MONASH UNIVERSITY PRIVACY COMPLIANCE MANUAL

Last updated: September 2009

TABLE OF CONTENTS

Introduction 4

Checklist For Compliance With The Privacy Laws – All Staff 5

Checklist For Compliance With The Privacy Laws – Managers 6

The Information Privacy Act 7

The Health Records Act 8

The Information Privacy Principles 9

- **IPP 1 - Collection** 9
- **IPP 2 – Use And Disclosure** 10
- **IPP 3 – Data Quality** 13
- **IPP 4 – Data Security** 13
- **IPP 5 - Openness** 14
- **IPP 7 – Unique Identifiers** 15
- **IPP 8 – Anonymity** 16
- **IPP 9 – Transborder Data Flows** 17
- **IPP 10 – Sensitive Information** 18

The Health Privacy Principles 19

- **HPP 1 - Collection** 19
- **HPP 2 – Use And Disclosure** 23
- **HPP 3 – Data Quality** 25
- **HPP 4 – Data Security And Data Retention** 26
- **HPP 5 - Openness** 27
- **HPP 6 – Access And Correction** 27
- **HPP 7 – Unique Identifiers** 28
- **HPP 8 – Anonymity** 28
- **HPP 9 – Transborder Data Flows** 29
- **HPP 10 – Transfer Or Closure Of The Practice Of A Health Service Provider** 30
- **HPP 11 – Making Information Available To Another Health Service Provider** 30

Collection Of Personal Information 31

Links **34**
Documents For Staff **34**
Exemptions In The Privacy Laws **35**
What Happens If Someone Complains To Monash University Or If Monash University Breaches The Privacy Laws? **36**
Disclosure Of Personal Information To 3rd Parties **37**
Monash University Privacy Policy **38**
Monash University Collection, Storage And Destruction Of Credit Card Details Policy **45**
Guidelines For Collecting / Distributing Student Results / Assignments And Other Information **49**
Frequently Asked Questions - Relating To Staff **53**
Frequently Asked Questions - Relating To Students **58**
Collection And Storage Of Tax File Numbers **63**
Case Studies **65**
Monash Controlled Entities **68**
The Privacy Act **68**
Contacts **71**

INTRODUCTION

Monash values the privacy of every individual's personal information and is committed to the protection of personal information.

Monash has established a privacy regime that strives to:

- Promote an understanding and acceptance of the privacy principles and their objectives throughout the university community;
- Educate people within the university about information privacy;
- Handle any complaints received in an efficient and appropriate manner; and
- Monitor privacy compliance and keep the university informed of updates to procedures.

Checklist For Compliance With The Privacy Laws – All Staff

- ☑ Have you been trained in privacy laws or attended a privacy briefing session?
- ☑ Have you considered the privacy implications for all new projects?
- ☑ Do you only collect personal information that is necessary for Monash's functions and activities?
- ☑ When collecting personal information, do you make sure that individuals providing the information know the purposes for collection, any law that requires collection, the types of organisations to which Monash discloses the information, the individual has the right to access their information, any consequences of not providing the information and the Privacy Officer's contact details?
- ☑ Do you only use and disclose personal information for the primary purpose of collection or a secondary purpose the individual would reasonably expect? If it does not fall within the primary or secondary purpose do you obtain the consent of the individual?
- ☑ When disclosing personal information to third parties, do you request the third party to sign a privacy agreement which requires them to treat the information in accordance with the privacy laws?
- ☑ Do you make sure personal information is accurate, complete and up to date?
- ☑ Do you take reasonable steps to protect personal information from misuse, loss, unauthorised access, modification or disclosure?
- ☑ Do you provide individuals with the opportunity to access their personal information in accordance with the Freedom of Information laws?
- ☑ Do you know where to locate the Monash University Privacy Policy? Do you make it available to anyone who asks for it?
- ☑ Do you, wherever it is lawful and practicable, provide individuals with the option of remaining anonymous when dealing with Monash.
- ☑ When transferring information outside of Victoria, do you make sure that the recipient has equivalent privacy laws, the individual consents or you request the recipient to sign a privacy agreement?
- ☑ Do you only collect sensitive or health information with the consent of the individual, or if it is required or authorised by law?

CHECKLIST FOR COMPLIANCE WITH THE PRIVACY LAWS – MANAGERS

- ☑ Have you considered the obligations imposed on all staff of the university by the privacy laws? (See check list on page 5 for more details)
- ☑ Are you aware of obligations placed on Monash by the privacy laws?
- ☑ Have all staff who handle personal, sensitive or health information as a part of their normal day to day duties been trained in privacy laws and has training on privacy laws been included in all new staff member's induction?
- ☑ Have you conducted an audit of your area's current practices to ensure that Monash is complying with the privacy laws? Do you conduct regular follow up audits to monitor ongoing compliance with the laws?
- ☑ Have you considered the privacy implications for all new projects?
- ☑ Is a privacy compliance culture promoted within your area? Are staff encouraged to consider privacy consequences in activities they undertake on behalf of the university?
- ☑ Do you know who your Privacy Co-ordinator is, or if your area does not have one, do you know how to contact the Privacy Officer?

THE INFORMATION PRIVACY ACT

Monash University is required to comply with the Information Privacy Act (Vic) 2000.

Objectives of the Information Privacy Act

The objectives of the Information Privacy Act are to:

- Balance the public interest in the free flow of information with the public interest in respecting privacy and protecting personal information in the public sector; and
- Promote the responsible and transparent handling of personal information in the public sector and promote awareness of these practices.

Compliance with the Information Privacy Act

The Act took effect from the 1st September 2001, with individuals being able to lodge complaints with the Office of the Victorian Privacy Commissioner from 1st September 2002.

With limited exemptions, all Victorian government agencies, statutory bodies and local councils must comply with the IPP's. Monash University is required to comply because the Act applies to 'a body established or appointed for a public purpose by or under an Act'. Monash University is established by the *Monash University Act 1958*.

The Act contains ten Information Privacy Principles (IPP's) which are the central part of the laws.

Relevant Definitions

The Information Privacy Act applies to two types of information:

Personal Information: basically means recorded information or opinion, whether true or not, about an identifiable individual. It also includes information from which the identity of the individual can be reasonably ascertained. Examples: name, address, telephone number, title.

Sensitive Information: racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal record *that is also personal information.*

THE HEALTH RECORDS ACT

Monash University is required to comply with the Health Records Act (Vic) 2001.

Objectives of the Health Records Act

The objectives of the Health Records Act are to:

- require responsible handling of health information in the public and private sectors;
- balance the public interest in protecting the privacy of health information with the public interest in the legitimate use of that information;
- enhance the ability of individuals to be informed about their health care or disability services;
- promote the provision of quality health services, disability services and aged care services.

Compliance with the Health Records Act

The Act took effect from the 1st March 2002, with individuals being able to lodge complaints with the Office of the Health Services Commissioner from 1st July 2002.

The Health Records Act applies to health, disability and aged care information handled by a wide range of public and private sector organisations. Examples of the types of information which Monash University collects, uses and discloses which would be covered by this legislation is sick leave information, maternity leave information, special consideration applications, deferment applications, Academic Progress Committee documents and any information held by Community Services. Some Faculties (eg Medicine, Nursing and Health Sciences and Science) may also hold information which is covered by this legislation.

The Act contains eleven Health Privacy Principles (HPP's) which are the central part of the laws.

Relevant Definitions

The Health Records Act applies to health information:

Health Information: information or opinion about the physical, mental or psychological health at any time of an individual, a disability of an individual, an individual's expressed wishes about future provision of health services to him or her or a health service provided or to be provided to an individual *that is also personal information.* It also includes other personal information collected to provide a health service (eg name, address) and information about donation of body parts, organs or body substances and genetic information.

THE INFORMATION PRIVACY PRINCIPLES

The Information Privacy Act has created new privacy rights that enable individual's to exercise greater control over how an organisation collects, uses and discloses personal information that relates to them. The Information Privacy Act has implemented ten Information Privacy Principles (IPP's) to describe how personal information and sensitive information is to be handled.

The purpose of this section is to provide a summary of the ten Information Privacy Principles.

IPP 1 - COLLECTION

- Monash must only collect personal information if it is **necessary** for our functions and activities.

It is not acceptable for Monash to collect information simply because we would like to have it, or because it might be needed at some time in the future. Information is necessary only if there is legitimate justification for its collection.

- Monash must only collect information by lawful and fair means and not in an unreasonably intrusive way.

To decide whether something is fair, lawful and not intrusive, consider whether relevant laws are complied with eg surveillance must be conducted in accordance with the Surveillance Devices Act (Vic), is the individual made aware of the collection eg the use of cookie technology to track an individual's use of the website without making it clear to them via a prominent privacy notice or do we have an unfair advantage when collecting information eg unequal relationship such as children/adult, non-English speaking people or traumatised individual.

- At or before the time of collection, Monash must take reasonable steps to inform individuals of the following matters:
  - the identity of Monash and how to contact it;
  - the fact that he or she is able to gain access to the information;
  - the purposes for which the information is collected;
  - to whom, or the types of organisations to whom, Monash discloses information of this kind;
  - any law that requires the particular information to be collected; and

- the main consequences (if any) for the individual if all or part of the information is not provided.

Monash University has created the following standard wording which complies with the above requirements. The wording can be amended depending on the circumstances for collection. It is recommended that this wording is included on all forms (paper and electronic) which collect personal information. If you would like to make changes to this wording it is recommended that you obtain confirmation from the Monash University Privacy Officer that the amended wording meets the requirements of the privacy laws.

The information on this form is collected for the primary purpose of **[insert primary purpose].** Other purposes of collection include **[insert secondary purposes].** If you choose not to complete all the questions on this form, it may not be possible for [**insert name eg. the Faculty]** to **[insert consequence]**. Personal information may also be disclosed to **[list any 3rd parties personal information is disclosed to (do not include Monash staff)]** You have a right to access personal information that Monash University holds about you, subject to any exceptions in relevant legislation. If you wish to seek access to your personal information or inquire about the handling of your personal information, please contact the University Privacy Officer at privacyofficer@adm.monash.edu.au.

- If it is reasonable and practicable Monash must only collect personal information about an individual only from the individual. However, if Monash collects personal information about an individual from a third party (eg, Monash International, VTAC), we must take reasonable steps to inform the individual of the matters outlined in the box above, unless this would pose a serious threat to the life or health of any individual.

If you regularly collect information about individuals from a third party you may like to consider contractually binding the third party to provide the relevant notification in accordance with the privacy laws and indemnification if they fail to provide the notification. For advice on the necessary contractual clauses please contact the Monash University Privacy Officer or the Solicitor's Office.

IPP 2 – USE AND DISCLOSURE

- Monash may only use or disclose personal information about an individual for the primary purpose for which it was collected or a related purpose (directly related for sensitive information) the individual would reasonably expect.

To determine how personal information can subsequently be used and to who it can be disclosed, requires an understanding of the primary purpose that the information was collected. If the requirements of IPP

1 have been met, the primary purpose should be clear and should have been communicated to the person at the time of collection.

If it doubt about whether a use or disclosure falls within the secondary purpose obtain consent from the individual or seek advice from the Monash University Privacy Officer.

- Personal information can also be used or disclosed for a secondary purpose if:

  - the individual has consented to the use or disclosure.

It is preferable to obtain written consent. In some circumstances, written consent is not practicable. Verbal or implied consent can be relied upon however if a dispute were to arise it would be more difficult to prove that we had obtained consent.

It is important to consider the elements of consent when obtaining consent:

- *individual must have **capacity** to consent*
- *consent must be **voluntary***
- *consent must be **informed***
- *consent must be **specific***
- *consent must be **current***

  - the use or disclosure is necessary for research in the public interest when it will be published in a non-identifiable format and it is not practicable to seek the individual's consent and in the case of disclosure, Monash reasonably believes the recipient will not disclose the information.

All research conducted by Monash University involving humans must receive ethics approval from the Standing Committee on Ethics in Research Involving Humans (SCERH). SCERH may approve projects which fall within the category of acceptable use and disclosure in accordance with the privacy laws. If you require further information related to ethics approval, please contact the Human Ethics Officer via email SCERH@adm.monash.edu.au or phone 9905 2052.

  - Monash believes the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health or safety and welfare or a serious threat to public health, public safety or public welfare.

By their nature, such circumstances would be unusual and uncommon. In general, the recipient of the information would need to be

appropriate police, emergency services or health authorities. The Victorian Privacy Commissioner has indicated that the decision to rely on this exemption for using or disclosing information should only be made by senior staff.

- Monash has reason to suspect that unlawful activity has been or is being engaged in and uses or discloses the personal information to investigate the matter or to report concerns to relevant persons or authorities.

Suspicion should be based on reasonable grounds and not on gossip or rumour. The activity should be unlawful, not just unethical or objectionable. The information should be confined in the early stages of investigation to only those individuals who must have access. The relevant persons or authorities should be those who need to have access to the information because they have relevant duties to perform.

- The use or disclosure is required or authorised by or under law.

Examples of use or disclosure required or authorised by or under law at Monash is the reporting of certain student information to the Department of Education, Science and Training, or information about international students to the Department of Immigration, Multicultural and Indigenous Affairs. For advice about whether something is required or authorised by or under law please contact the Monash University Privacy Officer or the Solicitor's Office.

- A law enforcement agency has requested personal information and authorisation has been obtained from the Monash University Privacy Officer to assist the law enforcement agency.

The law relating to use and disclosure of personal information to a law enforcement agency (eg Victoria Police, Australian Federal Police) is complex and advice must be obtained from the Monash University Privacy Officer prior to releasing information.

TIP: If you are in doubt about whether you can use or disclose personal information in accordance with Information Privacy Principle 2 obtain the consent of the individual for the use or disclosure of information or alternatively, contact the Monash University Privacy Officer for advice.

