Monash University Procedure

Procedure Title	Information Technology Acceptable Use Procedure
Parent Policy	Information Technology Acceptable Use Policy
Date Effective	29 May 2018
Review Date	29 May 2021
Procedure Owner	Director, Support Services and Engagement, eSolutions
Category	Operational
Version Number	10.6 (Minor amendments effective 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	Protect the essential interests of the University without inhibiting the use of the information technology environment, which is intended for the greater benefit of students, staff and the University .
PROCEDURE STATEMENT	

1. Access to Information Technology Resources

Granting of Access

1.1 Access to the IT resources is restricted to authorised users only.

1.2 Access to IT Resources is authorised by the relevant University Officer/Supervisor, and provided by eSolutions or other organisational unit responsible for managing the IT Resource (e.g. the Library, faculty staff, finance manager).

1.3 Access to IT Resources is based on the user's need to access the resource and their current status within the University.

User Declaration Form

1.4 Users may be required to complete a User Declaration form prior to authorisation being granted for access to certain IT Resources (e.g. Callista).

Restrictions to Access

1.5 Users must not access accounts, data or files on Monash IT Resources or any other IT Resource where prior authorisation by a relevant University officer has not been granted. The administrator of an IT Resource may restrict access to an individual not complying with this.

Third Party Access

1.6 Staff other than eSolutions must not negotiate nor grant third parties access to the University IT Resources, communications and network infrastructure. Applications for access should be made in writing by an authorised Monash staff member via an IT request to the User Access Management team, eSolutions.

Software License Restrictions

1.7 Use of proprietary software is subject to terms of licence agreements between the University and the software owner or licensor, and may be restricted in its use.

Access Cloud Services

1.8 The University provides a range of cloud services that are only to be used for educational, professional and research work-related activities. Use of these sites for storing personal files/information/programs/games is prohibited. The University reserves the right to actively remove content without warning for items that are not deemed appropriate to the University.

Access on expiry of authorised access period

1.9 Email and computer access will cease on expiration of the relationship the authorised user has with the University. For strictly professional or work-related reasons, staff and other authorised users may request that computer access be extended for a period up to 30 days.

1.9.1 To extend computer access, approval must be given by the Head of Unit /Department or Portfolio Head or delegate. Following this approval, the Dean/ Divisional Director or equivalent may subsequently authorise emails to be forwarded to another external email account for a period of up to, but not exceeding, 6 months.

2. Responsibilities of users

When using of University computer accounts, each authorised user is responsible for:

- the security of personally-owned computers and equipment used in conjunction with the University's IT Resources;
- usage of the unique computer accounts which the University has authorised for the user's benefit, these accounts are not transferable;
- selecting and keeping a secure password for each of these accounts, including not sharing passwords and logging off after using a computer;
- co-operating with other users of the ICT facilities to ensure fair and equitable access to the facilities;
- observing the obligations under these Procedures;

- observing the Terms of Service or Acceptable Use policies of third-party products or services that have been engaged by the University; and
- not using IT Resources for private commercial purposes, except where the paid work is conducted in accordance with the University's Paid Outside Work Procedure, or the work is for the purposes of an entity in which the University holds an interest.

The University accepts no responsibility for:

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

3. Internet Usage

Academic, Research and Work Purposes

3.1. Authorised users are permitted to access the internet for academic, work, research-related purposes and communications with staff and other students. All electronic communications must follow the practices outlined below at section 4. 'Email and Messaging'.

Personal Usage

3.2. Access is permitted for personal purposes provided such use is lawful and reasonable in terms of time and cost to the University and is not a prohibited use of IT resources as outlined below at section 6. Examples of permitted personal use are Online banking; Travel bookings; Browsing.

Reasonable Use Determination

3.3. Whether or not use was reasonable in the particular circumstances will be a matter to be determined by the user's Head of Unit or Portfolio Head, or equivalent.

Publication of Personal Web sites

3.4. Authorised users are permitted to publish personal web pages on computers connected to the University network. The content of material on personal websites must be in accordance with:

- relevant laws;
- the standards and principles outlined in this procedure and other related policies and procedures;
- the standing of the user in relation to the University and commensurate with the standard of care owed by the user to the University; and
- the University mission and strategy.

3.5. The University reserves the right to regularly monitor personal websites hosted on Monash servers, and to remove material, or request the user to remove or alter the content on their personal website should it be inconsistent with any of the above.

3.6. Special care must be taken with regard to web contents not infringing on any third-party copyright.

Disclaimer Required on Personal Web Pages

3.7. A personal website must carry the Monash Personal Page Disclaimer as a standard disclaimer on every page. The disclaimer states that the website is not authorised by Monash University and that any opinions expressed on the pages are those of the author and not those of the University.

