

LA TROBE UNIVERSITY

**EXPLANATORY MEMORANDUM FOR THE USE OF COMPUTER
FACILITIES STATUTE 2009**

Council is invited to make the attached **Use of Computer Facilities Statute 2009** (the new Statute).

The new Statute provides for the use of the University's computer facilities, and has been developed in consultation with the Chief Information Officer. It replaces Statute 37 – Use of Computer Facilities and Regulation 37.1 – Use of Computer Facilities.

The Statute regulates use of the University's computer facilities in a number of ways—

- Section 3 restricts use of computer facilities to persons who are approved computer users.
- Section 4 provides that the University may impose charges for the use of computer facilities.
- Section 5 requires computer users to obtain computer accounts prior to use and limits use in accordance with the access privileges granted to the user, along with any Restricted Access System developed by the University.
- Section 6 prohibits a wide range of harmful and inappropriate conduct in relation to the use of computer facilities, including using another person's computer account and using computer facilities to engage in various forms of misconduct, such as making hoax calls, sending unsolicited e-mails, harassing or interfering with the work of other computer users, or committing a breach of any law.
- Section 7 provides that the use of computer facilities is subject to a range of specified conditions.

Section 12 provides the Chief Information Officer with certain enforcement powers, and links those powers to the procedures set out in the **General Misconduct Statute 2009**.

LA TROBE UNIVERSITY

USE OF COMPUTER FACILITIES STATUTE 2009

The Council of La Trobe University makes this Statute under section 30 of the *La Trobe University Act 1964*.

1. Name and commencement

- (1) This Statute is the **Use of Computer Facilities Statute 2009**.
- (2) This Statute comes into full force and effect on 1 July 2009.

2. Interpretation

- (1) In this Statute—

Approved Computer User means a Computer User who has been duly authorised by the University to use Computer Facilities;

Approved Purposes means purposes associated with the legitimate teaching, research or administration of the University or authorised under this Statute or any University Policies or Procedures but excludes any illegal or improper purpose;

CIO means the person occupying or acting in the position of Chief Information Officer of the University (or any new position having substantially the same duties as that position) or a nominee of the Chief Information Officer and includes any person authorised by the Council to exercise the powers of the Chief Information Officer under this Statute;

Computer Facilities includes—

- (a) computer hardware, communications hardware (including for wireless communications) peripherals and all other computer equipment, computer and communications software, data in digital form, voice communications and all cables and other equipment necessary for the networking of computers and hardware which is—
 - (i) owned, leased, provided or used under licence by the University (“University computers”); or
 - (ii) owned or maintained by other persons, including members of the University, but made available

for use by Computer Users through an agreement with the University;

- (b) online services, hosted or communications services (including wireless communications) provided by the University including internet, intranet and e-mail services; and
- (c) all other computing and communications services wherever situated where access is by means of computer facilities referred to in paragraphs (a) and (b) of this definition;

Computer Program has the same meaning as **computer program** has in the *Copyright Act 1968* (Cth);

Computer User means a person using Computer Facilities;

Intellectual Property Laws means any law of the Victorian or Commonwealth Parliament creating or regulating intellectual property rights;

Privacy Laws means all laws for the protection of privacy and personal information to which the University is subject;

Prohibited Content means material the creation, publication, transmission, display, making available, sale or possession of which is prohibited or restricted under any law of the Commonwealth or Victorian Parliament;

Restricted Access System means any adult verification system developed by the University to restrict access to adult material on the Internet to persons who are 18 years or older;

Secret Information means information such as a password or a private cryptographic key or other identifier which a Computer User is intended to keep secret and which is used by the Computer User (whether or not in conjunction with the Computer User's Username or a Token) to log-in or to access Computer Facilities in accordance with the Computer User's level of access privileges;

Technological Protection Measure has the same meaning as **technological protection measure** has in the *Copyright Act 1968* (Cth);

Token means a hardware device (including a card or USB key) which a Computer User is required to use to log-in or to access Computer Facilities in accordance with the Computer User's level of access privileges (whether or not used in conjunction with a Username or Secret Information);

University Network means the network of University computers and all hardware and Computer Programs and other infrastructure necessary for the operation of the network;

University Procedures and Policies includes, without limitation, the University's Policies and Procedures on Harassment, Sexual Harassment and Discrimination and procedures and policies on the use of Computer Facilities issued by the University from time to time;

Username means the username allocated to a Computer User by the University at the time of the establishment of the Computer User's computer account which (whether or not in conjunction with the Computer User's Secret Information or a Token), enables the Computer User to log-in or to access Computer Facilities in accordance with the Computer User's level of access privileges.

