Approved: 17/12/2014
Review Date: December 2016

Privacy Policy

Contents

1. Purpose

1.1. MSA exists to provide a range of opportunities and services to students at the Clayton campus of Monash University. In order to achieve this, MSA must collect personal information from a range of people (largely, but not solely students at Monash), and for a wide variety of uses.

1.2. The legislative instruments that constrain the use of private information include:

a) Privacy Act 1988 (Commonwealth)
b) Information Privacy Act 2000 (Vic)
c) Health Records Act 2001 (Vic)

1.3. MSA does not engage in the sale or disclosure of private details, it does not run a health service, but at present it has an annual turnover exceeding the eligibility threshold amount ($3 million). This means that it is subject to legislation restricting its collection and use of private information under the Privacy Act 1988 (Commonwealth). MSA is not subject to the Information Privacy Act 2000 (Vic) as this applies to Victorian statutory bodies only.

1.4. Monash University, however, is subject to this legislation and must ensure that the flow of information outside the institution (including to MSA) complies with this.

1.5. Parts of MSA are subject to the Health Records Act 2001 (Vic) as they collect information that falls under the definition of Health Records.

2. Application of this policy

2.1. This policy applies to all aspects of MSA's operations.

2.2. This policy applies to the following persons, collectively referred to in this policy as 'workplace participants':

a) all prospective and current full-time, part-time and casual employees of MSA;
b) all volunteers engaged by MSA;
c) all agents and contractors engaged from time to time by MSA; and
d) all office bearers and members of MSA bodies

3. Definitions

3.1. This policy is based upon definition of "information" as used in the Privacy Act 1988 (Commonwealth).

3.2. **Health information** means:

3.2.1. information or an opinion about:

a) the health or a disability (at any time) of an individual;
b) an individual's expressed wishes about the future provision of health services
c) to him or her;
d) a health service provided, or to be provided, to an individual; that is also personal information;

3.2.2. other personal information collected to provide, or in providing, a health service; or

3.2.3. 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; or

3.2.4. genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual

3.3. **Personal information** means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

3.4. **Sensitive information** means:

3.4.1. information or an opinion about an individual's that is also personal information that is:

a) racial or ethnic origin;
b) political opinions;
c) membership of a political association;
d) religious beliefs or affiliations;
e) philosophical beliefs;
f) membership of a professional or trade association;
g) membership of a trade union;
h) sexual preferences or practices; or
i) criminal record;

3.4.2. health information about an individual; or

3.4.3. genetic information about an individual that is not otherwise health information

3.5. It is noted that documents pertaining to matters such as police checks, grievance resolution and complaints handling are normally seen as sensitive information, Photos, images and financial transaction records may also constitute personal / sensitive information.

4. Policy Statement

4.1. MSA views the Commonwealth Privacy Act (1988) as constituting current best practice for the management of personal and sensitive information, and will ensure internal compliance with it via this privacy policy, regardless of whether or not MSA continues to meet the threshold tests for compulsory compliance. MSA will also comply with the Health Records Act 2001 (Vic) where this applies, and will ensure that relevant departments also have codified procedures for ensuring compliance with this legislation.

4.2. MSA recognises that the needs of its departments may vary, and will allow for more tailored policy and procedures to be developed at a departmental level where necessary, but that all such departmental policies must be in accordance with the legislation and the MSA Privacy Policy and Procedure. Any such departmental policies/procedures must be endorsed by the MSA's Privacy Officer and be included as schedules to the MSA Privacy Policy.

4.3. MSA is committed to ensuring best practice in information management, and will conduct regular internal training sessions to ensure that all staff and student members of the association who may collect, access or use personal or sensitive information are aware of the MSA Privacy Policy and the Australian Privacy Principles (APP).

5. MSA's Commitment to the Australian Privacy Principles

5.1. Collection of personal and sensitive information (APP1, 3 and 5)

5.1.1. MSA will only collect personal information necessary for fulfilling one or more of its purposes, which are listed in clause 3 of the MSA constitution as being:

a) to be the recognised means of communication between students and the academic and administrative authorities of the University;
b) to make representations on behalf of students to the community at large;
c) to publish such student newspapers, magazines and other publications as MSA from time to time may determine;
d) to administer the funds of MSA in accordance with this constitution, whether received from fees collected from students by the University or otherwise;
e) to make recommendations to the appropriate bodies of the University on the allocation of funds to MSA;
f) to use the funds of MSA for payment of any expenses incurred in furthering the purposes of MSA;
g) to co-operate with, and affiliate to other persons and bodies in pursuit of its purposes;
h) to promote the right of all students to a free education;
i) to defend the principles of universal membership and the right of students to an autonomous and self-governing organisation;
j) to otherwise protect, promote and develop the interests and welfare of students;
k) to make representations on matters affecting students to any member or body of the University, and in particular to the Council, the Academic Board, the Vice-Chancellor; and
l) to be an accountable, representative and democratic body for students