Responsibility for Personal Websites

3.8. Legal responsibility for personal websites rests with the user. The University will not defend a user named in an action arising from material published on a personal website and will not be liable for any damages awarded against the user by a court or commission.

4. Email and Messaging

User Responsibilities

4.1. When using the email or messaging system users must always:

- respect the privacy and personal rights of others;
- take all reasonable steps to ensure copyright is not infringed – refer section 'Forwarding of Emails – Privacy and Ownership of Copyright';
- take all reasonable care not to plagiarise another person's work;
- not forward or otherwise copy a personal email (except with permission of the author) or an email which contains personal information or an opinion about a person whose identity is apparent (except with permission of that person);
- not send forged messages, or obtain or use someone else's email address or password without proper authorisation;
- not send mass distribution bulk messages and/or advertising without approval of the user's Head of Unit or Portfolio Head;
- not send SPAM. The user must ensure that the recipient(s) of the intended email have consented to receive such email(s);
- not intimidate or threaten another person/s;
- not send sexually explicit material, even if it is believed that the receiver will not object. Remember, the intended receiver may not be the only person to access the communication; and
- adhere to the practices as set out in this procedure.

Standards Required When Using Email

4.2. Appropriate standards of civility should be used when using e mail and other messaging services to communicate with other staff members, students or any other message recipients. Further information can be found in the Behaviours in the Workplace Procedure for staff, and in the Student Charter.

Forwarding of Emails – Privacy and Ownership of Copyright

4.3. Monash owns copyright in all email correspondence created by members of its staff in relation to their employment duties, except in correspondence created by academic staff in respect to their research or being conducted in accordance with the University's Paid Outside Work Procedure.

4.4. Copyright in work-related email will not be infringed by forwarding a message to another staff member or interested party (such as a consultant providing services to the University) on a need-to-

know basis. However, care must be taken if an email contains personal information. This kind of information must not be forwarded or copied without prior permission from the person who is the subject of the personal information.

4.5. Copyright in a personal/non-work related email belongs to the writer of the message. A personal email must never be copied or forwarded without permission of the writer.

Commercial Usage Prohibited

4.6. The private commercial use of email and messaging is not allowed. Messaging and email must not be used for private commercial purposes except where the paid work is conducted in accordance with the University Paid Outside Work Procedure, or the work is for the purposes of an entity in which the University holds an interest.

5. Security of Information Technology Resources and Data

Authorised User's Responsibilities

5.1. Authorised Users have a responsibility to always:

- act lawfully;
- keep all Monash IT Resources secure and to observe the Monash Electronic Information Security Policy;
- not compromise or attempt to compromise the security of any IT Resource belonging to Monash, other organisations or individuals, nor exploit or attempt to exploit any security deficiency;
- take reasonable steps to ensure physical protection including mitigating the risk of damage from improper use, food and drink spillage, electrical power management, anti-static measures, protection from theft, and sound magnetic media practices;
- ensure computers are not left unattended without first logging-out and/or securing the entrance to the work area – particularly if the computer system to which they are connected contains sensitive or valuable information; and
- adhere to the requirements as set out in this procedure.

Records Management

5.2. Authorised Users are required to always:

- take reasonable steps to ensure that important University data is stored appropriately on University infrastructure for preservation and backup;
- ensure course materials are placed on official University infrastructure;
- ensure course materials are not placed on personal web pages or servers; and
- observe appropriate University record management protocols.

Confidential Information

5.3. Authorised Users have a duty to keep confidential:

- all University data unless the information has been approved for external publication; and
- information provided in confidence to the University by other entities.

5.4. Each staff member is under a duty not to disclose University business information unless authorised to do so. Breach of confidentiality through accidental or negligent disclosure may expose a User to disciplinary action.

6. Prohibited use of Information Technology Resources

Monash Name, Crest and Logo

6.1. The Monash Name, crest or logo may only be used with prior approval from the Chief Marketing Officer. All use must be in accordance with the Monash University Brand Guide, or with the prior approval of the Chief Marketing Officer.

Advertising and Sponsorship

6.2. Paid advertisements are not permitted on any website using a Monash domain name, personal website or any website, which has a substantial connection with the University (such as a website for a research program) except with the prior written permission of the Chief Operating Officer .

Business Activities

6.3. Authorised users are not permitted to run a business or publish a non-Monash journal/magazine (unless prior written authorisation has been obtained from the University) on Monash IT Resources.

6.4. Users must not publish their Monash email address on a private business card.

Databases, online journals, eBooks

6.7. Use of electronic resources provided by Monash is governed by individual licence agreements and is for non-commercial research and study purposes only. Users are required to comply with use restrictions set out on the specific site or stated in the licence agreement, and must not systematically download, distribute or retain substantial portions of information. Using software, including scripts , agents or robots is prohibited and may result in loss of access to the resource for the whole Monash community.