IPP 3 – DATA QUALITY

- Monash must take reasonable steps to make sure that personal information it collects, uses or discloses is accurate, complete and up to date.

The accuracy, completeness and currency of the information should be established at the time of collection, and reviewed when the information is used or re-used, and when it is disclosed to another organisation. Organisations do not have to monitor data quality when information is dormant. Personal information collected and used for a particular purpose and then archived does not need to be constantly checked for accuracy.

Staff and students should be encouraged to keep their personal information accurate by directly updating their information online or by completing the relevant form and forwarding it to Monash.

IPP 4 – DATA SECURITY

- Monash must take reasonable steps to protect personal information from:
  - misuse;
  - loss;
  - unauthorised access;
  - unauthorised modification; and
  - unauthorised disclosure.

In the case of a large organisation such as Monash, just because an individual provides personal information to one part of Monash, does not mean that they expect all parts of Monash to use this information. This is particularly relevant in the case of sensitive information. Personal information must be protected from misuse, loss, unauthorised access, modification or disclosure both within Monash as well as from misuse, loss etc to external parties.

There are a number of things that individual staff members can do to enhance compliance with this privacy principle which include:

- *locking offices when unattended*
- *not leaving personal information lying around*
- *for open plan offices, staggering lunch breaks to ensure someone is always present in the office*
- *storing sensitive or confidential personal information in locked filing cabinets*
- *changing passwords on computers regularly*
- *activating a screen saver on computers*

- Monash must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed.

Staff should comply with the Public Records Act when considering when information is no longer needed. When determining how long personal information should be stored for please refer to the 'Records Disposal Authority' which is managed by Monash University Archives. The Authority is available from http://www.adm.monash.edu.au/magpie/restrict/archives/RDAfront.html

Personal information must be destroyed securely when it is no longer needed. Examples of secure destruction include shredding, pulping or disintegration of paper files, fire, confidential disposal in accordance with any guidelines provided by Records & Archives, or contracting an authorised disposal company for secure disposal.

IPP 5 - OPENNESS

- Monash must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.

Monash University has developed the Monash University Privacy Policy. This is available from page 38 or on the web at http://www.privacy.monash.edu.au/pc_privacy_pol.htm. It can also be obtained by contacting the Monash University Privacy Officer.

- On request by a person, Monash must take reasonable steps to let the person know generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information. If a request of this type by a student, please refer them to the Privacy Co-ordinator from the relevant faculty. If the request is made by a staff member, please refer them to the Privacy Officer.

IPP 6 – ACCESS AND CORRECTION

- Individuals have the right to seek access to their personal information and make corrections. Monash will, on request, provide students and staff with access to information it holds about them and allow them to make corrections unless an exemption applies at law.

Staff may access their personnel files in accordance with the *Monash University Freedom of Information Policy available from: http://www.adm.monash.edu.au/unisec/foi/foimupol.html*.

Students may access their files in accordance with the Monash University Freedom of Information Policy available from: http://www.adm.monash.edu.au/unisec/foi/foimupol.html.

In some instances if a student would like to access their student records they need to contact the Manager, Client Services, and HR Division. Please refer to section 5.2 of the Monash University Privacy Policy.

- Freedom of Information laws continue to apply. If access cannot be granted, please contact the Monash University Privacy Officer or the Monash University Freedom of Information Officer (contact details below).

- For more information about Freedom of Information at Monash University please go to http://www.adm.monash.edu.au/unisec/foi/ or contact the Freedom of Information Officer by telephone (03) 9905 5137 or email foi@adm.monash.edu.au.

IPP 7 – UNIQUE IDENTIFIERS

- **Unique identifiers** are numbers or codes which are assigned to an individual to assist with identification. Examples of common unique identifiers used by Monash University are the student ID number and the staff ID number.

- Monash must only assign unique identifiers if it is necessary for Monash to carry out any of its functions efficiently.

When thinking about creating a new type of unique identifier (other than the student/staff number), consider whether it is necessary, eg would it be sufficient to identify the individual by their name. In some sensitive or delicate situations unique identifiers may enhance privacy. In testing whether efficiency is established, an assessment of efficiency from the perspective of both Monash and those with whom it deals is required.

- Monash must not adopt as its own unique identifier of an individual, the unique identifier of the individual which has been created by another organisation unless it is necessary to enable Monash to carry out any of its functions efficiently, or it has consent from the individual for the use of the unique identifier. Examples of unique identifiers which have been created by other organisations are VTAC number, drivers licence number, tax file number or Medicare number.

- Monash can only use or disclose a unique identifier assigned to an individual by another organisation in the following circumstances:

- the use or disclosure is necessary for Monash to fulfil its obligations to the other organisation
- Monash has the consent of the individual to the use or disclosure
- Monash believes the use or disclosure is necessary to lessen or prevent a serious or imminent threat to an individual's life, health or safety or a serious threat to public health, public safety or public welfare.
- Monash has reason to suspect that unlawful activity has been or is being engaged in and uses or discloses the personal information to investigate the matter or to report concerns to relevant persons or authorities.
- The use or disclosure is required or authorised by or under law.
- A law enforcement agency has requested personal information and authorisation has been obtained from the Monash University Privacy Officer to assist the law enforcement agency.

In most cases reviewed at Monash University to date, the use or disclosure of unique identifiers which have been created by another organisation (eg VTAC number, tax file number) are in accordance with the above requirements. (Eg authorised by law or with the individuals consent). If you are unsure about whether the use of a unique identifier created by another organisation is in accordance with the laws please contact the Monash University Privacy Officer.

- Monash must not require an individual to provide a unique identifier in order to obtain a service unless the provision of the unique identifier is required or authorised by law or the provision is in connection with the purpose (or a directly related purpose) for which the unique identifier was assigned.

In most cases, the requirement to provide a unique identifier to Monash is required by law (eg tax file number for HECS or employment) or is in connection with the purpose for which the unique identifier was assigned. If you are unsure as to whether the provision of a unique identifier by an individual is in accordance with the laws please contact the Monash University Privacy Officer.

IPP 8 – ANONYMITY

- Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering into a transaction with Monash.

As a general rule, it is not lawful and practicable for individuals to remain anonymous when dealing with Monash. For example it is not possible to award a degree to someone without knowing who they are. Examples of situations where individuals remain anonymous are the sale of products or services by cash such as books or theatre tickets, or the making of general enquiries such as 'What time are you open?'

IPP 9 – TRANSBORDER DATA FLOWS

- Monash may only transfer information about an individual to someone (other than the individual or Monash) who is outside of Victoria if one or more of the following applies:

- Monash reasonably believes the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of information that are substantially similar to the Information Privacy Principles.

Commonwealth government organisations, companies with annual turnover of more than $3million, some state government agencies (eg NSW) or a selection of other types of organisations in Australia have equivalent privacy laws. Therefore transfers to these types of organisations located outside of Victoria comply with this Transborder Data Flow principle.
Some countries have equivalent privacy laws in place (eg United Kingdom) and transfer can occur under this provision. However, many countries do not have equivalent privacy laws (eg no laws in Malaysia or South Africa) and a transfer must fall within one of the following categories in order to comply with this principle.

-the individual consents to the transfer

When obtaining consent from the individual to transfer information to an organisation who is located outside Victoria, the individual must be made aware of whether the privacy protection will travel with the information for legitimate consent to be obtained.

-the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request
-the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party

-all of the following apply:
- the transfer is for the benefit of the individual
- it is impracticable to obtain the consent of the individual to that transfer
- if it were practicable to obtain that consent, the individual would be likely to give it.

-the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Information Privacy Principles.

If a transfer of personal information outside of Victoria does not fall within any of the above categories, then this category can be complied with if the recipient of the information is requested to sign a contract which binds them to comply with the Information Privacy Principles. The standard privacy contract can be obtained from the Monash University Privacy Officer.

PLEASE NOTE: *Monash University South Africa and Monash University Malaysia are not considered to be transfers to Monash and therefore transfers to these overseas campuses must be treated in accordance with this principle. The Monash University centres located in Prato, Italy and London, United Kingdom are considered to be transfers to Monash and therefore do not have to be treated in accordance with this principle.*

IPP 10 – SENSITIVE INFORMATION

- Monash must not collect sensitive information about an individual unless: (for the definition of sensitive information please go to page 7)

  -the individual has consented (eg implied consent by including details on form)

  -the collection is required under law (eg collection of racial/ethnic origin for DEST reporting)

  -the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns-
    - is physically or legally incapable of giving consent to the collection or
    - physically cannot communicate consent to the collection

  -the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

If you would like to collect sensitive information to provide additional services, for statistical analyses or for any other purpose which is not required under law, it is recommended that the question is made optional. If the person chooses to complete an optional question we have implied consent to use the sensitive information for the purposes outlined in the privacy notice required by IPP 1.

THE HEALTH PRIVACY PRINCIPLES

The Health Records Act has created new privacy rights that enable individual's to exercise greater control over how an organisation collects, uses and discloses health information that relates to them. The new Act has implemented eleven Health Privacy Principles (HPP's) to describe how health information is to be handled.

The purpose of this section is to provide a summary of the eleven Health Privacy Principles.

When referring to this section, please be aware that the HPP's are very similar to the IPP's. The requirements contained in the IPP's in relation to 'sensitive information', are comparable.

HPP 1 - COLLECTION

- Monash must only collect health information if it is **necessary** for our functions and activities and at least one of the following applies

It is not acceptable for Monash to collect information simply because we would like to have it, or because it might be needed at some time in the future. Information is necessary only if there is legitimate justification for its collection.

- the individual has consented

It is preferable to obtain written consent. In some circumstances, written consent is not practicable. Verbal or implied consent can be relied upon however if a dispute were to arise it would be more difficult to prove that we had obtained consent.

It is important to consider the elements of consent when obtaining consent:

- *individual must have **capacity** to consent*
- *consent must be **voluntary***
- *consent must be **informed***
- *consent must be **specific***
- *consent must be **current***

- the collection is required, authorised or permitted by law

- the information is necessary to provide a health service and the individual is incapable of giving consent due to age, disability, mental

disorder etc and there is no authorised representative available to provide consent

- the collection is for a secondary purpose directly related to the primary purpose and the individual would reasonably expect the organisation to collect the information for the secondary purpose

If it doubt about whether the collection falls within the secondary purpose obtain consent from the individual or seek advice from the Monash University Privacy Officer.

- the organisation has reason to suspect that unlawful activity has been, or is being engaged in and collects the information as a necessary part of its investigation of the matter or in reporting its concerns to the relevant persons or authorities (and if it relates to a health service provider eg Community Services, it is not a breach of confidence)

"Breach of confidence" relates to the general law of confidence (including but not limited to the common law or in equity), which requires, amongst other things, that a duty of confidence exists under that law which is not, in the particular circumstances, outweighed by any countervailing public interest under that law.

Suspicion should be based on reasonable grounds and not on gossip or rumour. The activity should be unlawful, not just unethical or objectionable. The information should be confined in the early stages of investigation to only those individuals who must have access. The relevant persons or authorities should be those who need to have access to the information because they have relevant duties to perform.

- the information is collected about a deceased or missing person or a person involved in an accident who is unable to consent and the health information is collected for the purposes of identifying the individual and contacting family members unless this is against expressed wishes of the individual before they died, went missing or became incapable of providing consent

- the collection is necessary for research in the public interest and it is not practicable to seek the individual's consent and is conducted in accordance with guidelines produced by the Health Services Commissioner

All research conducted by Monash University involving humans must receive ethics approval from the Standing Committee on Ethics in Research Involving Humans (SCERH). SCERH may approve projects

which fall within the category of acceptable use and disclosure in accordance with the privacy laws. If you require further information related to ethics approval, please contact the Human Ethics Officer via email SCERH@adm.monash.edu.au or phone 9905 2052.

- Monash believes the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health or safety and welfare or a serious threat to public health, public safety or public welfare and the information is collected in accordance with any guidelines produced by the Health Services Commissioner

By their nature, such circumstances may be unusual. But in general, the recipient would need to be appropriate police, emergency services or health authorities. The decision to rely on this exemption for using or disclosing information should only be made by senior staff.

- the collection is by or on behalf of a law enforcement agency and the organisation reasonably believes that the collection is necessary for the law enforcement function and advice has been obtained from the Monash University Privacy Officer to confirm collection is in accordance with the laws.

The law relating to collection health information on behalf of a law enforcement agency (eg Victoria Police, Australian Federal Police) is complex and advice must be obtained from the Monash University Privacy Officer prior to collecting information.

- the collection is necessary for the establishment, exercise or defence of a legal or equitable claim

- other limited circumstances which are very specific to health service providers and would not as a matter of course occur at Monash.

- Monash must only collect health information by lawful and fair means and not in an unreasonably intrusive way.

To decide whether something is fair, lawful and not intrusive, consider whether relevant laws are complied with eg surveillance must be conducted in accordance with the Surveillance Devices Act (Vic), is the individual made aware of the collection eg the use of cookie technology to track an individual's use of the website without making it clear to them via a prominent privacy notice or do we have an unfair advantage when collecting information unequal relationship such as children, non-English speaking people or traumatised individual.

- At or before the time of collection, Monash must take reasonable steps to inform individuals of the following matters:
    - the identity of Monash and how to contact it;
    - the fact that he or she is able to gain access to the information;
    - the purposes for which the information is collected;
    - to whom, or the types of organisations to whom, Monash discloses information of this kind;
    - any law that requires the particular information to be collected; and
    - the main consequences (if any) for the individual if all or part of the information is not provided.

Monash University has created the following standard wording which complies with the above requirements. The wording can be amended depending on the circumstances for collection. It is recommended that this wording is included on all forms (paper and electronic) which collect health information. If you would like to make changes to this wording it is recommended that you obtain confirmation from the Monash University Privacy Officer that the amended wording meets the requirements of the privacy laws.

