INFORMATION TECHNOLOGY ACCEPTABLE USE PROCEDURE

SCOPE

This procedure applies to all Monash University staff, students, associates and visitors accessing and using the University's Information Technology (IT) environments.

For the purpose of this procedure, references to 'the University' include the activities of Monash University Australia, Monash University Malaysia, Monash University Indonesia, Monash College, Monash Suzhou, Monash University Prato Centre and the World Mosquito Program (WMP) Ltd (and its subsidiaries), unless otherwise indicated.

PROCEDURE STATEMENT

The University is committed to ensuring the responsible use of its IT environments to support its education, research, and engagement activities. This procedure details the expected conduct for users within the University's IT environments, including usage expectations and restrictions to ensure user safety and IT security. Users are required to comply with this procedure and the Cyber Security Management Policy.

1. Access to University IT environments

1.1 Access is granted through a Monash University IT account, another organisation's account, or a University-issued guest account.

1.2 Criteria for access include the user's role, the necessity of access, and authorisation from relevant University authorities, managed by designated organisational units, such as University IT teams, the University Library, faculties, and senior leadership.

1.2.1 Some IT environments are provided for specific purposes and are accessible only to users who have received authorisation.

1.2.2 Access to University library resources is contingent upon the specific terms outlined in the relevant licencing agreements and in compliance with the Library Terms of Use. The University Librarian has authority to determine who has access to library resources.

1.3 Users must not share their authentication credentials, including passwords and multi-factor authentication (MFA) codes, and must ensure their University IT environments are not accessed by other staff, students, friends, family, or individuals including third parties. To manage cyber risks, users must refer to the Cyber Security Management Policy and report any suspicious activities or security incidents immediately.

1.4 Access to University IT environments may be restricted or removed if a user does not comply with University policies, procedures and schedules and the expectations set out in mandatory University training modules related to IT and/or cyber security.

1.5 Access to University IT environments is contingent upon a user's ongoing affiliation with the University and will be disabled upon the termination of this affiliation.

1.5.1 Upon approval from the head of unit, portfolio head, or the WMP Director, Digital Technology and Information Management, extended access may be granted to a user for up to 30 days.

1.6 System administrators are responsible for continuously monitoring and updating user access rights, ensuring users have the appropriate permissions to access designated systems to the minimum level necessary to fulfil their roles and responsibilities.

1.6.1 As part of any employment changes, such as internal role changes, supervisors must revoke access permissions associated with a user's previous role within five business days. Managers must notify the relevant University IT team or system administrator of any discrepancy as soon as possible.

1.6.2 If a user becomes aware that they still have access to a University system they no longer have permission to access, they must notify the relevant University IT team or system administrator as soon as possible.

2. Use of University IT environments

2.1 Users are responsible for all activities originating from their accounts and/or when accessing University IT environments. Users must respect user privacy, act responsibly and in accordance with relevant laws, University policies and undertake mandatory training modules. This includes complying with the University's Cyber Security Management Policy, Ethics Statement Policy, Equity, Diversity and Anti-discrimination Policy, Integrity and Respect Policy, Freedom of Speech and Academic Freedom Policy, Data Protection and Privacy Procedure, Data Protection and Privacy Schedule - Monash University Indonesia, Student General Conduct Policy, and Monash College Student Code of Conduct.

2.1.1 Users must also comply with the Terms of Service or Acceptable Use policies of third-party products or services that have been engaged by the University.

2.2 While the University permits incidental personal use of its IT environments, users must ensure that such use does not disrupt the operation or access to these environments, incur additional costs for the University, or conflict with their University obligations.

2.3 Users are personally responsible for their use of social media and must comply with the Media and Social Media Policy.

2.4 Users are responsible for the security of University-issued and personally-owned devices.

2.5 To the extent allowed by law, the University accepts no responsibility for:

- loss or damage, or consequential loss or damage, arising from the use of its IT environments;
- loss of data or interference with files arising from its efforts to maintain the IT environments; and
- users whose actions breach legislation.