5.1.2. MSA operates various departments to meet the aims of its constitution, which are responsible for the day-to-day implementation of programs and assistance to students. MSA may collect personal information when it communicates with individuals, when individuals participate in MSA activities and programs, and when students choose to provide information to MSA. Such collection and subsequent storage may be electronic or hard-copy. MSA will only collect personal information by lawful and fair means and in a manner that is not unreasonably intrusive, as outlined in this policy.

5.1.3. MSA will endeavour to collect personal information about an individual directly from that individual. Where this is not possible or practicable, MSA will notify an individual that their personal details are held by MSA, in accordance with this policy, subject to the exceptions described in legislation.

5.2. Information provided on collection and use of information

5.2.1. MSA will develop a statement to be displayed at all locations where personal information is collected outlining the MSA's compliance with the Australian Privacy Principles (APP), in particular the information contained in section 5 of the APP, and advising individuals of the availability of this more comprehensive policy document for anyone who requests it. This Privacy Policy will also be made available on the MSA website.

5.3. Sensitive information

5.3.1. Departments of MSA may need to collect health or sensitive information about a student in order to fulfil their purposes, such as running a camp, conducting casework, or maintaining a contact list. Such information will only be collected, used and disclosed in accordance with the APPs and all staff and student members of the MSA will be trained on what constitutes sensitive information.

5.4. MSA use and disclosure of private information (APP 6 and 8)

5.4.1. MSA will not trade in personal information. MSA may only disclose an individual's personal information with their consent, or where its disclosure is provided for by law. This includes disclosure of personal information to the University or to an individual's family and friends.

5.4.2. MSA departments are required to codify procedures dealing with situations relevant to their purposes where disclosure with and without explicit consent might be applicable under the APP.

5.4.3. MSA will only use information held about an individual for the purpose stated at the time of collection or the secondary purposes allowed for in legislation. All direct marketing by MSA will be conducted in line with the APP, specifically ensuring that individuals are advised that they may opt not to receive further direct marketing material.

5.4.4. MSA does not anticipate a need to send personal or sensitive information overseas. In such cases where this might be necessary however, information will only be sent out of Australia if MSA has taken reasonable steps to ensure that it will be dealt with in accordance with the APP at its final destination.

5.5. Ensuring the safety of private information (APP 11)

5.5.1. MSA will ensure that personal and sensitive information will be stored systematically and safely to prevent misuse and loss. Information must be stored in secure areas that are only accessible to those authorised to access the information. Information may only be used in MSA by workplace participants authorised to access a particular data set, and such access will only be for approved purposes. Departmental staff or office bearers are responsible for the safe-keeping of information held by their department, and may not grant access to others to view, modify or use that information unless that access is required to fulfil the purposes of their department and is allowable under the APP. Departments must codify the procedures used to ensure data security.

5.6. Ensuring Data Quality, Personal Access, and Anonymity (APP2, 9, 10, 11, 12 and 13)

5.6.1. MSA will ensure that personal information it holds uses or discloses is accurate, complete, and up-to-date for its purposes by developing review schedules for all data sets, and codifying the length of time that personal information will be stored. MSA will retain, archive and destroy records in accordance with organisational policy and legislative requirements.

5.6.2. Individuals may request to see information held about them at any time, subject to any relevant exemptions or limitations in legislation and may inform MSA of corrections that need to be made. MSA will then deal with such corrections in accordance with Australian Privacy Principle 11.

5.6.3. No identifier assigned by a Commonwealth Agency (as defined in the legislation) will be used to identify individuals for the purposes of MSA operations in any MSA data sets (e.g. Medicare numbers). Monash University is a statutory body under State, not Commonwealth legislation, therefore the limitations on use of third party identifiers would not apply to the Monash student ID number.

5.6.4. MSA recognises that in some instances individuals may wish to remain anonymous when dealing with MSA. MSA respects this, but may not be able to offer a complete range of services to individuals who do not provide personal information.

6. Procedure

6.1. Collection of Personal and Sensitive Information (APP 2, 3 and 4)

6.1.1. The collection of personal and sensitive information is subject to a number of provisions.

6.2. Non-intrusive collection of information

6.2.1. Departments should only collect information that is directly relevant to their activity.

6.3. Anonymity

6.3.1. If individuals do not wish to provide personal/ sensitive information to MSA then this will be respected, although MSA will advise them that this could mean that MSA may not be able to assist them effectively. A statement to this effect will be contained in the documentation accompanying all requests for information.

