

# Provision and Acceptable Use of IT Policy (MPF1314)

## 1. Objectives

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 information technology systems and restrictions on use; and
- (d) provide authority for the University to investigate and act on allegations of misuse.

## 2. Scope

2.1. This policy applies to the provision of, and all users of, University information technology services, equipment and connectivity, including:

- (a) students;
- (b) staff;
- (c) honoraries;
- (d) contractors and consultants; and
- (e) visitors.

2.2. This policy applies to all uses of University networks or connectivity services including using a user-owned device to connect to the system.

## 3. Authority

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 students and staff.
- 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 students and staff.

### **Use of University information technology**

4.5. All users of University information technology services, equipment and connectivity are expected to use these facilities and services in an appropriate and responsible manner.

4.6. It is the responsibility of authorised users of information technology services, equipment and connectivity to make themselves aware of the University's policies, terms and conditions of use and processes related to information technology, and to conduct their activities accordingly.

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

4.8. Users must not misuse University computing or network facilities.

4.9. Users who are alleged to have misused University information technology services, equipment and connectivity are subject to investigation and, if misuse is established, will have penalties applied, as detailed in this policy.

### **Compliance with law and policy**

4.10. All use and management of University computing and network facilities must be consistent with relevant law and other University policies, including the [Information Security Policy](#), [Privacy Policy](#) and [Records Management Policy](#).

4.11. To the extent allowed by law, the University is not liable for loss, damage, or consequential loss or damage, arising directly or indirectly from:

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

## **5. Procedural principles**

### **University provision of services**

5.1. Infrastructure Services, in collaboration with stakeholder representatives including representatives of each division, develops and maintains appropriate IT standards.

5.2. Infrastructure 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 of facilities.

5.5. The IT Product and Services Catalogue specifies which products and services are common products or services.

5.6. The IT Product and Services Catalogue must include the following components of the life-cycle cost of IT products:

- (a) initial cost;
- (b) maintenance and ongoing costs, including energy and consumables;
- (c) disposal costs including packaging; and
- (d) environmental impact.

5.7. Divisions must not make purchases or commitments which have the effect of hindering or preventing transition to common IT products and services.

### **Provider powers and responsibilities**

5.8. Providers 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. Staff of providers must be properly qualified and appropriately trained.

5.9. Providers must impose appropriate security controls on access to facilities under their control, including on usernames, passwords and other authentication methods.

5.10. Providers must take reasonable steps to ensure that their officers, employees and agents use facilities only for authorised purposes and do not use facilities in a way that constitutes misuse.

5.11. Providers and their officers, employees and agents must not access information stored on or passing through facilities unless that information is required for the proper performance of their duties.

5.12. Providers 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.

5.13. The Executive Director, Business Services and Chief Technology Officer may request that providers furnish records for the purposes of investigating alleged misuse of facilities, and providers must comply with any such requests.

5.14. Providers 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; or
- (d) other purposes that the provider considers necessary to maintain or improve the operation, integrity or security of any facilities.

5.15. Providers may impose and collect proper charges for the use of facilities under their control or the provision of related services.

5.16. Providers must obtain approval from the Executive Director, Business Services and Chief Technology 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 provider.

### **Privileges and responsibilities of users**

5.17. Facilities may be used only for authorised purposes.

5.18. 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.

5.19. Any use of facilities which incurs a charge from a provider must be approved by the provider, and if applicable, also by the organisational unit which will be paying the charge.

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

5.21. 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 privacy officer immediately.

### **Misuse**

5.22. Use 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, or 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 offensive or menacing images, data or other material, or any data capable of being resolved into such images or material, except in the case of the appropriate use of facilities for properly supervised University work or study purposes;
- (e) use which constitutes an infringement of any intellectual property rights of another person;
- (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;
- (h) deliberate or reckless undertaking of activities resulting in:
  - i. the imposition of an unreasonable burden on a University facility;

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. introduction or transmission of a virus into the facilities.

### Specifically prohibited activities

5.23. Users may not:

(a) circumvent user authentication or access control measures, security or restrictions on the use of any facilities or account, including the unauthorised distribution or use of tools for compromising 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; or

(e) make any use of IT facilities which, while lawful, contravenes the intent of section 5.23 and appears in the list of terms and conditions of use, as approved and amended from time to time by the Executive Director, Business Services and Chief Technology Officer.

### Removal of material

5.24. A provider may at any time, without prior notice, remove or disable access to any material stored on or accessible via any facilities which it considers constitutes or may constitute, or be in furtherance of, misuse or possible misuse of any facilities.

5.25. Without limiting 5.24, a provider 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 intellectual property rights of any person.