- (2) The provisions of the *Copyright Act 1968* (Cth) are taken to be incorporated into this Statute to the extent necessary to give full meaning and effect to the definitions of **Computer Program** and **Technological Protection Measure** set out in subsection (1).

3. Availability of Computer Facilities

- (1) A person must not use the Computer Facilities unless the person is an Approved Computer User.
- (2) A Computer User must—
 - (a) use the Computer Facilities for Approved Purposes only;
 - (b) when using Computer Facilities, comply with all relevant laws, Statutes and regulations and University Procedures and Policies.

4. Charges for use of Computer Facilities

- (1) The University may determine any charges payable for use of any Computer Facilities and shall publish any such charges in a form readily available to Computer Users.
- (2) A Computer User shall pay any charge as so determined in relation to the use of any Computer Facilities.

5. Computer access

- (1) Unless otherwise determined by the CIO, a Computer User shall obtain a computer account prior to the Computer User's initial use of any Computer Facilities.

- (2) A Computer User shall use Computer Facilities within the limits of the access privileges granted to the Computer User and in compliance with any Restricted Access System developed by the University.
- (3) A Computer User must not provide—
 - (a) his or her Username or Secret Information; or
 - (b) any identifier allocated to the Computer User as part of a Restricted Access System; or
 - (c) a Token allocated to the Computer User—to any other person, unless authorised to do so by the CIO.

6. Restrictions on use of Computer Facilities

- (1) A Computer User must not—
 - (a) use another person's computer account despite any permission from the account holder unless it is a special group account authorised by the CIO;
 - (b) use any Computer Facilities which the Computer User is not authorised to use;
 - (c) use Computer Facilities in violation of the terms of any Computer Program licence agreement;
 - (d) use Computer Facilities to infringe any Intellectual Property rights or to contravene any Intellectual Property Laws;
 - (e) without the permission of the owner, copy, rename, change, examine or delete files or content belonging to another Computer User or any other person;
 - (f) use terminals, computer equipment, network devices or any other associated equipment in an unauthorised or unlawful manner;
 - (g) collect, remove or discard any computer output without the owner's permission;
 - (h) without the written permission of the CIO, use Computer Facilities for the purpose of private profit making or other private commercial activities;
 - (i) use the Computer Facilities in any way that may damage the Computer Facilities or interfere with or interrupt the Computer Facilities or any other telecommunications network, equipment, facilities or cabling whether controlled or used by University or

not, or any other supplier of telecommunications services;

- (j) use the Computer Facilities in any way that may damage any property or injure or kill any person;
- (k) use Computer Facilities to transmit, publish or communicate any defamatory, offensive, abusive, harassing, objectionable, fraudulent, indecent or menacing material;
- (l) use Computer Facilities to make any hoax call, including calls to an emergency service;
- (m) use Computer Facilities to violate or infringe any duty or obligation owed to any person under law;
- (n) use Computer Facilities to send unsolicited commercial e-mail;
- (o) use Computer Facilities to engage in sexual harassment; sexual harassment or racial discrimination;
- (p) use Computer Facilities to transmit, distribute or make available online any internal e-mail communication or other materials prepared for use within the University to persons external to the University unless expressly authorised;
- (q) use Computer Facilities to make an unauthorised disclosure of any confidential information of the University;
- (r) use Computer Facilities to harass or interfere with the work of other Computer Users;
- (s) use Computer Facilities to misrepresent himself or herself as another person online;
- (t) use Computer Facilities to create, download, store, transmit, distribute, publish, display or make available on-line content which is Prohibited Content, unless in compliance with any restrictions imposed by the law regulating such content;
- (u) use Computer Facilities to reproduce, download, transmit, distribute, publish or make available online any Computer Program or other copyright material unless—
 - (i) authorised by law; or
 - (ii) with the express permission of the copyright owner and in compliance with the terms of any applicable copyright licence or notice,

and shall ensure that the terms of any applicable copyright licence or notice are communicated to any person to whom the

copyright material is transmitted, distributed, published or made available; or

- (v) use Computer Facilities to engage in any other conduct prohibited by law or in breach of any of the University Statutes and regulations or University Policies or Procedures.

