SPAM Policy

Section 1 - Background and Purpose

(1) La Trobe University is committed to ensuring that the SPAM Act 2003 is not breached. Educational institutions have special exemptions under the Act and this Policy will outline where sending of unsolicited commercial electronic messages is permitted and where it is not. Breaches of the Act can result in severe financial penalties.

Section 2 - Scope/ Application

(2) Applies to:

a. All campuses
b. All Staff
c. All Colleges, Schools, Departments, Divisional Units and external partners e.g. Navitas/API

Section 3 - Policy Statement

(3) All members of the University are bound by the SPAM Act 2003. The Act and the Use of Computer Facilities Statute 2009 prohibit the sending of SPAM.

(4) The SPAM Act 2003 regulates the sending of one or more commercial electronic messages and prohibits the use of address harvesting software and harvested address lists.

(5) It is prohibited to send unsolicited commercial electronic messages without consent. This applies to messages with an Australian link, either originating in Australia or with an Australian destination, or if the device used to access the message is in Australia.

(6) There is an exemption for educational institutions. Unsolicited commercial messages may only be sent to an electronic account-holder if the following conditions have been met:

a. the sending of the message is authorised by an educational institution; and
b. either or both of the following subparagraphs applies:
    i. the relevant electronic account-holder is, or has been, enrolled as a student at the University;
    ii. a member or former member of the household of the relevant electronic account-holder is, or has been, enrolled as a student at the University; and
c. the message relates to goods or services; and
d. the University is the supplier, or prospective supplier, of the goods or services concerned."

(7) Where any commercial electronic messages are sent there must be a functioning Unsubscribe Facility at the end of each message. The messages must also have clear and accurate sender information.

Section 4 - Procedures

(8) Nil.

Section 5 - Definitions

(9) For the purpose of this Policy:

a. Electronic Message:
    i. A message can be text, graphics or a combination of those.
    ii. Using an internet or other carriage service such as the internet or a mobile telephone service
    iii. To an electronic address (eg: Email addresses or telephone numbers)
    iv. Includes email, SMS, MMS, Instant Messaging and similar services
    v. Voice Calls using standard telephone services are excluded.
b. Commercial Electronic Message:
    i. An Electronic message which has a commercial purpose
    ii. Includes an offer to supply or sell goods or services or to advertise or promote goods.
    iii. Includes for example and email sent offering to supply or promote educational services or business opportunities.
c. Unsolicited: Unasked for or sent without prior consent
d. SPAM: Unsolicited commercial electronic messages
e. Electronic account-holder: The individual or organisation that is responsible for the messaging account. This may be an email address or a telephone number.

Section 6 - Stakeholders

Responsibility for implementation – All staff who are responsible for sending unsolicited electronic messages.

Responsibility for monitoring implementation and compliance – Chief Information Officer.

Status and Details

Status	Current
Effective Date	1st November 2016
Review Date	9th March 2023
Approval Authority	Vice-Chancellor
Approval Date	24th October 2016
Expiry Date	Not Applicable
Unit Head	Peter Powell Chief Information Officer
Author	David Hird Head, Security, Standards and Compliance
Enquiries Contact	Information Services 03) 9479 1500