6.8. Any use of electronic resources for teaching purposes must comply with the contractual terms of use of the electronic resource from which the material was sourced. Each electronic resource has its own set of contractual terms. To check whether your proposed usage falls within the relevant contractual terms, send an email to lib-eResources-l@monash.edu. Your email should include a description of the way in which you propose to use the material and the names of the electronic resources (and journals) from which the material was sourced.

Peer to Peer File Sharing

6.9. Installation or use of peer-to-peer file sharing software such as Kazaa, BitTorrent, DC++ (Direct connect) etc is not permitted on the Monash network. Exceptions for legitimate teaching or research use must be approved by the Head of Unit or Portfolio Head or delegate, and only where no alternative technology is appropriate.

Pornography

6.10. Authorised users are not permitted to utilise the University's IT Resources to access pornographic material or to create, store or distribute pornographic material of any type.

7. Privacy and Surveillance

Security and Privacy

7.1. The accounts, files and stored data including, but not limited to, email messages belonging to users at the University are normally held private and secure from intervention by other users, including the staff of eSolutions.

7.2. Authorised Staff, including authorised delegates, may disconnect IT equipment from the University network when monitoring detects a breach in IT security, a breach of the law or University policy. Such disconnection would normally be preceded by notice to the relevant authorised user, but in an emergency, notice will follow disconnection.

7.3. Users should be aware that eSolutions staff may from time to time become aware of the contents of user directories and hard disk drives in the normal course of their work, and they are bound to keep this information confidential.

Access to and Monitoring

7.4. The University reserves the right to access and monitor:

- any computer or other electronic device owned or controlled by the University; and
- any computer or other electronic device connected to the University network. The University reserves the right to remove access or disconnect systems and services where risk is identified to the University.

7.5. Authorised staff may access or monitor an authorised user's computer or other electronic devices in circumstances including, but not limited to:

- suspected breaches by the user of their duties as a staff member; and
- unlawful activities or breaches of University policies.

7.6. Access to location services on devices must be authorised by the Director, Workplace Relations or delegate. Access may be authorised for circumstances including, but not limited to:

- suspected breaches of policy/procedure by an authorised user; or
- unlawful activities; or
- lost/stolen devices; or
- locate missing staff; or
- facilitating an emergency response in times of crisis;
- providing information to relevant emergency services sector organisations for the purpose of staff safety; or
- other reasons as determined appropriate by the Director, Workplace Relations or delegate.

7.7. Access to and monitoring includes, but is not limited to, email, websites, server logs and electronic files. Information obtained under this approval will be treated as confidential, and only disclosed to relevant parties.

7.8. The University may engage third parties to provide monitoring services for leaked or compromised University information, which may include, but is not limited to, University email addresses.

7.9. The University may keep a record of any monitoring or investigations.

7.10. Prior approval must be obtained from the Divisional Director, Human Resources Division (or nominee), before a user's email, files or data may be accessed by authorised staff. Any

information obtained under this approval will be treated as confidential, and only disclosed to relevant third parties. Access to the information will be strictly on a need-to-know basis.

Responsibility for implementation	Chief Information Officer CEO, Monash College PVC Monash University Malaysia PVC Monash University Indonesia PVC Monash Suzhou
Status	Revised
Approval Body	**Name:** Chief Information Officer **Meeting:** IT Security and Risk Steering Committee **Date:** 29-May-2018
Definitions	**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. **Monash University Officer/Supervisor:** Dean, Head of Organisational Unit or Registrar or other such staff member who has the authority (or delegated authority) to recommend a staff appointment. **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. **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 Monash business regardless of location. **Personal Web Page**: Personal web pages are those pages produced by authorised users that are not directly related to work responsibilities. They may not include any commercial information and must not under any circumstances be used for business-related activities. They cannot be placed on official websites. Any web server that hosts official and personal pages must make a clear and unambiguous distinction between the official site and the personal page area.

	Refer to Web page definitions **Publish**: to make information available for access by others via any method or format, including, but not limited to, on a web page, email, or the use of peer-to-peer programs. **Electronic device:** is any device capable of making or transmitting still or moving photographs, video recordings, or images of any kind; any device capable of creating, transmitting, or receiving text or data; and any device capable of receiving, transmitting, or recording sound. **Authorised User**: any person who has been authorized 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. SPAM: irrelevant or unsolicited messages sent over the internet, typically to a large number of users.
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 The Surveillance Devices Act 1999 Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019 (Cth)

Related Policies	Data Protection & Privacy Procedure Data Protection & Privacy Schedule - Monash University Indonesia Resolution of Unacceptable Behaviour & Discrimination Procedure Copyright Compliance Policy Equal Opportunity Policy Electronic Information Security Policy Domain Names Procedures Paid Outside Work Procedure Web Accessibility Policy
Related Documents	N/A