Prohibited use

2.6 Users must not use the University's IT environments to:

- engage in threatening, bullying, harassing, stalking, vilifying, victimising or unlawful discriminatory behaviour against any individual;
- use, disclose or collect personal information about staff, associates and/or students contrary to the Data Protection and Privacy Procedure and applicable Collection Statements and Data Protection and Privacy Schedule - Monash University Indonesia;
- compromise academic integrity, such as unauthorised sharing of course material, in accordance with the Student Academic Integrity Procedure;
- infringe upon intellectual property rights or violate privacy rights of others;
- distribute defamatory material that could be actionable under defamation law;
- access or distribute material that is illegal, deceptive, or harmful, thereby exposing the University to potential legal or reputational risks, or posing a threat to any individual;
- unauthorised access or use of another person's account;
- send bulk messages and/or advertising without head of unit or portfolio head approval;
- send unsolicited email (spam) without the recipient's consent;
- interfere with, degrade, impair or deny access to University IT environments, unless explicitly authorised by the relevant University IT team;
- make unauthorised alterations to the University's IT environments, including but not limited to the installations of unauthorised software, hardware or remote access solutions;
- attempt to bypass, tamper or remove cyber security measures or user restrictions; and
- breach the terms of use or agreements for any services (including services provided by a third party) accessed via the University's IT environments.

2.7 Users are prohibited from using University IT environments, including emails and library resources, for private commercial purposes, personal financial gain, or benefiting a third party without authorisation. Use for private commercial activities is only permitted with approval from the Chief People Officer, in line with the Paid Outside Work Procedure, or for WMP staff by the WMP Chief Financial Officer.

Security

2.8 Users are required to:

- comply with the Cyber Security Management Policy to maintain a secure IT environment;
- keep passwords and MFA codes confidential, and note that University IT teams or approved IT services will never request such information;
- refrain from compromising or attempting to compromise the security of any University IT environments, whether belonging to the University or other entities, and avoid exploring any security deficiencies unless explicitly approved by the Group Chief Information Security Officer;
- take reasonable precautions to avoid damage to or theft of devices; and
- ensure that devices are always locked when unattended.

2.9 Users must report any actual or suspected IT/cyber security incidents, including loss of a University device, in accordance with the Cyber Security Management Policy.

Monitoring and access

2.10 University IT staff may monitor devices connected to the network and are authorised to disconnect them in the event of security breaches, legal issues, or policy violations, with or without prior notice based on the urgency of the situation.

2.11 The University reserves the right to access and manage any University-owned or connected device to mitigate risks and ensure network integrity.

2.11.1 The Chief People Officer, or equivalent role at Monash College and WMP Ltd, may authorise the monitoring of staff IT activity in cases of suspected misconduct.

2.11.2 The Chief Operating Officer or the Monash College CEO may authorise the monitoring of student IT activity in cases of suspected misconduct or if there are concerns for the welfare of the student.

2.12 All monitoring activities will comply with legal requirements and will be recorded. Any information obtained will be treated as confidential and shared only with relevant parties.

3. Physical IT assets

3.1 All University staff and associates, along with graduate research students from Monash University Malaysia, may be allocated a standard laptop, desktop computer, tablet and/or smartphone, depending on their specific role requirements.

3.2 In accordance with the University's position on sustainable reuse, assets provided by the University will be in good working order but may not be new.

3.3 All physical IT assets must be acquired through an authorised procurement channel determined by the relevant University IT team. Any device not purchased through this approved process or failing to meet the minimum security standards may be prohibited from accessing the University's IT environments.

3.3.1 Graduate research students at Monash University Malaysia commencing from 2022 onwards, are exempt from this requirement in accordance with clause 3.17.

3.4 The relevant University IT team manages repairs of faulty assets within their warranty period in accordance with the terms provided by the hardware manufacturer. During the repair process, a loan device may be provided if necessary.

3.5 Before returning a University IT asset, users are responsible for saving any important data. The relevant University IT team will then erase all data on the device following their standard procedures for disposal or reuse.

3.6 Staff and associates are responsible for ensuring all University data is deleted from a personally-owned device before disposal, ensuring the data is permanently erased and cannot be retrieved.

Monash University Australia: Asset management

3.7 IT asset management at Monash University Australia and Monash College is overseen by the Vice-President (Services).

3.8 Faculties and portfolios have the option to obtain new assets on a multi-month lease term or single upfront payment in accordance with the Centrally Funded Equipment (CFE) program.

