

Information Technology Use Policy - Staff & Other Authorised Users

For Use by University Staff and Other Authorised Users of Information Technology Resources

Policy Statement

This policy deals with the provision of information technology resources by Monash University and the associated responsibility of authorised users when accessing these information technology resources. These resources include, but are not limited to, the Monash network, computer systems and software, access to the Internet, electronic mail, telephony and related services.

The policy is based on the following principles, which must be adhered to by all those responsible for the implementation of this policy and to whom this policy applies:

- The information technology resources of Monash University are provided to support the teaching, research and administrative activities of the University;
- Authorised users are granted access to valuable University resources, sensitive data and to external networks on the basis that their use of IT resources shall be responsible, ethical and lawful at all times;
- Authorised users are required to observe University policy, and Australian or other local laws which may apply;
- Data and information relating to persons and other confidential matters acquired for business purposes shall be protected;
- University Business information shall be protected from unauthorised and/or accidental disclosure; and
- University IT resources must not under any circumstances be used to humiliate, intimidate, offend or vilify others on the basis of their race, gender, or any other attribute prescribed under anti-discrimination legislation.

Broad Overview

1. **What Is Provided and Why** – The information technology resources of Monash University are provided to support the teaching, research and administrative activities of the University. These resources include the Monash network, computer systems and software, access to the Internet, electronic mail, telephony and related services.
2. **Access** – This policy prescribes the conditions under which access to Monash IT resources is granted.
3. **Responsible Usage** – Staff and other specifically authorised users who are granted access to IT resources are required to utilise IT resources in a responsible, ethical and lawful manner.
4. **What is and is Not Acceptable Usage** – This policy, to which all staff and other authorised users should adhere, identifies what is acceptable usage including the personal use of IT resources.
5. **Breach of Policy** – This policy identifies the possible consequences should a breach of the policy occur.

Application	All University staff, honorary appointees, contractors; and guest/visitors of the University; plus any authorised users or organisations accessing Monash's IT resources.
Operative Date	Effective immediately
Policy Authorisation	Vice-Chancellor's Group
Policy Administrator	Director - Client Services, Information Technology Services Division Director, Policy and Consultancy, Human Resources Division

DETAILED POLICY

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 including all computers, computing laboratories, lecture theatres and video conferencing rooms across the University together with use of all associated networks, internet access, 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 means 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.

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 <http://www.its.monash.edu.au/policies/web-page-definitions.html>

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.

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.

For information relating to Acceptable use of information technology facilities by students refer to the Executive Services Policy Bank <http://www.adm.monash.edu.au/execserv/policies/Information-Technology-Policies/Acceptable-use-of-information-technology-facilities-by-students.html>

ISSUES ADDRESSED

1. Access To Information Technology Resources

1.0 Lawful Use

The use of IT Resources must be lawful at all times. Unlawful use will breach this Policy and will be dealt with as a discipline offence.

Unlawful use of IT Resources may also lead to criminal or civil legal action being taken against individual authorised users. This could result in serious consequences such as a fine, damages and/or costs being awarded against the individual or even imprisonment.

The University will not defend or support any authorised user who uses IT resources for an unlawful purpose. For further information on some (but not all) relevant laws, refer to the section of this policy titled Relevant Australian Legislation, Policies and Associated Documentation.

1.1 Granting of Access

Access to IT Resources is authorised by the relevant Monash University Officer/Supervisor, and provided by the Information Technology Services Division or other organisational unit responsible for managing the IT Resource (eg, the Library). Access is normally based on a need to access that IT Resource and an individual's current status with the University as recorded in the University's SAP Human Resources database, University Alumni database or other database managed by the Information Technology Services Division or the Human Resources Division or Student and Community Services Division.

1.2 User Declaration Form

Users may be required to complete a User Declaration form prior to authorisation being granted for access to certain IT Resources.

1.3 Access on contract expiry or authorised access period

Email and computer access will cease on expiration of contract or end-date as recorded in the SAP Human Resources database. 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. 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.

1.4 Responsibilities

Regarding Use of Monash University Computer Accounts

Each authorised user is responsible for:

- 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; and
- Familiarising themselves with legislative requirements which impact on the use of IT Resources and acting accordingly. The University takes no responsibility for users whose actions breach legislation – for further information refer to the section of this policy titled Relevant Australian Legislation, Policies and Associated Documentation.