6.4. Receiving third party information

6.4.1. Third party information means information about an individual who is not the person MSA receives the information from. The departments most likely to receive third party information would be:

a) Student rights (casework where it contributes to a student's case)
b) Host Scheme (where students are enrolled by proxy)
c) Short Course Centre (e.g. registration records)

6.4.2. If MSA receives personal information and did not solicit the information, then within a reasonable period after receiving the information, MSA must determine whether or not the entity could have collected the information under Australian Privacy Principle 3 if the entity had solicited the information.

6.4.3. MSA may use or disclose the personal information for the purposes of making the determination under subclause 6.4.2

6.4.4. If MSA determines that it could not have collected the personal information; and the information obtained is not contained in a Commonwealth record; MSA must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.

6.4.5. If subclause 6.4.4 does not apply in relation to the personal information, Australian Privacy Principles 5 to 13 applies in relation to the information as if the entity had collected the information under Australian Privacy Principle 3.

6.4.6. Departments that collect third party information must make reasonable attempts to inform the third parties of this fact, and will codify the procedures used to do this as part of their privacy procedures.

6.5. Information statement

6.5.1. The following information statement must be prominently displayed at points of collection, and/or included on all paper or electronic forms where personal/sensitive information is solicited:

a) The information collected here is for the primary purpose of insert primary purpose. Other purposes of collection include attending to administrative matters; corresponding with you, verifying student/subscriber status, insert secondary purpose, and marketing of MSA activities. If you choose not to complete all the information on this form, MSA [*insert departmental name*] may not be able to help you. You have a right to access personal information that the MSA holds about you, subject to any exemptions in relevant legislation.

b) If you wish to seek access to your personal information or enquire about the handling of your personal information, please contact the MSA Privacy Officer at privacy.msa@monash.edu.au. Further information can also be found at www.msa.monash.edu/privacy

6.5.2. The MSA Privacy Policy will also be made available on the MSA website, along with contact details for the Privacy Officer, and information on the right of an individual to view (and amend) their own information as appropriate and how to achieve this (see below).

6.6. Sensitive Information

6.6.1. All staff and student members of MSA will be trained on what constitutes sensitive information, and this will form part of staff and office-bearer induction packages. Sensitive information kept by departments, divisions and authorised staff and office-bearers must be done so in accord with their departmental and/or organisational privacy procedures.

6.6.2. It is incumbent upon all staff and office-bearers to check with the Privacy Officer should there be any uncertainty regarding the appropriateness of the collection, retention and disclosure of information seen as sensitive. Where information must be collected for an ad hoc purpose, e.g. the running of an event or activity (such as a camp), personal and sensitive information should be destroyed within twelve (12) months of the conclusion of the event or activity unless otherwise authorised by the Privacy Officer.

7. MSA Use and Disclosure of Private Information (APP 6 and 7)

7.1. MSA departments are required to codify procedures dealing with situations relevant to their purposes where disclosure with and without explicit consent might be applicable under the APP.

7.2. Disclosure with consent of individual

7.2.1. Procedure for documenting consent:

a) The Privacy Officer will develop a disclosure form as required for centralised operational requirements, and advise relevant departments should they require more specific forms

b) Written consent is preferable for all requests but verbal consent is acceptable in low level situations such as “do you want me to speak to the lecturer about this for you” (although a written record of whether consent is given needs to be undertaken)

7.3. Disclosure required by law

7.3.1. Procedure to follow if it is believed disclosure might be required by law:

a) If in doubt, firstly speak to Privacy Officer

b) Follow Privacy Officer’s recommendation on whether to disclose or not

c) Document who made the request, what information was provided and in what form, the date of request, where the information was sent, and retain a copy of the authorising instrument

7.4. Marketing purposes

7.4.1. Departmental contact lists are not to be used for general MSA marketing purposes unless this is mentioned at the time of collection

7.4.2. All marketing information must include address, phone number, and electronic contact details of MSA.

7.4.3. All marketing information must have an "opt out" clause as follows:

"You have received this information because MSA believes it may be relevant or of interest to you. If you do not wish to receive further such marketing information from the MSA, please send an e-mail to privacy.msa@ monash.edu.au. This will not affect your personal information held by MSA. For more information visit www.msa.monash.edu/privacy"

7.5. Trans-border information flows

7.6. If MSA needs to send information overseas:

a) The authorised person must firstly contact the host institution and ensure that they have adequate procedures in place, or
b) Obtain written consent (where practicable) to send information overseas from the individuals concerned
c) Keep a full record outlining compliance (e.g. noted on individual's file, or with data set)

8. Ensuring the Safety of Private Information (APP 11)

Information is only to be accessed/used/disclosed for primary (and secondary, where appropriate) purpose/s for which it was collected, as documented at the point of collection.

