Monash University Policy

Policy Title	Information Technology Acceptable Use Policy
Date Effective	29 May 2018
Review Date	29 May 2021
Policy Owner	Director, Support Services and Engagement, eSolutions
Category	Operational
Version Number	10.3 *(Minor amendments effective on 02 April 2021)*
Content Enquiries	servicedesk@monash.edu
Scope	For the purpose of this policy, references to 'the University' includes all authorised users: ● accessing Monash University's IT resources; ● connecting personally owned devices to the University network; and/or ● storing any University data on personally owned devices, at Monash University Australia, Monash University Malaysia, Monash University Indonesia, Monash College Pty Ltd, Monash Suzhou and the Monash University Prato Centre, unless otherwise indicated.
Purpose	This Policy sets out the rules applicable to the use of University IT and expresses the commitment of the University to providing and maintaining a secure, effective and reliable IT infrastructure and services to support the University's operations.

POLICY STATEMENT

1. Acceptable and Unacceptable Use of IT

1.1. University IT resources must be used in a lawful, ethical and responsible manner, and in accordance with the Information Technology Acceptable Use Procedure, IT Security Framework, other applicable University policies, and any additional terms of use that may apply to particular software or services.

1.2. University IT resources are provided for use in the academic, administrative, commercial and community activities of the University. Some reasonable non-commercial personal use may be allowed, but as a privilege and not a right, and if that privilege is abused it will be treated as a breach of this policy.

1.3. Account holders must take all reasonable steps to protect their account from unauthorised use.

1.4. Use of University IT resources or BYOD must not jeopardise the fair, secure, and productive IT environment of the University community, nor the University's operations, assets, data integrity or reputation.

1.5. Users must not install or use unlicensed or malicious software on University IT or BYOD, nor circumvent the University's IT security measures.

1.6. Users are expected to report actual or suspected breaches of this policy or other malicious activity that may be a threat to the security of University IT in a timely manner.

2. Breaches of this Policy and its Procedures

2.1. The University treats any breach of its policies, procedures and schedules seriously; it encourages reporting of concerns about non-compliance, and manages compliance in accordance with the applicable Enterprise Agreement, relevant instrument of appointment and/or applicable contract terms. A failure to comply may result in action by the University. Such action may include disciplinary and other action up to and including potential termination of employment for employees, or the cessation of engagements with the University for other persons.

2.2. Breaches of this Policy and its procedures may result in suspension of access to University IT resources.

2.3. Authorised users not related to Monash University may be subject to appropriate action as determined by the University.

2.4. Breaches of this policy and procedure may also be reported to external parties as required under law.

Supporting Procedures	Information Technology Acceptable Use Procedures
Responsibility for implementation	Chief Information Officer: Monash University CEO Monash College
Status	Revised
Approval Body	**Name:** Peter Marshall **Title:** Chief Operating Officer **Date:** 27 – June - 2018
Endorsement Body	**Name:** Chief Information Officer **Meeting:** IT Security and Risk Steering Committee **Date:** 29 – May - 2018
Definitions	**BYOD (Bring Your Own Device):** the practice of allowing authorised users to use their own computers, smartphones, or other devices for work purposes. **Email and Messaging**: Email means the University-provided electronic mail systems and computer accounts. Additional messaging facilities may include but are not limited to calendar and scheduling programs, chat sessions, IRC, newsgroups and electronic conferences. **Information Technology Resources (IT Resources)**: covers all IT facilities owned, leased or hired by the University including all devices such as computers, mobile devices, computing laboratories, lecture theatres and video conferencing rooms across the University together with use of all associated networks, internet access, servers, email, hardware, dial-in access, data storage, computer accounts, software (both proprietary and those developed by the University), telephony services and voicemail. **Authorised User**: any person who has been authorised by the relevant Monash University Officer/Supervisor to access any Monash IT system or IT facility, including but not limited to: • Staff of Monash • Staff of any entity/company in which Monash has an interest

	• Staff of any entity/company /organisation with which Monash is pursuing a joint venture • Students • Consultants • Visitors • Honorary appointees • Collaborative Researchers • Alumni
Legislation Mandating Compliance	• Copyright Act (1968) (Commonwealth) • Trade Marks Act (1995) (Commonwealth) • Competition and Consumer Act 2010 (Commonwealth) • Spam Act (2003) (Commonwealth) • Racial Discrimination Act (Cth) 1975 • Sex Discrimination Act (Cth) 1984 • Telecommunications Act (Cth) 1997 • Privacy and Data Protection Act 2014 No.60 (VIC) • Disability Discrimination Act (Cth) 1992 • Equal Opportunity Act (Vic) 2010 • Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019 (Cth)
Related Policies	• Data Protection and Privacy Procedure • Data Protection and Privacy Schedule - Monash University Malaysia • Resolution of Unacceptable Behaviour & Discrimination Procedure • Copyright Compliance Policy • Equal Opportunity Policy • Electronic Information Security Policy • Access Control (Electronic) Policy • Domain Names Procedures • Paid Outside Work Procedure • Web Accessibility Policy
Related Documents	N/A