Note:

A contravention of subsection (1) by a student would constitute *general misconduct* within the meaning of section 4 of the **General Misconduct Statute 2009**.

- (2) A person must not—
 - (a) without the permission of the CIO, copy, rename, change, examine or delete files or content belonging to or controlled by the University;
 - (b) attempt to discover or use a Computer User's Secret Information or Token or to circumvent any Restricted Access System;
 - (c) reproduce, decompile, reverse engineer, disclose or transfer any Computer Program provided by the University without the written permission of the CIO;
 - (d) do, or attempt to do, any of the following—
 - (i) modify Computer Facilities;
 - (ii) obtain extra resources without authorisation;
 - (iii) degrade the performance of any System;
 - (iv) circumvent the restrictions associated with any Computer System, Computer Account, Network Service or Technological Protection Measure;

Note:

See subsection (4) below regarding the interpretation of capitalised terms used in paragraph (d) above.

- (e) tamper or attempt to tamper with any filtering software installed by the University on any Computer Facilities for the screening of Prohibited Content;
- (f) use any networks or Computing Facilities at other sites connected to the University Network in an unauthorised or unlawful manner;
- (g) smoke near terminals, computer equipment or other associated equipment forming part of the Computer Facilities or eat or drink in areas designated as no eating or drinking areas by the CIO; or

- (h) access or attempt to access the electronic mailbox of a Computer User unless authorised by the University.

Note:

A contravention of subsection (2) by a student would constitute *general misconduct* within the meaning of section 4 of the **General Misconduct Statute 2009**.

- (3) The CIO shall determine what is an authorised manner for the purposes of subsection (1)(f) and (2)(f) by issuing determinations from time to time with prospective effect. Such determinations may be of general application or pertain to specified conduct or to a class of or to particular Computer Users.
- (4) In subsection (2)(d), *Computer System*, *Computer Account*, *Network Service*, *System* and *Technological Protection Measure* mean any such thing forming part of the Computer Facilities.
- (5) Each of the provisions of subsections (1) and (2) must be construed independently of each other and do not limit one another.

7. Conditions to which use of Computer Facilities is subject

- (1) The use by a Computer User of the University's Computer Facilities is subject to the following conditions—
 - (a) the University provides the Computer Facilities without any express or implied guarantees as to—
 - (i) the accuracy of computational results and output;
 - (ii) computer availability or computer performance;
 - (iii) network availability, network bandwidth or network performance; or
 - (iv) the compatibility between the University Computer Facilities and any Computer Program, device or any other information technology hardware or software installed by the Computer User and which is not part of the University's standard operating environment.
 - (b) the University is not responsible for—
 - (i) any consequences arising from the inaccuracy of any information generated or transmitted through the use of Computer Facilities; or
 - (ii) the loss or corruption of any information or Computer Program stored in or sent or provided to or entered into any Computer Facilities;

- (c) notwithstanding the operation of standard back up procedures on central Computer Facilities, each Computer User is responsible for the maintenance of duplicates of any information or Computer Program belonging to the Computer User;
 - (d) the University may apply any Computer Program upgrades and configuration as the University deems necessary to ensure that a Computer User's personal device (including without limitation a Computer User's personal laptop) is upgraded or configured to an acceptable level for connection to the University's Computer Facilities.
- (3) The University is not liable to—
- (a) a person for any loss or damage arising from the use of Computer Facilities by that or any other person; and
 - (b) a Computer User for any damage caused to the Computer User's personal device as a result of the application of a Computer Program upgrade or configuration referred to in subsection (2)(d).

8. Connection of hardware to Networking Facilities

A person must not connect computer hardware to the University's Network unless otherwise permitted under the University Procedures and Policies or unless the person has obtained the written approval of the CIO.