The information on this form is collected for the primary purpose of **[insert primary purpose].** Other purposes of collection include **[insert secondary purposes].** If you choose not to complete all the questions on this form, it may not be possible for [**insert name eg. the Faculty]** to **[insert consequence]**. Personal information may also be disclosed to **[list any 3rd parties personal information is disclosed to (do not include Monash staff)]** You have a right to access personal information that Monash University holds about you, subject to any exceptions in relevant legislation. If you wish to seek access to your personal information or inquire about the handling of your personal information, please contact the University Privacy Officer at privacyofficer@adm.monash.edu.au.

- If it is reasonable and practicable Monash must only collect health information about an individual only from the individual. However, if Monash collects health information about an individual from a third party, we must take reasonable steps to inform the individual of the matters outlined above, unless this would pose a serious threat to the life or health of any individual.

If you regularly collect information about individuals from a third party you may like to consider contractually binding the third party to provide the relevant notification in accordance with the privacy laws and indemnification if they fail to provide the notification. For advice on the necessary contractual clauses please contact the Monash University Privacy Officer or the Solicitor's Office.

- **'Information given in confidence'** is a special category of information which applies to health service providers such as Community Services and some areas within the Faculty of Medicine, Nursing and Health Sciences.

'Information given in confidence' under the privacy laws is information about an individual which has been provided to the health service provider by someone other than the individual or another health service provider with a request that the information is not communicated to the individual to whom it relates. If someone provides 'information in confidence', the health service provider must confirm that the information is to remain confidential, take reasonable steps to ensure it accuracy and take reasonable steps to record that the information is given in confidence and is to remain confidential.

HPP 2 – USE AND DISCLOSURE

- Monash may only use or disclose health information about an individual for the primary purpose for which it was collected or a directly related purpose the individual would reasonably expect.

To determine how health information can subsequently be used and to who it can be disclosed, requires an understanding of the primary purpose that the information was collected. If the requirements of IPP 1 have been met, the primary purpose should be clear and should have been communicated to the person at the time of collection.

- Health information can also be used or disclosed for a secondary purpose if:

  - the individual has consented to the use or disclosure.

It is preferable to obtain written consent. In some circumstances, written consent is not practicable. Verbal or implied consent can be relied upon however if a dispute were to arise it would be more difficult to prove that we had obtained consent.

It is important to consider the elements of consent when obtaining consent:

- *individual must have **capacity** to consent*
- *consent must be **voluntary***
- *consent must be **informed***
- *consent must be **specific***
- *consent must be **current***

  - The use or disclosure is required or authorised by or under law.

Examples of use or disclosure required or authorised by or under law at Monash is the reporting of communicable diseases to the Department of Human Services. For advice about whether something

is required or authorised by or under law please contact the Monash University Privacy Office.

- the use or disclosure by a health service provider is necessary to provide a health service and the individual is incapable of giving consent due to age, disability, mental disorder etc and there is no authorised representative available to provide consent

- the use or disclosure is necessary for research in the public interest when it will be published in a non-identifiable format and it is not practicable to seek the individual's consent and in the case of disclosure, Monash reasonably believes the recipient will not disclose the information.

All research conducted by Monash University involving humans must receive ethics approval from the Standing Committee on Ethics in Research Involving Humans (SCERH). SCERH may approve projects which fall within the category of acceptable use and disclosure in accordance with the privacy laws.

- Monash believes the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health or safety and welfare or a serious threat to public health, public safety or public welfare and is in accordance with guidelines issued by the Health Services Commissioner.

By their nature, such circumstances would be unusual and uncommon. In general, the recipient of the information would need to be appropriate police, emergency services or health authorities. The decision to rely on this exemption for using or disclosing information should only be made by senior staff.

- Monash has reason to suspect that unlawful activity has been or is being engaged in and uses or discloses the health information to investigate the matter or to report concerns to relevant persons or authorities (and if it relates to a health service provider eg Community Services, it is not a breach of confidence)

"Breach of confidence" relates to the general law of confidence (including but not limited to the common law or in equity), which requires, amongst other things, that a duty of confidence exists under that law which is not, in the particular circumstances, outweighed by any countervailing public interest under that law.

Suspicion should be based on reasonable grounds and not on gossip or rumour. The activity should be unlawful, not just unethical or objectionable. The information should be confined in the early stages of investigation to only those individuals who must have access. The relevant persons or authorities should be those who need to have access to the information because they have relevant duties to perform.

- A law enforcement agency has requested health information and authorisation has been obtained from the Monash University Privacy Officer to assist the law enforcement agency.

The law relating to use and disclosure of health information to a law enforcement agency (eg Victoria Police, Australian Federal Police) is complex and advice must be obtained from the Monash University Privacy Officer prior to releasing information.

- Health information can be used or disclosed in other limited circumstances which are very specific to health service providers and would not as a matter of course occur at Monash.

TIP: If you are in doubt about whether you can use or disclose health information in accordance with Health Privacy Principle 2 obtain the consent of the individual for the use or disclosure of information or alternatively, contact the Monash University Privacy Officer for advice.

HPP 3 – DATA QUALITY

- Monash must take reasonable steps to make sure that health information it collects, uses or discloses is accurate, complete and up to date and relevant to its functions or activities.

The accuracy, completeness and currency of the information should be established at the time of collection, and reviewed when the information is used or re-used, and when it is disclosed to another organisation. Organisations do not have to monitor data quality when information is dormant. Health information collected and used for a particular purpose and then archived does not need to be constantly checked for accuracy.

It is important to identify the main risks associated with the use or disclosure of inaccurate, incomplete or out-of-date information. The degree to which any such measures might be considered a requirement of reasonable steps which an organisation should take will depend on the risks involved to the individual. Eg: a health service provider that provided a person with medication or advised a medical procedure without ensuring that the information which was held about the

individual was up to date would be likely to have breached the principle because of the risks for the individual in the use of the out-of-date information.

HPP 4 – DATA SECURITY AND DATA RETENTION

- Monash must take reasonable steps to protect health information from:
  - misuse;
  - loss;
  - unauthorised access;
  - unauthorised modification; and
  - unauthorised disclosure.

In the case of a large organisation such as Monash, just because an individual provides health information to one part of Monash, does not mean that they expect all parts of Monash to use this information. Health information must be protected from misuse, loss, unauthorised access, modification or disclosure both within Monash as well as from misuse, loss etc to external parties.

There are a number of things that individual staff members can do to enhance compliance with this privacy principle which include:

- *locking offices when unattended*
- *not leaving health information lying around*
- *for open plan offices, staggering lunch breaks to ensure someone is always present in the office*
- *storing sensitive or confidential health information in locked filing cabinets*
- *changing passwords on computers regularly*
- *activating a screen saver on computers*

- Monash must take reasonable steps to destroy or permanently de-identify health information if it is no longer needed. (The health service providers which are a part of Monash University (eg Community Services) have additional obligations detailed below.)

Staff should comply with the Public Records Act when considering when information is no longer needed. When determining how long health information should be stored for please refer to the 'Records Disposal Authority' which is managed by Monash University Archives. The Authority is available from http://www.adm.monash.edu.au/magpie/restrict/archives/RDAfront.html

- A health service provider can only delete information about an individual if

- the deletion is permitted by law
- if the health information was collected while the individual was a child, after the child reaches 25 years or
- in any other case, more than 7 years after the last occasion on which the health service was provided

- If a health service provider deletes health information it must make a written note which details the name of the individual, the period it related to and the date it was deleted. A written note containing these details must also be made if a health service provider transfer health information to another organisation and does not continue to hold a record for that individual.

Health information must be destroyed securely when it is no longer needed. Examples of secure destruction include shredding, pulping or disintegration of paper files, fire, confidential disposal in accordance with any guidelines provided by Records & Archives, or contracting an authorised disposal company for secure disposal.

HPP 5 - OPENNESS

- Monash must set out in a document clearly expressed policies on its management of health information. The organisation must make the document available to anyone who asks for it.

Monash University has developed the Monash University Privacy Policy. This is available from page 38 or on the web at http://www.privacy.monash.edu.au/pc_privacy_pol.htm. It can also be obtained by contacting the Monash University Privacy Officer. Other areas within the university have separate privacy policies which deal more specifically with the collection of heath information eg Community Services Privacy Policy

- On request by a person, Monash must take reasonable steps to let the person know generally, what sort of health information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

HPP 6 – ACCESS AND CORRECTION

- Individuals have the right to seek access to their personal information and make corrections. Monash will, on request, provide students and staff with access to information it holds about them and allow them to make corrections unless an exemption applies at law.

Staff may access their personnel files in accordance with section 9.8 of the Staff Handbook available from:

http://www.adm.monash.edu.au/sss/handbook/sh_9-8.htm. The Staff Handbook requires staff to make a request to the Divisional Director, HR Division to access their personnel file.

Students may access their files in accordance with the Monash University Freedom of Information Policy available from: http://www.adm.monash.edu.au/unisec/foi/foimupol.html. This policy states that if a student would like to access their student records they need to contact the Manager, Client Services, **Student and Community Services Division**.

Individuals who want access to their medical records held by Monash University (eg Community Services) should be referred to their health care professional (eg doctor, counsellor).

- Freedom of Information laws continue to apply. If access cannot be granted under either of the above policies, please contact the Monash University Privacy Officer or the Monash University Freedom of Information Officer (contact details below).

- For more information about Freedom of Information at Monash University please go to http://www.adm.monash.edu.au/unisec/foi/ or contact the Freedom of Information Officer by telephone (03) 9905 5137 or email foi@adm.monash.edu.au.

HPP 7 – UNIQUE IDENTIFIERS

- **Unique identifiers** are numbers or codes which are assigned to an individual to assist with identification. Examples of common unique identifiers used by Monash University are the student ID number and the staff ID number.

- Monash must only assign unique identifiers if it is necessary for Monash to carry out any of its functions efficiently.

When thinking about creating a new type of unique identifier (other than the student/staff number), consider whether it is necessary, eg would it be sufficient to identify the individual by their name. In some sensitive or delicate situations unique identifiers may enhance privacy. In testing whether efficiency is established, an assessment of efficiency from the perspective of both Monash and those with whom it deals is required.

HPP 8 – ANONYMITY

- Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering into a transaction with Monash.

As a general rule, it is not lawful and practicable for individuals to remain anonymous when dealing with Monash. For example it may not possible to provide a complete health service to an individual without knowing who they are. Examples of situations where individuals remain anonymous are the sale of products or services by cash such as books or theatre tickets, or the making of general enquiries such as 'What time are you open?'

HPP 9 – TRANSBORDER DATA FLOWS

- Monash may only transfer information about an individual to someone (other than the individual or Monash) who is outside of Victoria if:

Monash University South Africa and Monash University Malaysia are not considered to be transfers to Monash and therefore transfers to these overseas campuses must be treated in accordance with this principle. The Monash University centres located in Prato, Italy and London, United Kingdom are considered to be transfers to Monash and therefore do not have to be treated in accordance with this principle.

- Monash reasonably believes the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of information that are substantially similar to the Health Privacy Principles.

Commonwealth government organisations, companies with annual turnover of more than $3million, some state government agencies (eg NSW) or a selection of other types of organisations in Australia have equivalent privacy laws. Therefore transfers to these types of organisations located outside of Victoria comply with this Transborder Data Flow principle.
Some countries have equivalent privacy laws in place (eg United Kingdom) and transfer can occur under this provision. However, many countries do not have equivalent privacy laws (eg no laws in Malaysia or South Africa) and a transfer must fall within one of the following categories in order to comply with this principle.

-the individual consents to the transfer

When obtaining consent from the individual to transfer information to an organisation who is located outside Victoria, the individual must be made aware of whether the privacy protection will travel with the information for legitimate consent to be obtained.

-the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request

-the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party

-all of the following apply:

- the transfer is for the benefit of the individual
- it is impracticable to obtain the consent of the individual to that transfer
- if it were practicable to obtain that consent, the individual would be likely to give it.

-the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Health Privacy Principles.

If a transfer of health information outside of Victoria does not fall within any of the above categories, then this category can be complied with if the recipient of the information is requested to sign a contract which binds them to comply with the Health Privacy Principles. The standard privacy contract can be obtained from the Monash University Privacy Officer.

HPP 10 – TRANSFER OR CLOSURE OF THE PRACTICE OF A HEALTH SERVICE PROVIDER

- This principle sets out the procedure which must be followed if a health service provider is closed or sold. Advice can be provided from the Monash University Privacy Officer if Monash University intends to close a health service provider it operates.

HPP 11 – MAKING INFORMATION AVAILABLE TO ANOTHER HEALTH SERVICE PROVIDER

- If an individual requests a health service provider to make health information relating to the individual held by the provider to another health service provider, or authorises another health service provider to request the health service provider to make information available to the health service provider about the individual, the health service provider who holds the information about the individual must provide copies or a summary of the health information to the health service provider.

- A health service provider must comply with the requirements of this principle as soon as practicable.

COLLECTION OF PERSONAL INFORMATION

Collection of your personal information

- Enrolment Forms Collection Statement
- HR Services Collection Statement

The privacy laws arise from Victorian Legislation. Consequently, the Monash University Privacy Policy applies only to personal information that a person provides to Australian campuses of Monash University. Students studying at Monash Malaysia or Monash South Africa should refer to local policies in relation to confidentiality or privacy.

Monash University values the privacy of every individual's personal and health information and is committed to protecting the information it holds and uses about all individuals who provide personal information to the university.

Personal information means information or an opinion (including information or an opinion forming part of a database) that is recorded in any form, whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. It may include sensitive and health information.

Monash University collects personal information in various ways. Monash University is currently working to make the collection of personal information more transparent including by providing you with the following information at the point where personal information is collected:

- the purposes for which the personal information is collected;
- the organisations to whom Monash University usually discloses the personal information;
- any law that requires the particular information to be collected; and
- the main consequences for you if all or part of the information is not provided.