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

(a) they may provide to the Executive Director, Business Services and Chief Technology Officer a written submission in response to the decision;

(b) the Executive Director, Business Services and Chief Technology Officer, or delegate, must consider any such submission and investigate the matter and decide, as soon as practicable, whether to uphold, revoke or alter the decision, and advise the aggrieved person of that decision; and

(c) in making a decision, the Executive Director, Business Services and Chief Technology Officer, or delegate, must have regard to the purpose of this policy and the interests of the University.

5.27. Any action taken under clauses 5.24–5.26 must take into account any relevant requirements of the [Privacy Policy](#) or [Records Management Policy](#).

## Investigation

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

5.29. If an investigator considers that an allegation of misuse 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 Technology Officer, refer the allegation to the Executive Director, Business Services and Chief Technology 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](#); or
- (d) if the user is a member of staff, recommend that the allegation be dealt with under the [Appropriate Workplace Behaviour Policy](#) 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 5.29, 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 Technology Officer, provide a copy of that report to the Executive Director, Business Services and Chief Technology 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 the Executive Director, Human Resources and OH&S; 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 5.30, an investigator is satisfied on the balance of probabilities that there has been misuse of any facilities by any staff user, 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](#);
- (d) if the user is a member of staff, recommend that the allegation be dealt with under the [Appropriate Workplace Behaviour Policy](#) 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 Head of University Services;
- (f) decide to suspend or withdraw any service or the access of any user to any facilities, except that where the user is a student and access to facilities is necessary for the student to continue their studies, the decision can be made only 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 provider for the reasonable loss and damage occasioned by reason of the misuse; or
- (h) if the misuse results in a breach of privacy, refer to the relevant privacy breach 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 Technology Officer with a copy of the notice as soon as practicable or, if the investigator is the Executive Director, Business Services and Chief Technology 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 staff member:

- (a) the affected user may, within seven days of receiving the notice, provide to Executive Director, Business Services and Chief Technology Officer, or, in the case of the Executive Director, Business Services and Chief Technology Officer being the investigator, provide to the Vice-President (Administration & Finance) and Chief Operating Officer a written submission in response to the decision;
- (b) the Executive Director, Business Services and Chief Technology Officer or the Vice-President (Administration & Finance) and Chief Operating Officer, as appropriate, must consider the decision and such submission in response and decide, within seven days of receipt, whether to uphold, revoke or alter the decision, and advise the affected user of his or her decision as soon as practicable; and
- (c) a decision by the Executive Director, Business Services and Chief Technology 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 Executive Director, Human Resources and OH&S, or delegate, will be consulted before making a decision if practicable to do so.

5.35. If the affected user is a student, the student must be referred to the [Student Appeals to the Academic Board Policy](#) and associated process and advised of their right to present an appeal under that policy.

## 6. Roles and Responsibilities

<i>Role/Decision/Action</i>	<i>Responsibility</i>	<i>Conditions and limitations</i>
Use all IT 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 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 director (information technology)	Providers	Obtain approval from the director (information technology) for any computer or network naming or numbering system, or management practice, which has an impact beyond the facilities under the control of the provider
Consider provider 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 Technology Officer, or delegate	Where an allegation of misuse has been made against a member of staff or an honorary, the Executive Director, Human Resources and OH&S, or delegate, must be consulted before making a decision if practicable to do so
Hear submissions from users who have been found to have committed misconduct in an investigation by the director (information technology)  Determine whether the decision of the Executive Director, Business Services and Chief Technology 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 Executive Director, Human Resources and OH&S, or delegate, must be consulted before making a decision if practicable to do so



--	--	--

## 7. Definitions

**Authorised use** means purposes associated with work or study in the University, 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.

**Computing and network facilities** means computers, computer systems, data network infrastructure, dial-in network access facilities, email and other communications and information facilities together with associated equipment, software, files and data storage and retrieval facilities, all of which are owned or operated by 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.

**Provider** means the University division which provides and manages any part of the facilities.

**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 a provider.

## POLICY APPROVER

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

## POLICY STEWARD

Executive Director, Business Services and Chief Technology Officer

## REVIEW

This policy is to be reviewed by 2 June 2021.

## VERSION HISTORY

Version	Authorised by	Approval Date	Effective Date	Sections modified
1	Vice-Chancellor	2 June 2016	21 July 2016	New policy arising from the n Policy Consolidation Project. Regulation 8.3.R2 Computing Systems and Support Policy (MPF1 Telephony Procedure (MPF1
2	Executive Director, Infrastructure Services	8 December 2016	8 December 2016	Editorial amendment, incorp Behaviour Policy (MPF1328).
3	Vice-Chancellor	7 March 2019	30 April 2019	Changed Policy Approver to Operating Officer (previously
4	Vice-President (Administration & Finance) and Chief Operating Officer	18 April 2019	30 April 2019	Editorial amendments to com style guide.
5	University Secretary	31 July 2019	1 August 2019	Amended Policy Steward title