1.5 Restrictions to Access

Users are expressly forbidden unauthorised access to accounts, data or files on Monash IT Resources or any other IT resource. The Administrator of an IT Resource may restrict access to an individual user on the grounds that the user is in breach of this policy.

1.6 Third Party Access

Entities other than Information Technology Services may neither negotiate nor grant third parties access to the University communications and network infrastructure. Applications for access should be made in writing to the Office of the Executive Director, Information Technology Services Division.

1.7 Domain Name Registration

All domain names for Monash projects/activities must be registered through the Office of the Executive Director, Information Technology Services Division. This requirement must be observed in all instances. Users should note it is the University who owns and controls the site not the person who registers the name.

1.8 Software License Restrictions

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. See the Software Catalogue in the Schedule to this Policy.

2. Personal Use of Information Technology Resources

2.1 Extent of Personal Use

A user who is authorised to use the IT Resources may also use the IT Resources for limited, incidental personal purposes. Personal use of the IT Resources is permitted provided such use is lawful, does not negatively impact upon the user's work performance, hinder the work of other users, or damage the reputation, image or operations of the University. Such use must not cause noticeable additional cost to the University.

2.2 Commercial Use

IT Resources 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.

2.3 Reasonable Use Determination

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.

2.4 University Liability

The University accepts no responsibility for:

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

3. Internet, Email and Messaging

3.1 Access to the Internet

3.1.1 Work Purposes

Authorised users are permitted to access the Internet for work related purposes.

3.1.2 Personal Usage

Access is also permitted for personal purposes provided such use is lawful and reasonable in terms of time and cost to the University.

Examples of permitted personal use are:

- Online banking,
- Travel bookings
- Browsing.

3.1.3 Reasonable Use Determination

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.

3.2 Personal Web Pages

3.2.1 Publication of Personal Web Pages

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

- Relevant laws, particularly Copyright Law: see Schedule to this Policy;
- The standards and principles contained in this Policy;
- 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.

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

Special care must be taken with web pages not to infringe any third party copyright in an audio or video file, music charts/lyrics, photographs or text.

3.2.2 Disclaimer Required on Personal Web Pages

A personal web page site must carry the Monash Personal Page Disclaimer as a standard disclaimer on every page. The disclaimer states that the web page 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.

3.2.3 Responsibility for Personal Web Pages

Legal responsibility for personal pages 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.

3.3 Email and Messaging

3.3.1 User Responsibilities

When using the email or messaging system users must at all times:

- Respect the privacy and personal rights of others;
- Take all reasonable steps to ensure copyright is not infringed – refer section 3.3.3;
- 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 – refer also to section 3.3.2;
- 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 – refer to section 3.3.2; and
- Adhere to the practices as set out in sections 3.3.2, 3.3.3 and 3.3.4 below.

3.3.2 Standards Required When Using Email

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 on the basis of 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 preference, disability, or status as a parent or carer.

3.3.3 Forwarding of Emails – Privacy and Ownership of Copyright

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.

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**. Under the Information Privacy Act 2000 (Vic), "**Personal Information** means information or an opinion, whether true or not, about a person whose identity is apparent". This kind of information must not be forwarded or copied without prior permission from the person who is the subject of the personal information.

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.

Copyright will be infringed if you send, without permission of the copyright owner, an audio or video file, music charts/lyrics, commercial photographs, journal article or report to another person using email.

3.3.4 Commercial Usage Prohibited

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.

3.3.5 Forwarding of emails after contract expiry or end-date

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.

3.4 Course materials: making copyright material available online

Under the licence given to educational institutions in the Copyright Act 1968 (Cwth), as amended, a user is not permitted to make available online a part of a Work or off-air broadcast while any other part of that Work/broadcast is available online at the institution and continues to be so available. Failure to observe this requirement will constitute infringement of the copyright owner's right to communicate a Work. To avoid infringement, Copyright material should only be made available through the University's Centre for Digital Copying, managed by the central University Library, Clayton campus.