Monash University may also seek your consent to your personal information being used or disclosed for certain purposes. Whilst this process is being completed, please do not hesitate to contact the Monash University Privacy Officer for further information about the above matters.

If you would like further information on the information handling practices at Monash University please go to the Privacy Policy or contact the Privacy Officer at:

Privacy Officer
HR Division
PO Box 92
Monash University
Victoria 3800

Email: *privacyofficer@adm.monash.edu.au*
Phone: (03)9902 9589

The following information is provided to inform you on how we use your personal information collected in the enrolment forms you have completed.

Enrolment Forms Collection Statement

(Applies to: Course Enrolment Form, Unit Amendment Form, Variation to Personal Details, Enrolment Questionnaire, Summer Enrolment Form and Application for Deferment)

The information on these forms is collected for the primary purpose of providing you with the course of study for which you are enrolled. Other purposes of collection include:

- to correspond with you;
- attend to day to day administrative matters;
- inform you about your courses and other university courses/events;
- placing your name on the student electoral roll; and
- to comply with legislative reporting requirements.

The information collected on these forms may be disclosed to the following types of organisations:

- government departments such as the Australian Taxation Office, the Department of Education, Science and Training and the Department of Immigration, Multicultural and Indigenous Affairs;
- external organisations such as professional bodies, hospitals or government agencies, if the disclosure is necessary in order for you to undertake a practical experience/clinical component in your course;
- off-shore Monash campuses, if necessary for any overseas study undertaken
- Monash cooperative offshore partners, if necessary for the enrolment in, administration, promotion and management of related courses;
- Monash owned entities e.g. The Monash College group; and
- contracted service providers which the University uses to perform services on its behalf (such as banks, mailing houses, logistics and IT service providers).

If you choose not to complete all the questions on the form, it may not be possible for the University to enrol you. You have a right to access personal information that Monash University holds about you, subject to any exceptions in relevant legislation. If you wish to seek access to your personal information or inquire about the handling of your personal information, please contact the University Privacy Officer at privacy.officer@adm.monash.edu.au.

HR Services Collection Statement

(Applies to HR Services Forms)

The information on forms provided to HR Services is collected for the primary purpose of providing employment or enabling authorised persons to utilise Monash University's services and facilities. The information may also be used for a related secondary purpose in circumstances where you would reasonably expect such use or disclosure. These include to:

- determine and process your pay and other entitlements;
- correspond with you;
- inform you about the range of facilities and services available to staff;
- notify in the event of an emergency, your nominated emergency contact person;
- comply with legislative reporting requirements;
- attend to day to day administrative matters;
- prepare statistical analyses; and
- use the information as otherwise permitted by the privacy laws.

The information collected on these forms may be disclosed to the following types of organisations:

- your nominated financial institution for payment of salary;
- your superannuation scheme eg. Unisuper;
- government departments such as the Australian Taxation Office and the Department of Immigration, Multicultural and Indigenous Affairs;
- organisations that provide salary packaging benefits to eligible and participating staff members, such as Qantas Club membership, gymnasiums, childcare, car parking permits and novated leasing;
- organisations that provide staff with the option to request automated deductions for services, such as health insurance providers, union fees University Club fees and CityLink;
- off-shore Monash campuses, if necessary for any secondment or overseas work undertaken;
- contracted service providers which the University uses to perform services on its behalf (such as recruitment agencies, travel agents, banks, printers/mailing houses, logistics and IT service providers);
- the University's legal advisers or other professional advisers and consultants engaged by the University; and
- the disclosure is otherwise permitted by the privacy laws.

If all of the information requested is not provided, it may not be possible for the University to process the particular request or entitlement. You have a right to access personal information that Monash University holds about you, subject to any exceptions in relevant legislation. If you wish to seek access to your personal information or inquire about the handling of your personal information, please contact the University Privacy Officer at; privacyofficer@adm.monash.edu.au.

LINKS

- Freedom of Information at Monash University (*www.adm.monash.edu.au/unisec/foi/*)
- Records and Archives Services at Monash University (*www.adm.monash.edu.au/magpie/*)
- Privacy Victoria (*www.privacy.vic.gov.au*)
- Information Privacy Act 2000 (*http://www.dms.dpc.vic.gov.au/l2d/I/ACT01911/index.html)*
- Information Privacy Principles (available from Schedule 1 of the Information Privacy Act) (*http://www.dms.dpc.vic.gov.au/l2d/I/ACT01911/index.html)*
- Private Lives- Your Guide to Privacy Law in Victoria (produced by the Victoria Law Foundation) *(http://www.victorialaw.org.au/PrivateLives/index.htm*)
- Office of the Health Services Commissioner (*www.health.vic.gov.au/hsc*)
- Health Records Act 2001 (*http://www.dms.dpc.vic.gov.au/l2d/H/ACT01966/index.html)*
- Health Privacy Principles (*http://www.health.vic.gov.au/hsc/hppextract.pdf*)
- Office of the Federal Privacy Commissioner (*www.privacy.gov.au*)
- Privacy Act 1988 (*http://www.privacy.gov.au/act/index.html*)

DOCUMENTS FOR STAFF

- Privacy Brochure (to download)
- Summary of Privacy Laws (to download)
- Privacy Watch Newsletter (to download)

EXEMPTIONS IN THE PRIVACY LAWS

The following exemptions apply under the Information Privacy Act and the Health Records Act.

Courts and Tribunals

The privacy laws do not apply to the collection, holding, management, use, disclosure or transfer of personal or health information in relation to the judicial or quasi-judicial functions of a court or tribunal.

Publicly-available information

The privacy laws do not apply to personal or health information contained in:

- A generally available publication
- A library, art gallery, or museum for reference, study or exhibition
- A public record that is available for inspection under the Public Records Act
- Archives within the meaning of the Copyright Act 1968 (Cth)

Law Enforcement Agencies

There are certain components of the privacy laws (eg collection notices under IPP 1.3) which law enforcement agencies are not required to comply with if it believes on reasonable grounds the non-compliance is necessary for the purposes of its functions as a law enforcement agency.

Freedom of Information Act

IPP 6 and HPP 6 do not apply to a document containing personal or health information that would fall within the Freedom of Information Act.

HEALTH RECORDS ACT

There are further exemptions under the Health Records Act which apply specifically to health information. For example an exemption applies to health information:

- Collected, held, used or disclosed by an individual in connection with his or her personal, family or household affairs
- Collected, used or disclosed by the news media in connection with its news activities.
- About an individual who has been dead for more than 30 years.

INFORMATION PRIVACY ACT

The Information Privacy Act does not apply to deceased persons or companies. It only provides rights to living persons.

What Happens If Someone Complains To Monash University Or If Monash University Breaches The Privacy Laws?

Complaints or Concerns

- If an individual believes that Monash University has breached their privacy or is concerned about the potential for certain policies or procedures to do so, they may contact the relevant Privacy Co-ordinator within their Faculty or Division or the Monash University Privacy Officer to speak about their concerns.
- If they would like the matter investigated, they are required to put their complaint into writing.
- The matter will be investigated and a response to the complaint provided by Monash University.
- If the individual is unhappy with Monash's response they may take their complaint to either of the following organisations:

Victorian Privacy Commissioner

Telephone: +61 3 8619 8719
Facsimile: +61 3 8619 8700
Email: enquiries@privacy.vic.gov.au
Website: www.privacy.vic.gov.au

Victorian Health Services Commissioner

Telephone: +61 3 8601 5200
Facsimile: +61 3 8601 5219
Email: hsc@dhs.vic.gov.au
Website: www.health.vic.gov.au/hsc

The relevant commissioners will conciliate the matter and attempt to resolve the issues between the parties.

If the relevant Commissioner cannot resolve the matter, the complainant may make a claim with the Victorian Civil and Administrative Tribunal (VCAT). VCAT has the jurisdiction to award a variety of remedies.

Privacy Commissioner Powers

- The Privacy Commissioner may serve a compliance note on an organisation if it appears that the organisation has breached the privacy laws. The compliance notice requires the organisation to take specified action within a period of time specified. If an organisation does not comply with a compliance notice, it may receive penalties of up to $300,000.
- The Privacy Commissioner may also audit the university for compliance with the laws.

Disclosure of personal information to 3rd parties

The privacy laws specify that if Monash University provides personal, sensitive or health information to a third party and that third party breaches the privacy of the individual, then both Monash University and the third party may be liable for the breaches.

Monash can implement steps to protect itself against breaches of the privacy laws by a third party by including in the contract the necessary privacy clauses.

The contract between Monash and the third party should contain a requirement that the third party is bound by the privacy laws (Information Privacy Act and Health Records Act) with respect to any personal, sensitive or health information Monash provides the third party during the course of the relationship.

If the contract has the appropriate privacy clauses any act or practice by the third party which is contrary or inconsistent with the privacy laws is capable of being enforced against the third party in accordance with the procedures set out in the privacy laws.

IMPORTANT: *When providing personal, sensitive or health information to third parties, it is important to ensure that the appropriate contractual provisions are included in the contract. If no contract exists, stand alone privacy agreements are available. For advice about the appropriate privacy clauses in contracts please contact the Monash University Privacy Officer or the Solicitor's office.*

MONASH UNIVERSITY PRIVACY POLICY

For Use by all University Staff and Students at Australian Campuses

Policy Statement

Monash University values the privacy of every individual's personal and health information and is committed to protecting the information it holds and uses about all individuals who provide personal information to the university.

This policy outlines how Monash University intends to handle personal and health information. Monash University is required to comply with a number of privacy laws operating throughout Australia, including the *Information Privacy Act* 2000 (Vic), the *Health Records Act* 2001 (Vic) ("**Privacy Laws**"). The Privacy Laws regulate how personal information is handled throughout its life cycle, from collection to use and disclosure, storage, accessibility and disposal. It applies to any personal information or health information that a person provides to Australian campuses of Monash University.

Principles

The policy is based on the following principles:

- Monash University supports responsible and transparent handling of information;
- Monash University respects an individual's right to know how his or her personal information will be used, stored and disposed; and
- It is a necessary condition for Monash University to participate in global e-communications and e-transactions.

Broad Overview

The Information Privacy Act 2000 (Vic) sets out ten information privacy principles (IPPs) and the Health Records Act 2001 (Vic) sets out 11 Health Privacy Principles (HPPs). These principles concern the way in which information is collected, used, handled, disclosed and disposed. Monash University has established a privacy regime that strives to:

- Promote an understanding and acceptance of the privacy principles and their objectives throughout the university community
- Educate people within the university about information privacy
- Handle any complaints received in an efficient and appropriate manner
- Monitor privacy compliance and keeps the university informed of updates to procedures

This policy explains Monash University's approach towards protecting the privacy of an individual's personal and health information.

Application

All University staff and students and other individuals who transact with Australian campuses of the university.

The privacy laws arise from Victorian legislation. Consequently, the Monash University Privacy Policy applies only to personal information that a person provides to Australian campuses of Monash University. Students studying at Monash Malaysia or Monash South Africa should refer to local policies in relation to confidentiality or privacy.

Operative Date

Operative from first full pay period to commence on or after 30 August 2002

Policy Authorisation

Deputy Vice-Chancellor (Resources)

Policy Administrator

Director, Policy & Consultancy, Human Resources Division

DETAILED POLICY

Definitions

1.0 Definitions

1.1 Health Information: Personal Information or an opinion about

- the physical, mental or psychological health (at any time) of an individual
- a disability (at any time) of an individual
- an individual's expressed wishes about the future provision of health services to him or her
- a health service provided or to be provided to an individual

and also includes

- other personal information collected to provide or in providing, a health service
- other personal information about an individual collected in connection with the donation or intended donation by the individual of his or her body parts, organs or body substances
- other personal information that is genetic information about an individual in a form which is or could be predictive of the health (at any time) of the individual or of any of his or her descendents

1.2 Identifier: An identifying name or code (usually a number) assigned by an organisation to an individual to uniquely identify that individual for the purposes of the operations of the organisation. This does not include an identifier that consists only of the individual's name

1.3 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.
The *Health Records Act* excludes from its definition of personal information, information about anyone who has been dead for more than 30 years.
The *Health Records Act* includes information that is not recorded in a material form.

1.4 Primary Purpose: A primary purpose is one for which the individual concerned would expect their information to be used. Using the information for this purpose would be within their reasonable expectations.

1.5 Secondary Purpose: A secondary purpose may or may not be apparent to the individual concerned, or within their reasonable expectations. Collecting the information may be mandatory (because required by law) or optional. The main distinction is that the service could still be provided even if the secondary purpose were not served.

1.6 Sensitive Information: Information or an opinion about an individual's-

- Racial or ethnic origin
- Political opinions
- Membership of a political association
- Religious beliefs or affiliations
- Philosophical beliefs
- Membership of a professional or trade association
- Membership of a trade union
- Sexual preferences or practices
- Criminal record
- that is also **personal information**.

ISSUES ADDRESSED

Collection

2.0 Collection of Personal Information

2.1 To the extent required by the Privacy Laws:

- Monash University will not collect personal information about an individual unless that information is necessary for one or more of its functions.
- Monash University will collect personal information about an individual only by lawful and fair means and not in an unreasonably intrusive manner.

2.2 When Monash University collects personal information directly from an individual (for example if a student enrols in a course), Monash University will take reasonable steps at or before the time of collection to ensure that:

- the individual is aware of certain key matters, such as the purposes for which Monash University is collecting the information;
- the organisations (or types of organisations) to which Monash University would normally disclose information of that kind;
- the fact that the individual is able to access the information; and
- how to contact Monash University.