3.8.1 For the acquisition of any additional or non-standard device, including but not limited to tablets and/or smartphones, prior authorisation from the budget approver must be obtained. This authorisation should be explicitly included in any subsequent IT asset requests.

3.8.2 Approval from a head of unit or supervisor may also be required for the acquisition of specific IT assets, such as a smartphone.

3.9 Assets acquired through the CFE program remain the property of the University and will be monitored using a University asset tracking system.

3.9.1 Responsibility of assets that are lost, stolen, damaged beyond economic repair, returned for eWaste, or otherwise unreturned falls on the cost centre that participated in the CFE program. Outstanding payments for the remainder of the lending period will be charged to the responsible cost centre upon identification and reporting of such assets.

3.9.2 Faculties and portfolios will be provided access to reporting tools by eSolutions in order to assist in the management of their IT assets.

3.10 eSolutions reserves the right to demand the return of end-of-life assets to ensure assets are cleansed/sanitised in accordance with the NIST SP 800-88 security standard.

3.11 If an asset is returned to eSolutions before the end of the agreed lending period, whether voluntarily or due to damage, a financial

penalty will be imposed. The penalty will be either the equivalent of a minimum 3-month lease or the remainder of the lease period. This amount will be charged to the relevant cost centre and fund at the time of the asset's return.

Monash University Indonesia: Asset management

3.12 IT asset management at Monash University Indonesia is overseen by Operations and Facilities with support from eSolutions.

3.13 eSolutions at Monash University Australia will support Operations and Facilities in ensuring that all data is erased from an IT asset before being reissued for reuse or disposal.

Monash University Malaysia: Asset management

3.14 IT asset management at Monash University Malaysia is overseen by Campus Infrastructure and Technology Services.

3.15 The standard lifecycle for assets is five years, during which assets will be maintained, updated, and if necessary, replaced to ensure optimal performance and security.

3.16 Casual, temporary or sessional staff will not be issued an IT asset, but may be provided with an asset on loan dependent on availability.

3.17 Graduate research students commencing in 2022 onwards will receive a monetary allowance to purchase a computer device. School representatives must submit a bi-monthly list of commencing graduate research students with a confirmed commencement date to IT Services via Asana. The list must be submitted prior to the graduate research student receiving their allowance.

3.17.1 Upon completion of studies, graduate research students will keep the device as it is categorised as BYOD.

3.17.2 Graduate Research students commencing before 2022 will be assigned with an IT asset (desktop). Monash University Malaysia School representatives need to submit a request through the IT Service Requisition portal five days prior to the student's commencement date. Upon completion of studies, the Research Management Office (RMO) will raise an ITR ticket for IT Services to collect the device.

3.18 When it is determined that an asset is due for an update or replacement, it is the user's responsibility to back up all valuable data.

3.19 When staff movement occurs, whether within or between a School or administration unit or between campuses, it is the School or unit's responsibility to record the movement or re-assignment through the IT Service Requisition portal prior to the movement.

Monash University Prato Centre: Asset management

3.20 IT asset management at Monash University Prato Centre is overseen by Prato IT Services.

3.21 The standard lifecycle for the IT assets at the Prato Centre is five years, during which they will be maintained, updated, and if necessary, replaced to ensure optimal performance and security.

3.22 Prato IT Services manages the acquisition of new or additional devices with guidance and/or advice from eSolutions, and it requires authorisation from the Prato budget approver.

3.23 When it is determined that an asset is due for an update or replacement, it is the user's responsibility to back up all valuable data and bring it back to Prato IT Services.

3.24 Visiting staff from other campuses may be provided with an asset on loan dependent on availability. Responsibility of assets on loan that are lost, stolen, damaged beyond economic repair, or otherwise unreturned falls on the cost centre of the visiting staff member's School or unit.

Monash Suzhou: Asset management

3.25 IT asset management at Monash Suzhou is overseen by the IT and Campus Services team.

3.25.1 The standard lifecycle for assets is three years, during which they will be maintained, updated, and if necessary, replaced to ensure optimal performance and security.

3.25.2 Temporary, sessional or adjunct staff will not be issued an IT asset, but may be provided with an asset on loan dependent on availability.