9. Storage of personal information

9.1. The following procedures apply to the storage of personal information:

a) All departments that keep personal/sensitive information must have a lockable filing cabinet if information is stored in hard copy
b) All filing cabinets are to be locked when not in direct line of sight
c) All offices are to be locked when not occupied or not in direct line of sight
d) All electronic storage data sets to be password protected; either at computer level, or, if computer is accessed by many, at document level
e) Where appropriate and/or following direction from the Privacy Officer, such information is to be transferred to a secure central records repository to ensure that it is not lost or prematurely deleted.

10. Authorised people

10.1. Individuals authorised to access personal and sensitive information is limited to those who have a need to use the information for its primary purpose, as follows:

a) Staff-run departments:
   i. Departmental staff members who have a need to access, collect, or store data
b) Office-bearer departments:
   i. Relevant office-bearer/s only
c) Divisions (e.g. C&S, MAPS):

i. Divisional staff members who have a need to access, collect, or store data, and the President of the divisional executive committee (or a member of the divisional executive committee as nominated by the President).

d) Central initiatives (e.g. subscriber database)
   i. Staff member appointed from most relevant area, relevant manager and MSA President

10.2. The MSA Privacy Officer may search all data for the purposes of identifying whether data is held by a student in accordance with a student's desire to access their own data

10.3. The MSA President has automatic access to personal information stored in central records.

10.4. The MSA President has access to personal information stored by both office-bearer and staff-run departments where a demonstrated need has been provided to the MSA Privacy Officer and/or MSA Executive to do so. The Senior Managers have automatic access to personal information in the areas that fall under their brief.

11. Ensuring Data Quality, Personal Access, and Anonymity (APP 2, 9, 10, 11, 12 and 13)

11.1. Data review

11.1.1. All data sets containing personal and sensitive information will be updated annually in January unless otherwise endorsed by this policy.

11.1.2. Data is to be stored in line with standard archival requirements as outlined in relevant Commonwealth and State legislation and MSA policies. This includes the following provisions:
   a) Contact lists may be stored for one (1) year, but may be renewed after one (1) year
   b) Information relating to a specific program or activity may be stored for 1 year
   c) Student case files may be stored for seven (7) years
   d) Petitions (MSA internal) may be stored for seven (7) years

11.2. Personal information collected prior to Policy and Procedure effect

11.2.1. Where personal data was collected prior to this policy and procedure being formally approved, MSA is required to take reasonable steps to ensure that the individuals concerned are aware that the MSA holds such information.

11.2.2. To this end the information shall be flagged at the first review period and:
   a) The individuals concerned shall be notified immediately following the first review period that their personal details are held; or
   b) The individuals concerned shall be notified when next communicated with in the ordinary course of activities;
   c) depending upon the nature of the information held, and in consultation with the Privacy Officer

11.3. De-identification and destruction of records

11.3.1. When the required retention period for records has expired, the following actions need to be undertaken:
   a) Paper records identifying individuals personally must be shredded or similarly destroyed, or comprehensively de-identified (sections cut or deleted)
   b) Electronic records must be deleted in accordance MSA IT guidelines to ensure the irreversibility of the deletion.
   c) E-mails may constitute records of personal or sensitive information, and must be treated according to these principles.

11.4. Requests about personal information

11.4.1. Individuals may request to see information held about them at any time, subject to the relevant exemptions or limitations in legislation. Individuals should enquire to the authorised person (as defined under 10.1) at the relevant department that holds their personal information (if this is known) or apply to the Privacy Officer to determine which data sets contain their personal information.

