.33. Where a decision has been made regarding an allegation of misuse:

a) the investigator must notify the affected user, in writing, as soon as practicable, of the decision, with reasonable particulars, and of the right of appeal; and
b) the investigator must provide the Executive Director, Business Services and Chief Information Officer with a copy of the notice as soon as practicable or, if the investigator is the Executive Director, Business Services and Chief Information Officer, they must provide the notice to the role in charge of the local facility, if relevant.

5.34. If the affected user is a student, the student should be referred to the Student Appeals Policy (MPF1323) and associated process, and advised of their right to present an appeal under that policy.

5.35. For all other affected users:

a) the affected user may, within seven days of receiving the notice, make a written submission in response to the decision to the Executive Director, Business Services and Chief Information Officer, or, in the case of the Executive Director, Business Services and Chief Information Officer being the investigator, make this submission to the Vice-President (Administration & Finance) and Chief Operating Officer;
b) the Executive Director, Business Services and Chief Information Officer or the Vice-President (Administration & Finance) and Chief Operating Officer, as appropriate, shall consider the decision and any submission made in response and decide, within seven days of receipt, whether to uphold, revoke or alter the decision, and advise the affected user of the outcome as soon as practicable; and
c) a decision by the Executive Director, Business Services and Chief Information Officer or Vice-President (Administration & Finance) and Chief Operating Officer, or delegate is final. Where an allegation of misuse has been made against a member of staff or an honorary, the Chief People Officer, or delegate, will be consulted before making a decision if practicable to do so.

6. Roles and responsibilities

Role/Decision/Action	***Responsibility***	***Conditions and limitations***
Use all computing and network facilities appropriately, lawfully and in compliance with this and other relevant policies and rules of the University	Users	
Provide reliable, secure access to the IT services or facilities in their control Ensure they and their staff do not access data or information passing through the system except as required by policy, rule or law Perform all required	Service owners	Obtain approval from the Chief Information Security Officer and Director, Enterprise Technology for any computer or network naming or numbering system, or management practice, which has an impact beyond the facilities under the control of

Role/Decision/Action	*Responsibility*	*Conditions and limitations*
maintenance on systems, including imposing restrictions on use to facilitate maintenance Investigate, or cause to have investigated, allegations of system misuse Impose penalties or refer to other disciplinary processes if misuse is substantiated Report on all investigations to the Executive Director, Business Services and Chief Information Officer		the service owner
Consider service owner requests for non-standard numbering or naming systems and give or deny permission Establish, publish and maintain IT standards which prescribe standard services Establish and publish conditions of information technology system use Investigate, or cause to have investigated, allegations of system misuse Impose penalties or refer to other disciplinary/breach processes if misuse is substantiated	Executive Director, Business Services and Chief Information Officer, or delegate	Where an allegation of misuse has been made against a member of staff or an honorary, the Chief People Officer, or delegate, should be consulted before making a decision if practicable to do so
Authorise access to information under section 4.14	Executive Director, Business Services and Chief Information Officer	Access must be restricted to authorised personnel and the information accessed must be the minimum required to meet the purposes of the request. This includes de-identification where possible and prompt deletion of information that is no longer required for the stated purpose.
Determine whether the decision of the Executive Director, Business Services and Chief Information Officer should be upheld, modified or reversed	Vice-Chancellor or delegate	Where an allegation of misuse has been made against a member of staff or an honorary, the Chief People Officer, or delegate, should be consulted before making a decision if practicable to do so

7. Definitions

Asset owner means an individual who holds accountability for an information asset. Asset owner is the owner of specific data elements, wherever the data resides (e.g. employee HR data). Asset owner may delegate operational responsibility to many asset custodians.

Authorised purpose means purposes associated with work or study in the University, or provision of services to or by the University, which are approved or authorised by the relevant officer or employee of the University in accordance with University policies and procedures or pursuant to applicable contractual obligations, limited personal use, or any other purpose authorised by the relevant authority.

Bring Your Own Device (BYOD) means the practice of allowing the students and employees of an organisation to use their own computers, smartphones, or other devices for work purposes.

Computing and network facilities means computers, computer systems, data network infrastructure, wireless network access facilities, email and other communications and information facilities and related services together with associated equipment, software, files and data storage and retrieval facilities, all of which are owned or operated by or on behalf of the University and form part of the central facilities or the local facilities.

External provider means an external entity that provides computing and network facilities to the University.

Facilities means computing and network facilities.

Hacking tools are software utilities used to probe, test or circumvent security controls for the purposes of identifying and exploiting vulnerabilities or features in software or systems that might allow an attacker to gain unauthorised access to systems or data.

Materials means any type of content either physical or digital (i.e. image, sound, writing, web content).

Service owner means an individual who has been allocated responsibility for an information system (such as an. application, device, network, cloud service, or a specific component thereof). There is only one service owner for each information system. A service owner will commonly be delegated asset custodian responsibilities by several asset owners.

Unreasonable burden is an activity which a reasonable person would agree and has a disproportional impact on another user's ability to use the UoM network or degrades the performance of core services.

User means any member of staff or a student, or any other person, who is authorised to use the central facilities or a local facility, including a provider and any officer, employee or agent of an external provider.

POLICY APPROVER

Vice-President (Administration & Finance) and Chief Operating Officer

POLICY STEWARD

Executive Director, Business Services and Chief Information Officer

REVIEW

This policy is to be reviewed by (TBC).