3.25.3 When it is determined that an asset is due for an update or replacement, it is the user's responsibility to back up all valuable data.

3.25.4 When staff movement occurs, whether within or between a school or administration unit or between campuses, it is the School or Unit's responsibility to record the movement or re-assignment prior to the movement.

World Mosquito Program: Asset management

3.26 Asset management at WMP is tracked in the *WMP Digital Asset Register* and overseen by the Chief Financial Officer. Devices for staff of the WMP's international subsidiaries are procured locally and secured in accordance with the *WMP Device Setup Guide*.

DEFINITIONS

Associate	For the purposes of this procedure, 'associates' are defined as contractors, conjoint appointments, affiliates and adjunct appointees.
Centrally Funded Equipment (CFE) program	The CFE program is a cost recovery program where costs are recovered proportionally in accordance with the lending period and are charged monthly. Monthly payment is spread over 18 months for redeployed assets or 36 months for new assets, full upfront payment is available upon request.
Personal information	Information or an opinion (including information or an opinion forming part of a database) that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.
Physical IT asset	Covers all IT facilities owned, leased or hired by the University including all devices such as computers, mobile devices, monitors, tablets etc.
Student	A person who: a) is admitted to a course of study at the University; b) is enrolled at the University in a non-award study or one or more units of study on an assessed or non-assessed basis and without admission to a course of study; c) is pursuing a course of study or unit of study at the University through an exchange or study program or other arrangement between the University and another educational institution; d) is engaged in a student mobility program involving the University, whether or not the program is credited towards a course of study or unit of study; e) has completed a course of study but on or to whom the relevant degree or award has not been conferred or awarded; f) has deferred, or has intermitted, or has been suspended from, a course of study; g) is enrolled in a course of study or one or more units of study offered by the University through another educational institution; or h) has consented in writing to be bound as a student by the University statute and University regulations. The following terms are used to identify groups of students that are subject to different requirements (as defined below): ● domestic student; ● international student; and ● international student subject to Education and Services for Overseas Students (ESOS) requirements.
University IT environments	For the purpose of this procedure, 'University IT environments' includes all IT infrastructure including electronic devices, hardware, software, networks, websites, systems and services owned or controlled by the University, or a University controlled or associated entity.
University IT team	The IT team responsible for managing user access to University IT environments and physical IT asset management, including: ● Monash University Australia & Monash University Indonesia: eSolutions ● Monash University Malaysia: IT Services ● Monash University Prato Centre: it@monash.it ● Monash Suzhou: SZIT-servicedesk@monash.edu ● Monash College: eSolutions ● World Mosquito Program: dtim-team-group@worldmosquito.org
University networks	The digital environment which provides users the ability to communicate and interact with systems and data, including the wired and wireless network of University computers, all hardware, computer programs/software, mobile devices, servers, mobile provider networks (data carriers and Wi-Fi) and other infrastructure necessary for the operation of the University business regardless of location.

GOVERNANCE

Parent policy	Cyber Security Management Policy
Supporting procedures	
Supporting schedules	
Associated procedures	Data Protection & Privacy Procedure Paid Outside Work Procedure Resolution of Unacceptable Behaviour & Discrimination Procedure
Associated schedules	Data Protection & Privacy Schedule - Monash University Indonesia
Related legislation	***Australia*** Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019 (Cth) Spam Act 2003 (Cth) Privacy and Data Protection Act 2014 (Vic) ***China*** Criminal Law Ninth Amendment 2015 Cyber Security Law 2017 Data Security Law 2021 Personal Information Protection Law 2021 ***Indonesia*** Law No. 11 of 2008 on Electronic Information and Transactions as amended Law No. 27 of 2022 on Personal Data Protection Law ***Italy*** Italian Garante - Personal Data Protection Code (with reference to Regulation (EU) 2016/679) ***Malaysia*** Computer Crimes Act 1997 Cyber Security Act 2024 Personal Data Protection Act 2010
Category	Operational
Approval	Chief Operating Officer 25 July 2024
Endorsement	Vice-President (Services) 15 July 2024
Procedure owner	Group Chief Information Security Officer
Date effective	30 July 2024
Review date	30 July 2027
Version	11.0
Content enquiries	servicedesk@monash.edu