11.4.2. When a request is made by an individual to view their personal information, the authorised person must make sure, subject to 11.4.3, that there are no restrictions on them accessing personal information

11.4.3. Access might be restricted if, for example:

a) in the case of personal information (other than health information) where providing access would pose a serious and imminent threat to the life or health of any individual; or
b) providing access would have an unreasonable impact upon the privacy of other individuals; or
c) the request for access is frivolous or vexatious; or
d) the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings; or
e) denying access is required or authorised under law

11.4.4. Further exceptions are listed in APP 12.3 and need to be considered when dealing with such requests.

11.5. Requests to amend personal data

11.5.1. If an individual wishes to amend any personal or sensitive information s/he may inform the relevant authorised person of the corrections that need to be made. MSA will then deal with such corrections in accordance with Australian Privacy Principle 13, with the authorised person to make a prima facie determination as whether the request is reasonable. Situations where it may not be reasonable to amend data include:

a) where personal information includes an opinion about a student but the staff member believes that the opinion is still valid for sound reasons, including as an historical record
b) If the authorised person thinks there is a prima facie case for not amending the data they should speak to the Privacy Officer, who will then make the determination in consultation with the departmental authorised person.
c) Where a record is not amended, a record of the individual's request to do so and the reasons for refusal shall be included with the record (where practical).

11.6. Information to individuals

11.6.1. Contact details for the MSA Privacy Officer, and information on an individual's right to view (and amend) their own information and how to achieve this will be made available on the MSA website, along with the MSA Privacy Policy and Procedure.

11.6.2. A generic e-mail alias will be created – likely designated privacy.msa@ monash.edu.au - and linked to the Privacy Officer's email address. The following advice is to be included in relevant documentation provided to students and others as appropriate.

11.6.3. The MSA is committed to being open about the information it holds. Individuals have a right to view information held about them by the MSA, or request that it be corrected/ updated if necessary. This may be done either by:

a) Speaking to staff in the relevant MSA department directly, or
b) Contacting the MSA Privacy Officer if unsure of which department to contact.

11.6.4. There may be situations where MSA reserves the right not to disclose or amend information under law, but you will be advised if this is the case. If you have a complaint in regard to the handling of your personal information, please contact the MSA Privacy Officer at privacy.msa@monash.edu.au.

11.6.5. Complaints regarding MSA's handling of its Privacy Policy should be sent to the Privacy Officer via email on privacy.msa@monash.edu.au or sent to Privacy Officer, C/O MSA, Level 1, 21 Chancellors Walk, Monash University, Clayton.

11.6.6. The Privacy Officer must handle all complaints consistently and equitably. This will involve looking into the complaint, determining the validity of the complaint and responding to the complainant when first received the complaint to acknowledge receipt of complaint and then once a determination is made the outcome of the complaint.

11.7. Identifiers used by the MSA

11.7.1. MSA is allowed to use the Monash student ID number for the purposes of identifying students to the university, as Monash University is a statutory body under State, not Commonwealth legislation.

11.7.2. MSA will not use any Commonwealth markers to identify individuals, such as Tax File or Medicare numbers

12. Specific Data Sets

12.1. Specific data sets need to be dealt with in accordance with the relevant situation.

12.2. Contact lists

12.2.1. Departments may use their own contact lists for their own purposes, including promoting their own events or services, provided that these conform to the MSA Privacy Policy and the Personal Communication and the Use of Technology Policy.

12.3. Petitions

12.3.1. If leaving petitions in a public place for signing, a statement should be placed near the petition to inform petitioners of when the sheet was left, when it will be collected, and when the final recipient will receive the document.

12.4. Personal Case Files / Applications

12.4.1. Relevant departments (e.g. Student Rights, Short Courses,) must have their own procedures, which should be attached as schedules to this policy document. A high level of confidentiality must attach itself to such files given the likelihood of them containing private and sensitive information.

12.5. Club Lists

12.5.1. Relevant departments (e.g. Clubs & Societies) must develop their own procedures for maintaining club lists, which should be attached as schedules to this policy document.

13. Privacy Officer Appointment / Privacy Training

MSA will appoint a Privacy Officer, who shall be responsible for ensuring training and compliance within MSA, maintaining a list of all MSA authorised personnel, and any other duties as required under this policy or legislation. This includes objectively and impartially investigating complaints if a complainant is not satisfied with the initial internal complaints investigation, or with the time that has elapsed since the initial enquiry. The MSA Privacy Officer will normally be a senior full-time staff member.

14. Related Documents

MSA (Clayton) Incorporated Constitution and Regulations
Monash University Privacy Policy and Procedure

15. Legislative References

The legislative instruments that constrain the use of private information include:

- Privacy Act 1988 (Commonwealth)
- Information Privacy Act 2000 (Vic)
- Health Records Act 2001 (Vic)

16. Version History

Current Version

Author: Jennifer Gibson
MSC Approval: *16/2014; 17/12/2014*
Review Date: *December 2016*

Prior Versions

Version 2
Author: Jennifer Gibson
Governance Subcommittee Approval: *18/06/2012*
MSC Approval: *3/2012; 22/06/2012*
Review Date: *June 2014*

Version 1
MSC Approval: 18/12/2009