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	10.5
Content Enquiries	eSolutions Service Desk (ext. 51777 or servicedesk@monash.edu)
Scope	All University students, staff, honorary appointees, contractors; and guest/visitors of the University; plus, any authorised users or organisations using or accessing Monash's IT resources. This procedure also applies to users connecting personally owned devices such as laptop computers, smartphones and tablets to the University network, and/or storing any University data on such devices and/or on any cloud services.
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 in general.
PROCEDURE STATEMENT	

This procedure protects 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 in general.

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 Monash University Officer/Supervisor, and provided by eSolutions or other organisational unit responsible for managing the IT Resource (eg, the Library, faculty staff, finance manager).

1.3 Access to IT Resources are to be 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.

Restrictions to Access

1.5 Users are explicitly forbidden access to accounts, data or files on Monash IT Resources or any other IT Resource where prior authorisation by a relevant Monash 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 Entities other than eSolutions may neither negotiate nor grant third parties access to the University IT Resources, communications and network infrastructure. Applications for access should be made in writing by a valid permanent 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 Monash University and the software owner or licensor, and may be restricted in its use.

Access Cloud Services

1.8 Monash University provides a range of cloud services, these are to be used for only 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 which 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.

1.10 Approval must be given by Head of Department or equivalent. Following this approval, an option to forward email to another external email account can be authorised by the Dean/Divisional Director or equivalent and shall not exceed 6 months.

2. Responsibilities of users

Regarding use of Monash 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 transferrable;
- 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;
- Not using IT Resources for private commercial purposes, except where the paid work is conducted in accordance with the University Practice and Paid Outside Work Policy, or the work is for the purposes of a corporate entity in which Monash University holds an interest.

- Familiarising themselves with legislative requirements which impact on the use of IT Resources and acting accordingly, using the University IT Resources in an ethical and lawful way, in accordance with Australian laws/relevant local laws where a student is based in another country;

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;
- Users whose actions breach legislation – for further information refer to the section of this policy titled 'Relevant Australian Legislation, Policies and Associated Documentation'.

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 in the section '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 does not fall under section 6 of this document '*Prohibited use of Information Technology Resources'.*

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 Department or Administrative Head.

Publication of Personal Web sites

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

- Relevant laws, particularly Copyright Law;
- The standards and principles contained in this procedure;
- 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.

3.5. The University reserves the right to regularly monitor personal web sites hosted on Monash servers, and to remove material, or request the user to remove or alter the content on their personal web site 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 web site must carry the Monash Personal Page Disclaimer as a standard disclaimer on every page. The disclaimer states that the web site 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 Web sites

3.8. Legal responsibility for personal web sites rests with the user. The University will not defend a user named in an action arising from material published on a personal web site 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 plagiarize another person's work; or defame another person;
- 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 e-mail address or password without proper authorisation;
- Not send mass distribution bulk messages and/or advertising without approval of the user's Head of Department, or Administrative Head;
- Not send SPAM (refer Relevant Australian Legislation). The user must ensure that the recipient(s) of the intended email have consented to receive such email(s);
- Not harass, 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. When using the email or messaging system users must not send:

- **Angry or Antagonistic Messages:** these can be perceived as bullying or threatening and may give rise to formal complaints under grievance procedures or discrimination/sexual harassment procedures; or
- **Offensive, Intimidating or Humiliating Emails**: University IT Resources must not be used to humiliate, intimidate or offend another person/s based on their race, gender, or any other attribute prescribed under anti-discrimination legislation. Commonwealth and State laws and the University Equal Opportunity policy prohibit sexual harassment and discrimination,

vilification or victimisation on certain grounds such as race, gender, sexual orientation, disability, or status as a parent or carer.

Forwarding of Emails – Privacy and Ownership of Copyright

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

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 Monash) 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 e-mail belongs to the writer of the message. A personal e-mail must never be copied or forwarded without permission of the writer.