2.3 Monash University will collect personal information directly from an individual where it is reasonable and practicable to do so. Where Monash University collects information about an individual from a third party (for example if a student authorises a parent, spouse or partner to register for them on their behalf), Monash University will still take reasonable steps to ensure that the individual is made aware of the details set out above

2.4 While Monash University generally collects personal or health information directly from the relevant individual, in some cases we may collect it from a third party, such as VTAC, a temporary employment agency or a contractor.

2.5 The main functions of Monash University are to provide teaching and research services, together with ancillary services which, may support students and staff in their study or work at the university. Some information needs to be collected by Monash University as the government requires the information for statistical purposes.

2.6 If an individual chooses not to provide the information requested, Monash University may not be able to provide services to that individual.

Use and Disclosure

3.0 Use and Disclosure of Personal Information

3.1 Monash University has a duty to maintain the confidentiality of staff and students' personal and health information. To the extent required by the Privacy Laws, Monash University will only use or disclose personal information for a secondary purpose other than the primary purpose for which it was originally collected where:

- the secondary purpose is related to the primary purpose (or is directly related, in the case of sensitive information or health information), and a person would reasonably expect Monash University to use or disclose the personal information for that secondary purpose; or
- a person has consented to the use or disclosure of their personal information for the secondary purpose; or
- the use or disclosure is required or authorised by or under law; or
- the use or disclosure is otherwise permitted by the Privacy Laws.

Quality Data

4.0 Security and Quality of Personal Information

4.1 Monash University is committed to ensuring that personal information is held securely. To the extent required by the Privacy Laws, Monash University will take reasonable steps to:

- ensure that any personal information Monash University collects, uses and discloses is accurate, complete and up to date;
- protect the personal information that Monash University holds from misuse, loss, unauthorised access, modification or disclosure: and
- destroy or permanently de-identify personal information when required by the Privacy Laws.

4.2 Personal information may be stored in hard copy documents, as electronic data, or in Monash University's software or systems. Some of the ways Monash University seeks to protect personal information include the following:

- confidentiality requirements on the use of information by Monash University's employees
- policies on document storage and security
- security measures for access to Monash University's computer systems
- controlling access to Monash University's premises
- web site protection measures.

4.3. Staff and students can help Monash University keep the personal information that it holds accurate, complete and up to date, by directly updating information on-line through the SAP or Callista systems for address and contact details, or by promptly notifying Student and Staff Services, or alternatively by submitting an amendment form to the Privacy Officer.

4.4 Contact details for the Privacy Officer are as follows:

Privacy Officer
Human Resources Division
PO Box 92
Monash University, Victoria 3800
Email: privacyofficer@adm.monash.edu.au
Phone: 039902 9589

Access

5.0 Access to Personal Information

5.1 Monash University will, on request, provide staff and students with access to information it holds about them, unless there is an exception that applies under the Information Privacy Principles or Health Privacy Principles such as:

- access would pose a serious threat to the life or health of any individual;
- access would have an unreasonable impact on the privacy of others;
- the request is frivolous or vexatious;
- the information relates to commercially sensitive decision making process;
- access would be unlawful or denying access is required or authorised by law (e.g. Monash University has a duty of confidentiality and will not provide access to personal information about you if it will breach that duty);
- access would prejudice enforcement activities relating to criminal activities and other breaches of law, public revenue, a security function, or negotiations with the individual; or
- the information is to be used for legal dispute resolution proceedings

5.2 To make an application to access personal information, please contact the Freedom of Information Officer on (03) 9905 5137.

Students wishing to gain access to their student records may be permitted to do so by the Manager of Student Administration. Requests for access should be made in writing to the Divisional Director, Manager of Student Administration, PO Box 3C, Monash University, Vic 3800.

5.3 If Monash University doesn't provide a staff or student member with access, the staff or student member will be provided with written reasons for the refusal and informed of any exceptions relied upon.

5.4 Any request to provide information will be dealt with in a reasonable time and Monash University may recover from a student or staff member the reasonable cost of accessing and supplying this information.

Identifiers

6.0 Commonwealth and State Government Identifiers

6.1 Except to the extent permitted by the Privacy Laws, Monash University will not use Commonwealth or State government identifiers as its own identifier nor will it disclose such identifiers to anyone else.

6.2 Monash University will only assign identification numbers to individuals if the assignment of identifiers is reasonably necessary to enable it to carry out its functions efficiently. For example, both staff and student numbers are necessary to enable Monash University to carry out its functions.

Anonymity

7.0 Anonymity

7.1 Monash University will provide an individual with the option of not identifying who they are when it is lawful and practicable to do so. The nature of the business carried on by Monash University means that, generally, it is not possible for the university to provide services to student or staff members in an anonymous way.

Transborder Data Flows

8.0 Transborder Data Flows

8.1 Monash University may transfer your personal information overseas where it is necessary to do so, for example where a student studies or an employee works at an international campus. If Monash University transfers personal information outside Victoria, Monash University will comply with the relevant requirements of those Privacy Laws that relate to transborder data flows outside Victoria.

8.2 This stipulates that the recipient of the information must protect privacy of personal information to a similar standard as the Victorian IPPs.

Obligations of Staff and Students

9.0 Obligations of staff and students

9.1 When a staff or student member provides Monash University with personal and health information about other individuals, Monash University relies on that person to have made the other individuals aware:

- That their information will or may be provided to Monash University
- Of the types of third parties to whom Monash University may provide that information,
- Of the relevant purposes of the information, and
- how they can access it.

If it is sensitive information Monash University relies on the staff or student member to have obtained consent from the other individuals to the above uses.

9.2 If a staff member collects, uses, discloses or handles personal information on Monash University's behalf, the staff member must meet the relevant requirements of the Information

Privacy Principles set out in the *Information Privacy Act 2000* and the Health Privacy Principles set out in the *Health Records Act 2001*. Staff members must only collect, handle, use, disclose and store the information for the agreed purposes only.

To stop receiving Monash material

10.0 Opting out of receiving material produced by Monash University

10.1 If a student or staff member does not wish to receive Monash University's publications, then the student or staff member can opt out by sending an email to Monash University's Privacy Officer on privacyofficer@adm.monash.edu.au or by contacting Monash University's Privacy Officer on 039902 9589.

Contacting and/or complaining to Monash University about its privacy practices

11.0 How to contact Monash University regarding privacy issues

11.1 If a student or staff member has any privacy issues that he or she would like considered by Monash University, the person may contact the Privacy Co-ordinator within their faculty/divisional unit. The Privacy Co-ordinator will undertake a preliminary investigation of the issue and report back to the person who raised the issue, his or her view of whether there has been a breach of this policy or one or more of the Information Privacy Principles or Health Privacy Principles. The Privacy Co-ordinator will also indicate what action, if any, Monash University will take to rectify the situation.

11.2 If the student or staff member is not satisfied with the response of the Privacy Co-ordinator, the student or staff member can complete a Complaint Form attached to this policy and send it to Monash University's Privacy Officer for consideration. The Privacy Officer will conduct a further investigation and will report back to the person who raised the issue, his or her view of whether there has been a breach of this policy or one or more of the Information Privacy Principles or Health Privacy Principles. The Privacy Officer will also indicate what action, if any, Monash University will take to rectify the situation.

11.3 If a member of the public has an issue he or she would like considered then the member of the public should contact the Privacy Officer directly.

Disciplinary Action

12.0 Breach of this policy

12.1 If a staff member breaches this policy, depending on the circumstances it may be regarded as misconduct or poor performance and this may result in action being taken in accordance with the provisions set out in the Monash University enterprise agreement.

Change of Policy

13.0 Change of Policy

13.1 Monash University may change this Privacy Policy from time to time without prior notice.

Relevant Australian Legislation, Policies and Associated Documentation

Privacy

14.0 Legislation

- Information Privacy Act 2000 (Vic)
- Health Records Act 2001 (Vic)
- Freedom of Information Act 1982 (Vic)
- Privacy Amendment (Private Sector) Act 2000

Associated Policies and Legislation (including Guidelines & Procedures)

15.0 Associated Documentation

- Monash University Staff Handbook
- Monash University enterprise agreement
- Monash University Confidentiality Policy

Further Information & Policy Review Details

Further Information and Assistance

16.0 Further Information and Assistance

16.1 Adherence to this policy will generally ensure compliance with University requirements 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 an incident, should contact:

- The Privacy Officer on ext. 29589
- Policy and Consultancy Group, HR Division, on ext. 56044 or http://www.monash.edu.au/personnel/
- The University Solicitor's Office on ext. 55126.

16.2 For more information on privacy see the Victorian Privacy Commissioner's website at http://www.privacy.vic.gov.au/ or the Office of the Health Services Commissioner at http://www.dhs.vic.gov.au/ahs/health/hsc/ .

Review Dates

Amendment Number	Authorisation	Date	Reference

Key Words/Phrases

privacy, information, personal, sensitive, health, records, security, data quality, privacy officer

MONASH UNIVERSITY COLLECTION, STORAGE AND DESTRUCTION OF CREDIT CARD DETAILS POLICY

For Use by all University Staff

Policy Statement

Monash University values the privacy of credit card information and is committed to protecting the credit card details it holds and uses.

This policy outlines how Monash University intends to collect, store and destroy credit card details.

Principles

The policy is based on the following principles:

- Monash University must take reasonable steps to protect the credit card details it holds from misuse and loss and from unauthorised access, modifications and disclosure.
- It is a necessary condition for Monash University to provide credit card facilities to individuals for the payment of services and goods provided by Monash University.

Broad Overview

Monash University may consider the following matters when adopting reasonable steps to protect the credit card information it holds:

- The sensitivity of credit card details and an individual's expectations that this information will be protected from misuse and loss and from unauthorised access, modifications and disclosure;
- The harm likely to result if there is a breach of security; and
- The form in which the information is stored (eg on paper or electronically) processed and transmitted.

Application

All University staff.

Operative Date

Operative from first full pay period to commence on or after 18 May 2003

Policy Authorisation

Divisional Director, HR Division

Policy Administrator

Director, Policy & Consultancy, Human Resources Division

DETAILED POLICY

Application of Policy

1.0 Application of Policy

This policy is designed to deal with situations where a person provides details of their credit card to the university. The policy is also designed to ensure that Monash University will store and destroy credit card details in a manner which protects the credit card details from:

- misuse;
- loss;
- unauthorised access;
- unauthorised modification; and
- unauthorised disclosure.

Collection of Credit Card Details

2.0 Collection of Credit Card Details

Monash University is committed to ensuring that credit card details are collected in a secure manner. Monash University will take reasonable steps to protect the credit card details it holds from misuse and loss and from unauthorised access, modifications and disclosure during collection by adopting the following practices:

- preventing individuals from providing credit card details in an email;
- ensuring that where credit card details are collected on-line, encryption in accordance with the University's IT Security Policy and IT Security Framework is included within the on-line web page, databases and other supporting programs;
- only collecting credit card details in an appropriate environment, for example not requesting credit card details verbally in a public waiting room; and
- ensuring that when credit card details are collected via facsimile, the facsimile is placed in a secure location.

Storage of Credit Card Details

3.0 Storage of Credit Card Details

3.1 Monash University is committed to ensuring that credit card details are held securely. Monash University will take reasonable steps to protect the credit card details it holds from misuse and loss and from unauthorised access, modifications and disclosure by adopting the following practices:

- ensuring that credit card details are stored in a secure and protected manner such as locked filing cabinets;
- where possible, removing any credit card details from Monash University networked computers;
- ensuring that EFPTOS machines and other devices used to collect credit card details are stored securely, particularly when they are not in use (eg overnight);
- ensuring that appropriate staff only have access to credit card details; and
- ensuring information is transferred securely (for example, not transmitting credit card details via e-mail).

3.2 Credit card details may be stored in hard copy documents. If credit card details are stored as electronic data appropriate security measures must be utilised in accordance with the University's IT Security Policy and IT Security Framework. Some of the ways Monash University seeks to protect credit card details include the following:

- confidentiality requirements on the use of information by Monash University's employees;
- policies on document storage and security;
- security measures for access to Monash University's computer systems;

- controlling access to Monash University's premises;
- web site protection measures.

3.3 Credit Card details are required to be stored onsite or in an easily accessible location for 12 months for charge back purposes. After 12 months, credit card details may be moved offsite providing the credit card details are stored in a secure location.

3.4 Credit card details must be stored for the length of time prescribed by the Records Disposal Authority.

Destruction of Credit Card Details

4.0 Destruction of credit card details

Credit card details will be destroyed in a secure manner when they are no longer needed by Monash University. Examples of destruction in a secure manner include shredding, pulping or disintegration of paper files, fire, confidential disposal in accordance with any guidelines provided by Records & Archives, encryption or scrubbing of credit card number or contracting an authorised disposal company for secure disposal.

For further information

5.0 For further information

For further information about this policy please contact:

Privacy Officer
Human Resources Division
Monash University, Victoria 3800
Email: privacyofficer@adm.monash.edu.au
Phone: 039902 9589

Or refer to the IT Security Policy (www.adm.monash.edu.au/pol/itec13.html) and IT Security Framework Document (www.its.monash.edu.au/security/framework) for IT requirements.

Obligations of Staff

6.0 Obligations of staff

If a staff member collects credit card details on Monash University's behalf, the staff member must meet the relevant requirements of this policy in relation to the storage of credit card details.

Disciplinary Action

7.0 Breach of this policy

If a staff member breaches this policy, depending on the circumstances it may be regarded as misconduct or poor performance and this may result in action being taken in accordance with the provisions set out in the Monash University enterprise agreement.

Change of Policy

8.0 Change of Policy

Monash University may change this policy from time to time without prior notice.