4. Security of Information Technology Resources and Data

4.1 Authorised User's Responsibilities

Authorised Users have a responsibility at all times to:

- Act lawfully;
- Keep all Monash IT Resources secure and to observe the Monash IT Security Policy;
- Not compromise or attempt to compromise the security of any IT Resource belonging to Monash or 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 sections 4.2, 4.3 and 4.4 below.

4.2 Records Management

Authorised Users are required at all times to:

Take reasonable steps to ensure that important University data is stored appropriately on Monash servers for preservation and backup;
Ensure course materials are placed on official Monash servers;
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.

4.3 Confidential Information

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.

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

4.4 Personal Information

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 particular circumstances must be made by the University's Privacy Officer or the University Solicitor's Office.

4.5 University Liability

The University accepts no responsibility for:

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

5. Prohibited use of Information Technology Resources and Possible Consequences

5.1 Monash Name, Crest and Logo

The Monash Name, crest or logo may only be used with prior approval from the Executive Director, Marketing and Public Affairs. All use must be in accordance with the Monash University Visual Identity Manual or with the prior approval of the Executive Director, Marketing and Public Affairs.

5.2 Advertising and Sponsorship

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 Senior Deputy Vice-Chancellor and Senior Vice-President.

5.3 No Business Activities

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. Users must not publish their Monash e-mail address on a private business card.

5.4 Unauthorised Access

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

5.5 Infringement of Copyright

Authorised users are expressly forbidden to engage in any of the conduct described in the Schedule as infringing conduct. Wilful or negligent infringement of copyright (for example on personal pages or in breach of the statutory licence (CAL) may attract

- Personal liability for damages
- denial of access to computer facilities
- disciplinary action.

5.6 Databases, online journals, ebooks

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.

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. 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.

5.7 Peer to Peer File Sharing

Installation or use of peer to peer file sharing software such as Kazaa, BitTorrent, 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.

5.8 Pornography

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

5.9 Gambling

Authorised users are not permitted to utilize the University's IT Resources to gamble.

5.10 Possible Consequences

5.10.1 For Monash University Staff

Staff found to have breached this policy will be subject to disciplinary action in accordance with the disciplinary procedures contained in the Monash University Enterprise Agreement or the relevant AWA Terms and Benefits Policy and the Monash University Workplace Policies and Procedures as amended from time to time. Criminal offences will be reported to the police.

5.10.2 Authorised Users Other Than University Staff

Authorised users (other than Monash University staff) found to have breached this policy may be subject to appropriate action as determined by the University. Such action may include but is not limited to; sanctions and/or removal of access to Monash University IT Resources. Criminal offences will be reported to the police.

6. Privacy and Surveillance

6.1 Security and Privacy

The accounts, files and stored data including, but not limited to, e-mail messages belonging to users at the University are normally held private and secure from intervention by other users, including the staff of the Information Technology Services Division.

There are situations in which duly authorised Information Technology Services staff may be required to intervene in user accounts, temporarily suspend account access or disconnect computers from the network in the course of maintaining the University's IT Resources such as repairing, upgrading or restoring file servers or personal computer systems.

Users should be aware that Information Technology Services 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.

6.2 Access to and Monitoring

The University does not generally monitor e-mail, files or data stored on University IT resources or traversing the University network. However, the University reserves the right to access and monitor any computer or other electronic device connected to the Monash University network. This includes equipment owned by the University and personal computing equipment (e.g. laptops) that are connected to the network.

Access to and monitoring of equipment is permitted for any reason, including but not limited to, suspected breaches by the user of his/her duties as a staff member, unlawful activities or breaches of University legislation and policies. Access to and monitoring includes, but is not limited to e-mail, web sites, server logs and electronic files.

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

6.3 Prior Approval Required

Prior approval must be obtained from the Divisional Director, Human Resources Division (or nominee), before a user's e-mail, 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 3rd parties. Access to the information will be strictly on a need-to-know basis.

SCHEDULE

Relevant Australian Legislation, Policies and Associated Documentation

Copyright

Copyright Act (1968) (Commonwealth)

Copyright protects intellectual property rights in literary (including computer programs), dramatic, musical and artistic works (includes photographs/charts/maps) and in films/videos, recordings/tapes and TV and radio broadcasts. Use of any part of a copyright work without permission of the copyright owner will infringe copyright unless the use was for your personal research or study/criticism and review and in accordance with the fair dealing provisions of the Copyright Act OR for the educational purposes of the University and in accordance with the statutory licence in the Copyright Act (1968) (Commonwealth).