Commercial Usage Prohibited

4.6. The private commercial use of e-mail and messaging is not allowed. Messaging and e-mail must not be used for private commercial purposes except where the paid work is conducted in accordance with the University Practice and Paid Outside Work Policy, or the work is for the purposes of a corporate entity in which Monash University holds an interest.

Forwarding of emails after contract expiry or end-date

4.7. Email and computer access will cease on expiration of contract or end-date as recorded in the SAP Human Resources database. An option to forward email to another external email account for professional or work-related reasons must be authorised by the Dean/Divisional Director or equivalent and shall not exceed 6 months.

Course materials: Making copyright material available online

4.8. Under the educational statutory licences, educational institutions are limited in what they can make available online. To avoid infringement, it is recommended that staff use the online reading list service provided by the library when making text or images available online under the Part VB licence or when linking to electronic resources.

5. Security of Information Technology Resources and Data

Authorised User's Responsibilities

5.1. Authorised Users have a responsibility always to:

- 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 damage from improper use, food and drink spillage, electrical power management, anti-static measures, protection from theft, and sound magnetic media practices;

- Ensure their 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 practices as set out in all sections of this procedure.

Records Management

5.2. Authorised Users are required always to:

- Take reasonable steps to ensure that important University data is stored appropriately on Monash infrastructure for preservation and backup;
- Ensure course materials are placed on official Monash infrastructure;
- Ensure course materials are not placed on personal web pages or servers; and
- Observe appropriate University record management protocols such as the Electronic Mail Recordkeeping Protocol.

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.

Personal Information

5.5. Personal information about an individual, including personal information that is also Health Information, must not be disclosed without consent of the individual concerned. However, Privacy legislation does provide for release of personal information without consent in certain circumstances (e.g. where the information is requested by the police or where the University has reason to suspect that unlawful activity has been, or is being engaged in, such as intentional infringement of copyright). A decision on the legality of disclosure in the circumstances must be made by the University's Privacy Officer or theOffice of General Counsel.

University Liability

5.6. The University accepts no responsibility for:

- Loss or damage or consequential loss or damage, arising from the use of the University's IT Resources; and
- Loss of data or interference with files arising from the University's efforts to maintain the IT Resources.

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 Visual Identity Manual or with the prior approval of the Chief Marketing Officer.

Monash University Procedure

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 written permission of the Chief Operating Officer & Senior Vice-President.

No 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.

Unauthorised Access

6.5. Authorised users are expressly forbidden from unauthorised access or attempting to gain unauthorised access to IT Resources belonging to other organisations or other users.

Infringement of Copyright

6.6. Authorised users are expressly forbidden to engage in any infringing conduct. Wilful or negligent infringement of copyright may attract

- Personal liability for damages
- Denial of access to computer facilities
- Disciplinary action.

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 School or equivalent, 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 may disconnect IT equipment from the Monash University network when monitoring detects a breach in IT security or 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 Monash University; and
- Any computer or other electronic device connected to the Monash University network. The University reserves the right to remove access or disconnect systems and services where risk is identified to the University.

7.5. University officers may access or monitor 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 legislation and policies.

7.6. Access to location services on devices needs to be authorised by the Director Workplace Relations, such access may include in 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 University.

7.7. Access to and monitoring includes, but is not limited to email, web sites, 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.

Monash University Procedure

Responsibility for implementation	Chief Information Officer PVC and President: Monash South Africa PVC and President: Monash University President Monash College PVC Malaysia Campus
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 web-sites. 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.

Monash University Procedure

	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.
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	• Privacy Policy • Monash University Brand Guidelines • Monash University Resolution of Unacceptable Behaviour & Discrimination Procedure • Copyright Compliance Policy • Monash University Enterprise Agreements • Monash University Global Equal Opportunity Policy • Electronic information security policy

Monash University Procedure

	• Monash University –Access Control Policy • Monash Domain Names Procedures • Monash University Practice & Paid Outside Work Policy • Monash University Software Catalogue • Monash University Workplace Policies and Procedures • Monash Web Policy (Web Page Definitions) • Monash Personal Page Disclaimer
Related Documents	N/A