Relevant Australian Legislation, Policies and Associated Documentation

Privacy

9.0 Legislation

- Information Privacy Act 2000 (Vic) http://www.dms.dpc.vic.gov.au/l2d/I/ACT01911/index.html
- Health Records Act 2001 (Vic) http://www.dms.dpc.vic.gov.au/l2d/H/ACT01966/index.html
- Freedom of Information Act 1982 (Vic) http://www.dms.dpc.vic.gov.au/
- Electronic Transactions (Victoria) Act 2000 http://www.dms.dpc.vic.gov.au/sb/2000_Act/A00695.html

Associated Policies and Legislation (including Guidelines & Procedures)

10.0 Associated Documentation

- Monash University IT Security Policy www.adm.monash.edu.au/pol/itec13.html
- Monash University IT Security Framework www.its.monash.edu.au/security/framework
- Monash University enterprise agreement http://www.monash.edu.au/entbarg/
- Monash University Privacy Policy http://www.privacy.monash.edu.au/pc_privacy_pol.htm
- Monash University Confidentiality Policy http://www.adm.monash.edu.au/unisec/academicpolicies/policy/confidentiality.html

Further Information & Policy Review Details

Further Information and Assistance

11.0 Further Information and Assistance

Adherence to this policy will generally ensure compliance with University requirements and relevant 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 an incident, should contact:

- The Privacy Officer on ext. 29589
- The IT Security Policy (www.adm.monash.edu.au/pol/itec13.html) and IT Security Framework Document (www.its.monash.edu.au/security/framework).
- Policy and Consultancy Group, HR Division, on ext. 56044 or http://www.monash.edu.au/personnel/
- The University Solicitor's Office on ext. 55126.

Review Dates

Amendment Number	Authorisation	Date	Reference

Key Words/Phrases

Credit card details, storage, privacy, information, personal, records, security, privacy officer, IT Security Manager

GUIDELINES FOR COLLECTING / DISTRIBUTING STUDENT RESULTS / ASSIGNMENTS AND OTHER INFORMATION

The *Information Privacy Act (Vic) 2000* contains ten Information Privacy Principles (IPP) which regulate how personal information is handled throughout its life cycle, from collection to use and disclosure, storage, accessibility and disposal. Several of these IPP's impact on the distribution of student results and assignments and other information such as the distribution of information re practical placements. This document provides guidance on how to enhance compliance with the relevant IPP's when collecting the student information and distributing the student information.

In these guidelines:

Student Information includes (but is not limited to):

- Assignments
- Examinations
- Results
- Results
- Student results collated in a list with identification by student number only (The student ID number is likely to be considered personal information and therefore needs to be treated in accordance with the privacy laws)
- Practical Placement / Clinical Placement details

IPP 1- Collection

Assignments:

The university has general practices that require students to complete an assignment cover sheet when submitting an assignment. Information on this assignment cover sheet is regarded in law as 'personal information'. As a consequence, Monash has legal obligations to fulfil when collecting such information. For example, at or before the time of collecting personal information, Monash is required to inform individuals of the following matters:

- The fact that the individual is able to gain access to the information;
- The purposes for which the information is collected;
- To whom (or the types of individuals or organisation to which) Monash usually discloses information of that kind;
- Any law that requires the particular information to be collected; and
- The main consequences (if any) for the individual if all or part of the information is not provided.
- Privacy Officer details

- Who is the organisation collecting the information and how they can obtain access to it.

It is recommended that steps are taken to include notification of these matters on the assignment cover sheets. Below is an example of some standard wording which may be used.

> The information on this form is collected for the primary purpose of assessing your assignment. Other purposes of collection include recording your plagiarism and collusion declaration, attending to administrative matters and statistical analyses. If you choose not to complete all the questions on this form, it may not be possible for Monash University to allow the submission of your assignment. You have a right to access personal information that Monash University holds about you, subject to any exceptions in relevant legislation. If you wish to seek access to your personal information or inquire about the handling of your personal information, please contact the University Privacy Officer via email: privacyofficer@adm.monash.edu.au.

The privacy collection statement above contains the necessary requirements to comply with the privacy laws. If you would like to use an amended version of the collection statement, it is recommended that you provide the amended version to the Privacy Officer for confirmation that it meets the requirements of the privacy laws.

Other Information:

When collecting other personal information from students (eg practical placement preferences), it is also important to include a privacy collection notice. The privacy collection notice will need to be modified depending on the required uses and disclosures. Below is the model collection notice used by Monash University.

> The information on this form is collected for the primary purpose of **[insert primary purpose].** Other purposes of collection include **[insert secondary purposes].** If you choose not to complete all the questions on this form, it may not be possible for **[insert name eg. the Faculty]** to **[insert consequence]**. Personal information may also be disclosed to **[list any 3rd parties personal information is disclosed to (do not include Monash staff)]** You have a right to access personal information that Monash University holds about you, subject to any exceptions in relevant legislation. If you wish to seek access to your personal information or inquire about the handling of your personal information, please contact the University Privacy Officer on9902 9589.

If you require assistance drafting an appropriate collection notice, depending on the type of information collected, please do not hesitate to contact the Privacy Officer on by email: privacyofficer@adm.monash.edu

IPP 4- Data Security

Once you have received the personal information from the student eg. on the assignment cover sheet, there are further legal obligations which exist in relation to the protection of the information. IPP 4 requires Monash to take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

There are currently several practices within Monash for the distribution of student information. It is possible that some of these methods may now require improvements to enhance compliance with the privacy laws. With the existing practices, there may be risk of the personal information being accessed or disclosed without authorisation. This is because we may be disclosing student's personal information to other student's (or even other individuals) without consent by distributing their information in a public way.

The following recommendations could be implemented to allow students the option of giving consent for their information to be left in a public area. It provides further protection from breaching the privacy laws but also provides an efficient and effective means of distributing student information.

Preferred method for optimal compliance

- If the way in which we distribute student information does not disclose personal information to other students then we do not have to obtain consent from the student. Student information may be distributed in any of the following ways without obtaining consent:

    - During lectures or tutorials without disclosing the personal information (other than name) of students eg a name call (1st name only if possible).
    - Student information is left with an administrative staff member for collection. Students would need to present their student ID card for proof of identity
    - Students collect the student information from the lecturer of tutor outside class time. The lecturer or tutor may nominate a time when the information could be collected.

These options may take valuable class time and the time of staff. The use of class time and resources should be considered when working out the best way for distributing student information. The options above would be most beneficial for small classes and may not be practical for large classes or subjects which have many students.

Other options

- Seek consent from students for the student information to be distributed in the preferred way.

    To obtain consent, a statement such as the following should be placed on the document collecting the information which will ultimately be distributed to students eg assignment cover sheet, practical placement/ clinical placement preference sheet:

    > 'Your assignment/result (or practical placement- amend as necessary) will be returned as per the information given in the unit outline. If you do not want your assignment/result returned in this way please contact

your lecturer/tutor on or before the assignment due date and complete the approval below:

Alternative mode of assignment (or practical placement) return has been arranged **Date_____Signature_____ (to be signed by the lecturer/tutor)**

If the student does not contact the lecturer/tutor to make alternative arrangements, then we have implied consent to return the student information in the nominated way. From a privacy perspective this is not the preferred option, however with very large classes it may be the most efficient way of obtaining consent.

- Inform students verbally at the start of the semester of the proposed method of returning information to students. Let them know that they may speak to the lecturer / tutor if they would like to make alternative arrangements. This is another way which we can obtain implied consent. However, if we ever had a dispute about obtaining consent, it would be more difficult to prove that the information was given to the students if it is not in writing. For example, there may be difficulties proving that that the student was present when the information was provided. This option is not recommended, however as a last resort it may be utilised.

Group Assessment Activities

In many instances, it is necessary for students to participate in group assessment activities. This necessitates the collection of several students' information on the same document with disclosure to all other students involved in that assessment activity. In order to protect the privacy of the students' involved in the assessment activity it is preferable to collect as little information as possible about the student on the assignment cover sheet or other relevant documentation. For example, collection of the students name and ID number only is preferred. It is recommended that other personal information is not collected via group assessment activities. Distribution of the assignment results will mean that all participants of the group activity will be aware of other student results. This is not in breach of the privacy laws as it falls within the primary purpose of collecting the information.

FREQUENTLY ASKED QUESTIONS RELATING TO STAFF

1. CAN THE UNIVERSITY ACCESS MY EMAIL, INTERNET WEB LOGS AND OTHER ELECTRONIC FILES UNDER THE PRIVACY LAWS?

Yes, the privacy laws allow Monash to access email, internet web logs and other electronic files in certain circumstances. All email and internet usage should be conducted in accordance with the Information Technology Usage Policy – Staff and Other Authorised Users Policy (available from http://www.adm.monash.edu.au/unisec/pol/itec16.html). This policy sets out the circumstances in which Monash may access staff emails, internet web logs and other electronic files.

2. WHO CAN BE CONTACTED FOR MORE INFORMATION ABOUT THE PRIVACY LAWS WITHIN MONASH UNIVERSITY?

The first contact point for information about the privacy laws at Monash University is the Privacy Co-ordinator within your faculty or division. For the contact details of the Privacy Coordinators, please go to page 71.

Alternatively, you may like to contact the Monash University Privacy Officer as the first contact point within Monash for more information about the privacy laws.

Privacy Officer
Phone: 039902 9589
Email: privacyofficer@adm.monash.edu.au

Alternatively you may like to go to the Monash University privacy website:

www.privacy.monash.edu.au

3. AN INDIVIDUAL HAS COMPLAINED TO ME THAT MONASH HAS BREACHED THEIR PRIVACY. WHAT DO I DO?

If a person has a complaint they should be referred to the Privacy Co-ordinator in your area (if you have one) who is responsible for managing privacy complaints. For the contact details of Privacy Co-ordinators please go to page 71. If you do not have a Privacy Co-ordinator the person can be referred directly to the Monash University Privacy Officer. Alternatively, the individual can complain directly to the Privacy Officer.

4. DOES THE INFORMATION PRIVACY ACT APPLY ONLY TO DOCUMENTS?

No. The Information Privacy Act applies to anything that is recorded. This means that it applies to things such as documents, databases, electronic records, photographs and video footage.

5. A REAL ESTATE AGENT, BANK OR OTHER ORGANISATION HAS PHONED ME TO ASK ABOUT AN EMPLOYEES SALARY, LENGTH OF SERVICE AND OTHER INFORMATION. CAN I PROVIDE THIS INFORMATION TO THEM?

No. Before we provide information to an external organisation, such as a bank or real estate agent, about a staff member, we need to obtain the staff members consent to release the information. Verbal consent is sufficient provided that the person seeking consent is reasonably sure of the identity of the staff member. For information on how to establish a staff member's identity over the phone please refer to question 13 of the FAQ's - Staff. It is preferable to obtain written consent eg email response.

6. A JOB APPLICANT WORKED FOR A FRIEND/COLLEAGUE OF MINE. THE JOB APPLICANT HAS NOT LISTED THE FRIEND/COLLEAGE AS A REFEREE. CAN I CONTACT THEM FOR A REFERENCE?

No. You may be breaching the privacy laws by collecting information from a referee who the individual has not provided consent for Monash to contact.

7. I HAVE BEEN ASKED BY SOMEONE TO BE A REFEREE. I HAVE INFORMATION ABOUT THEIR HEALTH OR PERSONAL LIFE, WHICH THE PROSPECTIVE EMPLOYER MAY LIKE TO KNOW. CAN I TELL THEM?

No. When providing a reference for someone the following are useful guidelines:

- Ascertain the factors that are relevant to the position;
- Only disclose information about the job applicant that is within the applicant's reasonable expectations eg. skills, work experience and personal attributes relevant to the position; and
- Do not disclose personal information that the job applicant has requested not be disclosed.
- Do not disclose information that the job applicant would not reasonably expect you would disclose in the course of providing a reference.

Providing health or personal information to the prospective employer is likely to breach the individual's privacy. The only situation where it may be appropriate to disclose health information is information about a person's ability to cope with stress when that is a consideration that is relevant to the position eg high stress role.

8. DO INDIVIDUALS HAVE THE RIGHT TO ACCESS REFEREE REPORTS WE HAVE COLLECTED ABOUT THEM?

Yes. Subject to exemptions in the law, individuals may have the right to access referee reports under the Freedom of Information laws. It is therefore important to ensure that if you record details of the conversation with the referee, an accurate record of the conversation is recorded and information is only recorded about the applicant's suitability for the particular role. If a prospective employee would like to access their referee reports please refer them to the Freedom of Information Officer or the Privacy Officer for further information.

9. CAN I TAKE PHOTOS OF STAFF AND INCLUDE THEM ON OUR WEBPAGE OR STAFF NOTICE BOARD?

No. You must first obtain consent from staff to use their photos for a webpage or staff notice board. Consent can be obtained at the time of taking the photo. It is important to be aware that staff may revoke consent in the future and if they do, the photo must be removed from the webpage or staff notice board.

10. WHAT DO I NEED TO DO TO COMPLY WITH THE PRIVACY LAWS ON BEHALF OF MONASH?

A useful checklist is contained at the beginning of this compliance manual on page 5 for what staff should do to comply with the privacy laws. If you are implementing a new initiative or project it is important to consider the privacy laws and their ramifications on the project. If you need advice about how to comply with the privacy laws please contact the Monash University Privacy Officer.

11. CAN I USE A STAFF MEMBER'S ID NUMBER FOR GENERAL ADMINISTRATIVE / ORGANISATIONAL PURPOSES?

Yes. The Monash Staff ID Number is the authorised identification number utilised by Monash University. As the staff ID number is most likely personal information under the privacy laws, it must be used in accordance with the privacy principles.

12. CAN I USE A STAFF MEMBER'S MEDICARE NUMBER FOR GENERAL ADMINISTRATIVE / ORGANISATIONAL PURPOSES?

No. As a general guideline, the Medicare number cannot be used as an identifying number for administrative or organisational purposes. Identifiers such as Medicare numbers can only be adopted by Monash as our identifier with consent of the individual. Unique identifiers should only be used by Monash for the purpose for which they are collected. For example, the Medicare number may be used by Community Services for the purposes of providing the healthcare service.