Duration of Copyright and Infringement

The duration of copyright protection is generally 70 years following the death of the author. During this period, the copyright owner has the exclusive right to reproduce a work and to communicate (ie transmit electronically) a work to the public. A user will infringe the owner's copyright in a work if he/she copies a work or makes it available on line:

- outside the terms of the licence to educational institutions; or
- without prior permission of the copyright owner.

Infringement of copyright will expose a user to personal liability for damages.

Hypertext Links - Users should assume that all materials published on the web are in copyright, unless explicitly stated otherwise. If a user wishes to include material from another webpage in their own webpage, they should create a hypertext link pointing to the material rather than copy it. It is suggested that the permission of other webpage owners be sought prior to creating links to their pages. Permission must always be obtained from the owner prior to directing students to copy/download material from an external web site.

Conduct that infringes copyright

Examples of conduct that infringes copyright if undertaken without the permission of the copyright owner (eg. the relevant recording company), includes but is not limited to:

- a. converting a CD to an audio format, such as MP3, and using it on a PC;
- b. downloading a film, MP3 recordings, or software from the internet using University internet access or computers;
- c. uploading audio files, video files, software or commercial photographs, to a University website and making these available to the public;
- d. providing on a University website, links to other websites that directly offer copyright infringing material or direct users to copyright infringing material, including audio files such as MP3 recordings, video files, software or commercial photographs;
- e. sending copyright material, including audio files, such as MP3 recordings, video files, commercial photographs or software, to another person using University e-mail;
- f. storing copyright material, including audio files, such as MP3 recordings, video files, commercial photographs or software, on University computers or servers.

Copyright infringement could apply to any file format, including, but not limited to MP3.

Trademarks and Logos

Trade Marks Act (1955) (Commonwealth)

A user must not copy a trademark or logo belonging to another party. Trademark infringement may expose the user to liability for damages.

Misleading and Deceptive Conduct

Trade Practices Act (1974) (Commonwealth)

The Trade Practices Act contains provisions which prohibit passing off and misleading and deceptive conduct. For example, if a user were to copy material from an external site onto a Monash website (including features such as logos and trademarks) so that persons accessing the website would believe that Monash had been authorised to carry the material, this would constitute passing off or deceptive or misleading conduct.

Spam

Spam Act (2003) (Commonwealth)

This legislation sets up a scheme for regulating commercial e-mail and other types of commercial electronic messages. Under the Act, users must not send unsolicited commercial electronic messages, i.e. messages that are sent without the recipient's consent. Any commercial messages that are sent electronically (including email, instant messaging or

telephone accounts) must include information about the individual or organisation which authorised the sending of the message and provide for a functional unsubscribe facility.

Discrimination and Harassment

Anti-Discrimination Legislation

State and Commonwealth legislation prohibits discrimination on the basis of age, impairment/imputed impairment, industrial activity, lawful sexual activity, marital status, physical features, political belief or activity, pregnancy, race, religious belief or activity, sex, parental status or status as a carer. It is also prohibited to victimise a person who has made a complaint of discrimination under these Acts.

Defamation

A user must not publish a statement about another person (or entity) which could harm that other person's (or entity's) reputation. There is no need for the person to have been named specifically if he/she can reasonably be identified. Photographs and cartoons can also be defamatory if they hold someone up to ridicule or contempt. In a defamation case, truth is not always a defence.

Illegal material

Commonwealth and State laws prohibit publication of hard core pornography (in particular where it involves children, bestiality, violence, cruelty and/or exploitation). A breach of these laws would constitute a criminal offence and will also result in disciplinary action under the University's disciplinary procedures.

Incitement to commit a crime

Users must not publish material which is an incitement to commit or instruction in crime eg, material on how to prepare explosive devices, or how to steal.