9. Withdrawal of facilities

The University may withdraw the availability of any Computer Facilities without notice and without liability despite the terms of any agreement concerning use of the Computer Facilities.

10. Upgrading of facilities

The University may upgrade any Computer Facilities from time to time as required in the manner determined by its officers and shall determine the time and manner of notification of any such upgrades to Computer Users.

11. Monitoring and examination of use of Computer Facilities

For the purpose of ensuring compliance with applicable laws, Statutes and regulations, the University Policies and Procedures and to maintain a secure and effective computing environment, the University may, at any time—

- (a) monitor, copy and examine all computer files and electronic mailboxes of individual Computer Users; and
- (b) monitor all usage of Computer Facilities.

12. Enforcement

- (1) If the CIO has reason to suspect that there is or has been a breach of this Statute, the CIO may immediately and without notice—
 - (a) suspend a Computer User's access to Computer Facilities; and
 - (b) do one or both of the following—
 - (i) isolate an item of computer equipment, whether belonging to the University or not, which the CIO reasonably suspects is being or was used in breach of this Statute;
 - (ii) impound an item of computer equipment, whether belonging to the University or not, which the CIO reasonably believes will afford evidence of a breach of this Statute.
- (2) If the CIO, after initial investigation, is satisfied that—
 - (a) no breach of this Statute can be substantiated; or
 - (b) a breach of this Statute has occurred, but that any such breach is a minor one—

the CIO must terminate the suspension and, as soon as practicable—
 - (c) if an item of computer equipment was isolated under subsection (1)(b)(i), cease the isolation of that equipment; or
 - (d) if an item of computer equipment was impounded under subsection (1)(b)(ii), return the equipment to its owner.
- (3) If the Computer User is a student and the CIO after initial investigation determines that a breach of this Statute may have occurred and that the breach is not minor, the CIO shall—
 - (a) if the CIO is a general misconduct officer under the **General Misconduct Statute 2009**, deal with the matter in accordance with that Statute; or
 - (b) if the CIO is not a general misconduct officer under the **General Misconduct Statute 2009**, report the matter to a general misconduct officer.

- (4) If a suspected breach of this Statute is to be dealt with under the **General Misconduct Statute 2009**, a suspension under subsection (1) may, at the discretion of the CIO, remain in force until the suspected breach has been dealt with under that Statute.
- (5) If, after initial investigation, the CIO reasonably suspects that a breach of this Statute may have been committed by a Computer User who was a member of staff at the time of the suspected breach, the CIO must deal with the matter in accordance with the applicable industrial Award or Agreement, or where no Award or Agreement applies, as determined by the CIO (Personnel).
- (6) Any computer equipment impounded under subsection (1)(b)(ii) and retained as evidence for use in any proceedings against a Computer User under this Statute or the **General Misconduct Statute 2009** must be returned to the Computer User as soon as practicable after the conclusion of those proceedings.

13. Powers not to be in derogation

The powers conferred by this Statute shall be in addition to and not in substitution for any powers which may be conferred by any other Statute or regulations of the University.

14. Regulations

- (1) The Council may make regulations—
 - (a) for or with respect to or providing for—
 - (i) the control and use of Computer Facilities provided by the University; and
 - (ii) any other matter or thing for the purposes of this Statute; and
 - (b) amending or revoking any regulations made under this Statute.
- (2) A regulation made by the Council under this section may be limited in application to a specified campus of the University or a specified location within a campus of the University.
- (3) The Council must ensure that regulations made under this Statute are promulgated by having the regulations displayed on an official notice board of the University for a period of at least 14 days.
- (4) For the purposes of determining when regulations made under this Statute come into full force and effect within the meaning of section 30(4) of the Act, the regulations are taken to have been promulgated in accordance with sub-section (2) at the start of the first

day on which they are displayed on an official notice board of the University.

15. Revocation of earlier University legislation

The following Statute and regulations are **revoked**—

- (a) Statute 37 – Use of Computer Facilities;
- (b) Regulation 37.1 – Use of Computer Facilities.

=====

Approved by the Council—

Approved by the Minister—