13. A STAFF MEMBER HAS PHONED FOR INFORMATION ABOUT THEIR SALARY. I NEED TO CONFIRM THEIR IDENTITY PRIOR TO RELEASING THE INFORMATION OVER THE PHONE. CAN I ASK THEM FOR THEIR TAX FILE NUMBER AS A WAY OF IDENTIFYING THEMSELVES?

No. Under Tax file number laws it is illegal to request an individual to supply a tax file number to confirm identity. Please do not ask the staff member what their tax file number is to confirm their identity. Large penalties may be imposed for non-compliance.

Before releasing information to the staff number it is recommended that steps are taken to confirm the identity of the staff member.

Eg: the following questions are example which could be used to confirm identity:

- Staff ID Number
- Home phone number;
- Middle Name;
- Date of Birth; and
- Home address.

It is not necessary to record the details of every disclosure. If details are not recorded of every disclosure a customary practice should be established. This means that if a dispute were to arise about releasing information incorrectly, Monash could demonstrate that security measures have been implemented. For example, to establish that a customary practice exists it is recommended that all staff are trained in security of personal information and all staff ask on every occasion three pieces of identifying information to confirm identity prior to releasing information.

The following is appropriate wording of how to begin the process of confirming identity:

'Before I release the information, I am required to confirm your identity. Would you mind telling me….'

14. A STAFF MEMBER RINGS/EMAILS TO REQUEST THEIR TAX-FILE NUMBER. WHAT SECURITY SHOULD BE IMPLEMENTED BEFORE PROVIDING THE TAX- FILE NUMBER?

Providing staff with their tax-file number requires stricter security measures than other personal information.

A representative from the Australian Taxation Office (ATO) recommended that all organisations adopt the same security measures as the ATO when releasing tax-file numbers to staff. There are two methods available to Monash University.

1. Staff members attend the office with photo identification. The tax-file number should not be released until a representative from the office has viewed the ID.
2. A request can be made over the phone. The following pieces of information are required to confirm the individual's identity: full name, DOB and last postal address Monash University has in its records. The tax-file number should then be

sent via letter to the last postal address only. Please do not send it to another address even if requested by the staff member. The address will need to be changed in the system by the usual method eg completing a form or logging onto Eservices before the tax-file number will be sent to another address.

In all instances of releasing the tax-file number it is also recommended that a file note or copy of the letter is added to the staff member's file. If a copy of the letter is added to the staff member's file please ensure that the tax file number is deleted from the letter as tax file numbers must not be stored on an individual's file.

Alternatively, you may refer them to the Australian Taxation Office who release tax file numbers to individuals in a similar manner to that described above.

15. IS THERE ANYONE IN THE FACULTY OR DIVISION THAT I CAN TALK TO ABOUT PRIVACY MATTERS?

Yes. Every Faculty and some Divisions have a Privacy Co-ordinator who has knowledge of the privacy laws. The Privacy Co-ordinator's are listed on page 71. If you are unable to contact the Privacy Co-ordinator from your area or your area does not have a Privacy Co-ordinator please contact the Monash University Privacy Officer.

15. HOW DOES MONASH STORE PERSONAL, SENSITIVE OR HEALTH INFORMATION I PROVIDE?

Personal information may be stored in hard copy documents, as electronic data, or in Monash University's software or systems. Some of the ways Monash University seeks to protect personal information include the following:

- confidentiality requirements on the use of information by Monash University's employees
- policies on document storage and security
- security measures for access to Monash University's computer systems
- controlling access to Monash University's premises
- web site protection measures.

Different areas within the university have different storage systems in place depending on a variety of factors including the level of access required by staff and the sensitivity of the information. For specific information on how your personal information is stored please contact your Privacy Co-ordinator or the Privacy Officer.

16. CAN I SEND GLOBAL EMAILS TO STAFF OR SHOULD THEY BE SENT INDIVIDUALLY?

Global Emails can be sent to staff. If it is necessary for other staff member to see the recipients of the email it can be sent displaying other email addresses. If it is not necessary for other staff to see the recipients of the email you may like to consider sending it 'blind copy' (Bcc) to all recipients of the email.

Frequently asked questions relating to students

1. CAN I PUBLISH STUDENT RESULTS IN A PUBLIC VENUE?

No. Publishing details of student results in a public venue may breach the privacy laws unless we firstly obtain consent from students. 'Guidelines on the release of student results / assignments or other information' have been produced and are available on page 49. In general, lecturers or tutors should obtain the consent from the students if they would like to publish student results in a public venue and the guidelines provide examples of how to obtain consent.

2. CAN I PUBLISH DETAILS ABOUT SUCCESSFUL STUDENTS (EG AWARD WINNERS, HIGH ACHIEVERS, SCHOLARSHIP RECIPIENTS) IN OUR NEWSLETTER OR WEBPAGE?

No. Consent should be obtained from students prior to publicising their success. Verbal consent may be obtained however it is preferable to get consent in writing. If there were a dispute about consent we would need to prove that consent was obtained.

3. CAN I PROVIDE A LIST OF STUDENT DETAILS TO OTHER STUDENTS IN THE CLASS SO THEY CAN FORM STUDY GROUPS?

No. Consent should be obtained from students prior to providing their details to other students for the purpose of allowing them to form study groups. Verbal consent may be obtained however it is preferable to get consent in writing. If there were a dispute about consent we would need to prove that consent was obtained.

4. A STUDENT HAS APPROACHED ME WITH INFORMATION ABOUT THEIR HEALTH OR PERSONAL CIRCUMSTANCES WHICH IS AFFECTING THEIR STUDIES. CAN I INFORM THE STUDENT'S OTHER LECTURERS ABOUT THIS?

No. This information should be treated with extreme confidentiality and only used for the purpose for which it was provided. Given the sensitivity of the information, it is very likely that if it is misused in any way Monash will receive a complaint for breaching the individual's privacy. If there are circumstances which warrant the disclosure of this information (eg serious and imminent threat to life, health or safety of individual) please contact the Privacy Officer for advice.

5. I HAVE TAKEN PHOTOS OF CLASS ROOM SETTINGS AND OTHER MONASH LOCATIONS WHICH DEPICT STUDENTS. CAN I USE THESE PHOTOS TO PROMOTE THE FACULTY/DEPARTMENT/SCHOOL?

No. It is preferable to obtain consent from students to photograph them with the intention of promoting the Faculty/Department/School. It would be preferable to obtain the consent of the students at the time of photographing them. For example, you could explain to the students what the photos will be used for when taking them. If the student does not want to be included they can position themselves so that they

are not a part of the photo. If children are included in the photo (eg photographing Faculty of Education students in the classroom setting) it is important that the consent of the children's parent is obtained prior to them be used to publicising the Faculty/Department/School.

6. CAN I CONDUCT A SURVEY WITH STUDENTS TO PROVIDE FEEDBACK ON A PARTICULAR ASPECT OF THEIR UNIVERSITY LIFE?

Yes. If a survey is a part of a research project it must receive ethical clearance prior to it being conducted. If the survey is designed to assess services currently available to students it must be conducted in accordance with the privacy laws. It is recommended that unless it is necessary for the purposes of the survey to collect personal information, surveys are conducted on an anonymous basis. For further advice on how to comply with the privacy laws when conducting surveys please contact the Privacy Officer.

7. CAN I SEND GLOBAL EMAILS TO STUDENTS OR SHOULD THEY BE SENT INDIVIDUALLY?

Global Emails can be sent to students, however it is important to 'blind copy' (Bcc) all recipients of the email to ensure that the email address is not displayed to other recipients.

8. CAN I PROVIDE INFORMATION ABOUT A STUDENT TO THEIR PARENT/FRIEND/PARTNER? WHAT HAPPENS IF THEY ARE PAYING THE STUDENTS FEES? WHAT HAPPENS IF THE STUDENT IS UNDERAGE?

No. You cannot provide personal information about students to a parent, friend or partner unless you have firstly obtained the consent of the student. This is the same for parents who pay the fees of the student. You will also need to obtain consent from the student to release information to the parents.

In relation to underage students, the majority of underage students are aged 17 studying their first year of university. The privacy laws do not set an age at which an individual can provide consent however they provide guidance. A person can provide consent if they have the intellectual capability and maturity to understand the consequences of providing their consent. In the case of first year students who are 17 years old, as they are studying at university level it can be assumed that they have the ability to make their own decisions and information should not be provided to the parents, friends or partners without obtaining their consent. In relation to the few students who may be younger than 17 years of age a decision about whether to grant parents access to the information would need to be made on a case by case basis taking into account the ability of the student to have the relevant maturity and intelligence to understand the decision they are making. For advice please contact the Privacy Officer.

9. A PARENT HAS CALLED THE UNIVERSITY TO TRANSACT ON BEHALF OF HIS DAUGHTER/SON, FOR EXAMPLE TO PAY LIBRARY FINES. THE STUDENT IS OVERSEAS AND CANNOT CONDUCT THE

TRANSACTION THEMSELVES. CAN I CONDUCT THE TRANSACTION FOR THE PARENT ON BEHALF OF THE STUDENT?

Yes. Providing that no personal information is released to the parent some transactions may be conducted by parents. In determining whether it is appropriate for the parent to conduct the transaction, you will need to ask why the student is not able to do it themselves. If there is a valid reason, eg they are overseas, and the transaction can be conducted without releasing any personal information to the parent then you may proceed. Before conducting the transaction please take adequate steps to confirm that the parent is who they say they are by asking some identifying questions such as name of student, date of birth of student and ID number of student.

10. A STUDENT IS AT RISK OF SERIOUS AND IMMINENT THREAT TO THEIR HEALTH, SAFETY AND WELFARE. CAN I DISCLOSE THEIR INFORMATION TO PROTECT THEM?

Yes. Under the privacy laws, Monash may disclose personal information in situations where there is a serious and imminent risk to the individual's health, safety or welfare. The Victorian Privacy Commissioner has indicated that a decision relying on this exemption in the privacy laws should be made by a senior officer of the organisation. If you believe that Monash needs to disclose information about a serious and imminent threat to an individual, please contact the Privacy Officer or Solicitor's Office for advice on whether the situation warrants disclosure and for them to obtain the necessary approvals from senior staff of the university.

11. THE VICTORIAN POLICE (OR OTHER LAW ENFORCEMENT AGENCY) HAVE CONTACTED ME REQUESTING INFORMATION ABOUT A STUDENT. AM I OBLIGED TO PROVIDE THE INFORMATION?

No. Police requests are to be distinguished from police demands to release information pursuant to a search warrant or subpoena. If a law enforcement agency requests information (rather than demanding it) Monash may assist the law enforcement agency in limited circumstances. The laws relating to this area are quite specific and any release of information to law enforcement agencies pursuant to a request must have the Privacy Officers approval. If a law enforcement agency requests information from your area please contact the Privacy Officer or the Manager, Student Administration prior to releasing information to ensure compliance with the laws.

12. CAN I USE A STUDENT'S ID NUMBER FOR GENERAL ADMINISTRATIVE / ORGANISATIONAL PURPOSES?

Yes. The Monash Student ID Number is the authorised identification number utilised by Monash University. As the student ID number is most likely personal information under the privacy laws it must be used in accordance with the privacy principles.

13. CAN I USE A STUDENT'S MEDICARE NUMBER FOR GENERAL ADMINISTRATIVE / ORGANISATIONAL PURPOSES?

No. As a general guideline, the Medicare number cannot be used as an identifying number for administrative or organisational purposes. Identifiers such as Medicare numbers can only be adopted by Monash as our identifier with consent of the individual. Unique identifiers should only be used by Monash for the purpose for which they are collected. For example, the Medicare number may be used by Community Services for the purposes of providing the healthcare service.

14. A STUDENT HAS PHONED FOR INFORMATION ABOUT THEIR ACADEMIC RECORD. I NEED TO CONFIRM THEIR IDENTITY PRIOR TO RELEASING THE INFORMATION OVER THE PHONE. CAN I ASK THEM FOR THEIR TAX FILE NUMBER AS A WAY OF IDENTIFYING THEMSELVES?

No. Under Tax file number laws it is illegal to request an individual to supply a tax file number to confirm identity. Please do not ask the student what their tax file number is to confirm their identity. Large penalties may be imposed for non-compliance.

Before releasing information to the student it is recommended that steps are taken to confirm the identity of the student.

Eg: the following questions are example which could be used to confirm identity:

- Student ID Number
- Home phone number;
- Middle Name;
- Date of Birth; and
- Home address.

It is not necessary to record the details of every disclosure. If details are not recorded a customary practice should be established. This means that if a dispute were to arise about releasing information incorrectly, Monash could demonstrate that security measures have been implemented. For example, to establish that a customary practice exists it is recommended that all staff are trained in security of personal information and all staff ask on every occasion three pieces of identifying information to confirm identity prior to releasing information.

The following is appropriate wording of how to confirm identity:

'Before I release the information, I am required to confirm your identity. Would you mind telling me….'

15. A STUDENT RINGS/EMAILS TO REQUEST THEIR TAX-FILE NUMBER. WHAT SECURITY SHOULD BE IMPLEMENTED BEFORE PROVIDING THE TAX- FILE NUMBER?

Providing students with their tax-file number requires stricter security measures than other personal information. A representative from the Australian Taxation Office (ATO) recommended that all organisations adopt the same security measures as the ATO when releasing tax-file numbers to students. There are two methods available to Monash University.

1. Students attend the office with photo identification. The tax-file number should not be released until a representative from the office has viewed the ID.
2. A request can be made over the phone. The following pieces of information are required to confirm the individual's identity: full name, DOB and last postal address Monash University has in its records. The tax-file number should then be sent via letter to the last postal address only. Please do not send it to another address even if requested by the student. The address will need to be changed in the system by the usual method eg completing a form or logging onto the web before the tax-file number will be sent to another address.