Associated Policies and Legislation (including Guidelines & Procedures)

- Copyright Act (1968) (Commonwealth) – refer Monash University Copyright Website <http://www.copyright.monash.edu.au>
- Disability Discrimination Act (Cwlth) 1992 <http://scaleplus.law.gov.au/html/pasteact/0/311/top.htm>
- Equal Opportunity Act (Vic) 1995 http://www.austlii.edu.au/au/legis/vic/consol_act/EOA1995250/
- Privacy Policy <http://www.privacy.monash.edu.au/policies/privacy-policy.html>
- Monash University Brand Guidelines <http://www.adm.monash.edu.au/advancement/brand/>
- Monash University Discrimination and Sexual Harassment Grievance Procedures <http://www.adm.monash.edu.au/workplace-policy/> and <http://www.adm.monash.edu.au/sss/equity-diversity/equal-opportunity/discrim-procedures.html>
- Monash University Electronic Mail Recordkeeping Protocol <http://www.adm.monash.edu.au/records-archives/rmo/monash-only/email.html>
- Monash University Enterprise Agreements <http://www.monash.edu.au/entbarg/>
- Monash University Global Equal Opportunity Policy

**Associated Policies
and Legislation
(including
Guidelines &
Procedures)**

<http://www.adm.monash.edu.au/sss/equity-diversity/equal-opportunity/policies/globaleopol.html>

- Acceptable use of information technology facilities by students available at
<http://www.adm.monash.edu.au/execserv/policies/Information-Technology-Policies/Acceptable-use-of-information-technology-facilities-by-students.html>
- Monash University IT Security Policy
<http://www.its.monash.edu.au/policies/>
- Monash University – Network Access Control Policy
<http://www.adm.monash.edu.au/execserv/policies/Information-Technology-Policies/Network-Access-Control-Policy.html>
- Monash Domain Names Policy
<http://www.adm.monash.edu.au/execserv/policies/Information-Technology-Policies/restricted/Domain-Names.html>
- Monash University Practice & Paid Outside Work Policy
<http://www.adm.monash.edu.au/workplace-policy/conduct/paid-outside-work/>
- Monash University Software Catalogue
<http://www.its.monash.edu.au/staff/software/catalogue/>
- Monash University Workplace Policies and Procedures
<http://www.adm.monash.edu.au/workplace-policy/>
- Monash Web Policy (Web Page Definitions)
<http://www.its.monash.edu.au/policies/web-page-definitions.html>
- Monash Personal Page Disclaimer
<http://www.monash.edu.au/legals/personal.html>
- Racial Discrimination Act (Cwlth) 1975
<http://scaleplus.law.gov.au/html/pasteact/0/47/top.htm>
- Sex Discrimination Act (Cwlth) 1984
<http://scaleplus.law.gov.au/html/pasteact/0/171/top.htm>
- Telecommunications Act
- Trade Marks Act (1955) (Commonwealth)
- Trade Practices Act (1974) (Commonwealth)
- Information Privacy Act 2000 (Victoria)

Further Information and Policy Review Details

Further Information and Assistance

Adherence to this policy will generally ensure compliance with the requirements of Monash University and legislation. However, there may be instances where inadvertent breaches could occur. When in doubt users requiring assistance with interpretation of the policy, or who wish to report a breach of this policy, should contact:

- The ITS Service Desk on ext. 51777 or <http://www.its.monash.edu.au/contact/>
- Policy and Consultancy Group, Human Resources Division, on ext. 56936 or <http://www.adm.monash.edu.au/sss/>
- The University Solicitor's Office on ext. 55126.

Links to related University Policies and processes have been identified under Associated Policies and Legislation.

Amendment Number	Authorization	Date	Reference
8	Director, Client Services	October 2006	Updated web addresses
7	Manager, Policy and Consultancy, HR Division	August 2006	Amendments re: For Monash University Staff
6	Manager, Policy and Consultancy, HR Division	January 2006	Updating titles, web addresses and contact details
5	Director, Client Services, ITS	September 2005	New content on the use of library databases
4	Director Client Services, ITS	June 2005	Amendments re: Copyright information
3	Director, Client Services ITS	March 2005	Amendments re: Software licence restrictions
2	UNITPOL	November 2004	Amendments re peer to peer software, personal equipment, personal use, email forwarding and SPAM Act
1	Deputy University Solicitor	June 2003	Updated with additional copyright material

Key Words/Phrases

Information Technology, Acceptable Use, e-mail, internet, network services, guidelines, copyright, privacy, discrimination, ethical, personal use, security, disclosure, confidential information.