In all instances of releasing the tax-file number it is also recommended that a file note or copy of the letter is added to the students file. If a copy of the letter is added to the student's file please ensure that the tax file number is deleted from the letter as tax file numbers must not be stored on an individual's file.

Alternatively, you may refer them to the Australian Taxation Office who release tax file numbers to individuals in a similar manner to that described above.

Collection and storage of tax file numbers

Collection Of Tax File Numbers

Monash University is authorised to collect Tax File Numbers (TFN's) for tax-related purposes only. The following are examples of authorised TFN collection at Monash University:

- Tax File Number Declaration (for Employment)
- Postgraduate Education Loans Scheme (PELS) Loans Request Form
- Higher Education Contribution Scheme (HECS) Payment Options Declaration
- Bridging for Overseas-Trained Professionals Loan Scheme (BOTPLS)

A person's TFN must not be disclosed to anyone except the Australian Taxation Office.

A TFN must not be used to establish or confirm a person's identity.

When collecting TFN's, a person must be told:

- The legal basis for collection
- That declining to quote a TFN is not an offence; and
- The consequences of not quoting a TFN (eg for employment related purposes tax withheld at the highest marginal rate)

TFN's may be obtained in writing or over the phone.

TFN's provided in writing must be contained on the relevant Declaration forms or on the authorised form designed to collect the TFN (available from Student Administration). Declaration forms are to be forwarded to the Department of Education, Science or Training or the Australian Taxation Office (as required by legislation). It is strongly recommended that the declarations are sent via secure courier or registered post. Any copies of the authorised form which collects TFN's must be securely destroyed as soon as it is entered onto Callista or SAP (eg shredded).

When collecting TFN's via phone, the TFN should be entered directly onto SAP or Callista.

If an individual chooses not to delete their TFN from a document they provide to Monash, then Monash must delete the TFN from the document. In some cases, the TFN will need to be cut out, as blocking does not prohibit legibility.

Storage Of Tax File Number's Collected By Monash

If Monash has accidentally obtained a person's TFN, the procedure described above should be followed.

A TFN supplied in response to a request by Monash should be entered as soon as possible on the Callista or SAP. Under no circumstances should TFN's be retained on student/staff files or otherwise recorded or stored. (TFN's can only be viewed on Callista or SAP by authorised staff).

The copy of the Declaration which is available for Monash to keep must be stored in a secure location, not on the individual file. Examples of secure location are in locked filing cabinets, locked offices or secure storage locations.

Provision Of Tax File Numbers To Individual

A representative from the Australian Taxation Office (ATO) recommended that all organisations adopt the same security measures as the ATO when releasing tax-file numbers to individuals. There are two methods available to Monash University.

1. Students attend the office with photo identification. The tax-file number should not be released until a representative from the office has viewed the ID.
2. A request can be made over the phone. The following pieces of information are required to confirm the individual's identity: full name, DOB and last postal address Monash University has in its records. The tax-file number should then be sent via letter to the last postal address only. Please do not send it to another address even if requested by the student. The address will need to be changed in the system by the usual method eg completing a form or logging onto the web before the tax-file number will be sent to another address.

In all instances of releasing the tax-file number it is also recommended that a file note or copy of the letter is added to the student/staff file. If a copy of the letter is added to the student/staff file please ensure that the tax file number is deleted from the letter as tax file numbers must not be stored on an individual's file.

Alternatively, you may refer them to the Australian Taxation Office who release tax file numbers to individuals in a similar manner to that described above.

CASE STUDIES

Case study 1: Student application forms may need revising

Arising from a recent case of the NSW Administrative Decisions Tribunal, you may wish to consider amending your current application form for students.

A summary of the decision is provided below, with possible consequences for Monash University and suggested recommendations. If you would like to read the full text of the decision please go to http://www.lawlink.nsw.gov.au/pc.nsf/pages/cases. The decision was upheld on appeal. The full text of the appeal is also available from the website above.

DO –v- University of New South Wales [2002] NSWADT 211

Facts: Mr DO applied for admission to a PhD in optometry in the University of New South Wales (UNSW). Mr DO signed a declaration which stated in part that:

> *I authorise the University to obtain official records from any tertiary institution previously attended by me.*

UNSW accepted Mr DO's application and he was also awarded a scholarship. Subsequently, UNSW requested academic transcripts in relation to Mr DO from Adelaide University, the University of Queensland, Macquarie University and the University of Tasmania. His enrolment was cancelled as he did not disclose on his application form admission to the PhD program his previous enrolments at the other universities.

Mr DO complained that his privacy had been breached, as he had never authorised UNSW to obtain information from universities he had not included on the application form.

Decision: The complaint was considered by the NSW Administrative Decisions Tribunal in late 2002 and upheld on appeal in March 2003. The Tribunal found that Mr DO signed the authorisation stating that 'I authorise the University to obtain official records from any tertiary institution previously attended by me. This authorisation is not qualified in any way. It applies to any tertiary institution which Mr DO has attended. It is clear on the face of this document that Mr DO did authorise UNSW to collect information about his previous academic record from other universities. Mr DO cannot subsequently seek to restrict the scope of this authorisation. There is no breach of the privacy laws.

What this means for Monash University:

Currently, application forms at Monash contain the following types of statements:

- Information on this form may be disclosed to the relevant bodies for verification of qualifications

OR

- I acknowledge Monash University reserves the right to seek from other relevant bodies verification of the standing of my claimed qualifications

Based on the results of the above case, if an applicant signed a form with a statement such as those outlined above, Monash University would only have consent to verify qualifications. The second statement is even more restrictive as it only allows us to verify those qualifications included by the applicant on the application form.

Recommendations:

If Monash would like to obtain consent to collect information from any educational institution attended by applicants which extends beyond qualifications eg enrolments, then it is recommended that application forms are amended to include the following sentence:

> *I authorise the University to obtain official student records from any educational institution necessary to make an informed decision about the application or matters that concern the student's enrolment.*

This statement allows Monash to obtain information about students from both tertiary institutions and other educational institutions (eg secondary schools) which may be relevant to the decision about the application or ongoing enrolment.

If employment is also taken into account in determining whether an applicant is suitable for course acceptance (eg MBA) it is also important to obtain consent to verify employment. The following statement could be included on application forms where past or current employment is taken into account when determining an applicant's suitability for a position in a course.

> *I authorise the University to verify my past and current employment for the purpose of making an informed decision about the application or matters that concern the student's enrolment.*

Case Study 2: Reference complainant wins privacy case

A recent case note reported on the website of the Office of the Federal Privacy Commissioner (http://www.privacy.gov.au/act/casenotes/index.html) has highlighted the importance of taking into account the reasonable expectations of individuals before using or disclosing their personal information.

According to the case note, a federal government employee provided the name of a referee in the course of an interview for a position with another federal agency. The referee, who was the complainant's supervisor, disclosed during the course of the conversation that the employee suffered from epilepsy and depression and the length of time on sick leave. The referee also disclosed that the complainant did not cope well under stress. The complainant alleged that failure to be selected for the position was due to the referee disclosing this information.

The Commissioner took the view that the disclosure of the illnesses and sick leave information was in breach of the privacy laws because the individual would not reasonably expect that the referee would disclose medical information.

It was acknowledged that the complainant provided implied consent to disclosure of information relating to skills, work experience and personal attributes relevant to the position, however, the implied consent did not extend to disclosure of medical information.

The disclosure of information relevant to the individual's ability to cope with stress was found to be within the expectations of the individual as stress is a normal human characteristic properly relevant to employment. As a result of the Federal Privacy Commissioners investigation the agency issued an apology to the complainant and paid compensation of $7,000.

In view of this case, the Monash University Privacy Officer recommends that when providing references for employees, Monash staff who are asked to give references, and who are authorised to should:

- Ascertain the factors that are relevant to the position;
- Only disclose information about the job applicant that is within the applicant's reasonable expectations eg. skills, work experience and personal attributes relevant to the position; and
- Do not disclose personal information that the job applicant has requested not be disclosed.

MONASH CONTROLLED ENTITIES

Monash University controls various entities (eg companies) via:

- Ownership of more than 50% of the entity.
- More than 50% of the directors on the board are Monash representatives.

These are referred to as Monash Controlled Entities.

Monash Controlled Entities are required to comply with two pieces of privacy legislation which are:

- Privacy Act 1988 (Cth); and
- Health Records Act 2001 (Vic) (for information about compliance with this legislation, please refer to page 8 and 19 of this manual)

It is important to note that Monash University is not required to comply with the Privacy Act 1988. It is also important to note that the Privacy Act 1988 and the Information Privacy Act 2000 are different pieces of legislation and whilst there are similarities, there are also differences.

THE PRIVACY ACT

Monash University controlled entities are required to comply with the Privacy Act 1988 (Cth).

Compliance with the Privacy Act

Private sector amendments to the Privacy Act took effect from the 21st December 2001. With limited exemptions, private sector bodies and Commonwealth government agencies must comply with the legislation.

The Act contains ten National Privacy Principles (NPP's) which are the central part of the laws.

Relevant Definitions

The Information Privacy Act applies to two types of information:

Personal Information: basically means information or opinion, whether recorded in a material form or not and whether true or not, about an identifiable individual. It also includes information from which the identity of the individual can be reasonably ascertained. Examples: name, address, telephone number, title.

Sensitive Information: racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal record *that is also personal information* or health information about an individual.

Health Information: information or opinion about the health or disability (at any time) of an individual, an individual's expressed wishes about future provision of health services to him or her or a health service provided or to be provided to an individual *that is also personal information.* It also includes other personal information collected to provide a health service (eg name, address) and information about donation of body parts, organs or body substances and genetic information.

Differences between the Privacy Act and the Information Privacy Act

The differences between the Information Privacy Act and the Privacy Act can be summarised as follows. Please note, this is a guide only and should not be relied on as a definitive source in determining obligations under the various privacy laws.

	Privacy Act 1988	**Information Privacy Act 2001**
Applies to	Commonwealth Government Agencies, Private Sector (some exemptions) **Monash Controlled Entities**	Victorian Government Agencies **Monash University**
Definition of Personal Information	'whether recorded in a material form or not'	'that is recorded in any form'
Direct Marketing	Assumed secondary purpose, can market providing it is not reasonable to obtain consent from individual and individual can opt out of receiving future marketing material	Not assumed, must be related to purpose of collection. Individual must opt in eg consent must be obtained prior to marketing to them
Staff Records	Are excluded from the coverage of the act if it is directly related to the employment relationship between a current or former employee. Note:	All staff records are covered by the act.

	the act applies to prospective employees.	
Related Body Corporate	Personal information (excluding sensitive or health information) can be disclosed to related body corporate (eg Monash University	This exemption does not apply. To disclose personal, sensitive or health information to the Monash Controlled entities it must fall within the primary or secondary purpose of collection or Monash should obtain consent from the individual. If Monash University wants to disclose information to the controlled entities it is also recommended that Monash and the Controlled Entity enter a contractual agreement to ensure that the privacy protection is guaranteed.

CONTACTS

If you require further information about privacy at Monash please contact the Privacy Officer:

Privacy Officer
Postal Address:
Human Resources Division
Monash University
Building 2, Level 3
195 Wellington Rd
Clayton
Vic 3800

Telephone: +61 3 9902 9589
Facsimile: +61 3 9902 9591
Email: privacyofficer@adm.monash.edu.au
Website: www.privacy.monash.edu.au

Privacy Contacts

If you require further information about privacy at Monash please contact the Privacy Officer:

Privacy Officer
Postal Address:
Human Resources Division
Monash University
Building 2, Level 3
195 Wellington Rd
Clayton
Vic 3800

Telephone: +61 3 9902 9589
Facsimile: +61 3 9902 9591
Email: **privacyofficer@adm.monash.edu.au**

Privacy Co-ordinators

Name	Faculty / Divisions	Phone
Marina Tseng	Advancement	+61 3 9903 4827
Lucy Wiasak	Centre for Advancement of Learning and Teaching	+61 3 990 34483
Terry Hogan	Client Services	+61 3 990 53017
Adrian Stanners	Faculty of Art and Design	+61 3 990

		32707
Yvonne Joyce	Faculty of Arts	+61 3 990 52108
Judy Duffy	Faculty of Business and Economics	+61 3 990 31411
Sue Plowright	Faculty of Education	+61 3 990 59078
Samantha Lipscombe	Faculty of Engineering	+61 3 990 53418
Sue Gleeson	Faculty of Information Technology	+61 3 990 32512
Kelly Tsagournos	Faculty of Law	+61 3 990 58034
John Gibson	Faculty of Medicine, Nursing and Health Sciences	+61 3 990 53906
Carolyn Fox	Faculty of Pharmacy and Pharmaceutical Sciences	+61 3 990 39622
Steven Scroggie	Faculty of Science	+61 3 990 54609
Andrew Marks	Health Wellbeing and Development	+61 3 990 47019
Janine Reid	Monash College Pty Ltd	+61 3 9905 8490
Brendan De Souza	Monash Sport	+61 3 990 51071
Simon Barrett	Research Grants and Ethics	+61 3 990 20132
Souheir Houssami	Research Grants and Ethics	+61 3 990 52052
Bronwyn Drake	Security Advisory Office	+61 3 990 53134
Cathryn Bunney	Student Administration & Systems	+61 3 990 52574
Julie Burbidge	University Library	+61 3 990 55732

Privacy Commissioners:

Victorian Privacy Commissioner
Telephone: +61 3 8619 8719

Health Services Commissioner
Telephone: +61 3 8601 5200

Email: enquiries@privacy.vic.gov.au
Website: www.privacy.vic.gov.au

Email: hsc@dhs.vic.gov.au
Website: www.health.vic.gov.au/hsc