

ORG002 SOP Privacy and Confidentiality

1. Purpose

To ensure that all Health Information Management Association of Australia Limited (HIMAA) staff members are aware of privacy laws when collecting and disclosing personal information.

2. Scope

This Standard Operating Procedure applies to all staff members of HIMAA.

3. Definition

The Privacy Act 1988 (Privacy Act) and the Privacy Amendment (Enhancing Privacy Protection) Act 2012 regulates how personal information is handled. The Privacy Act defines personal information as:

...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.

Personal information includes information such as:

- *An individual's name or address*
- *Bank account details and credit card information*
- *Photos*
- *Information about your opinions likes and preferences.*

Data Provision Requirements – are the requirements for data provision as agreed by the Industry Skills Council and implemented by the VET Regulator as required by its governing legislation.

Confidentiality – the state of being secret; 'you must respect the confidentiality of your client's communications' concealment, private, secrecy, privacy – the condition of being concealed or hidden

Security – The state of being free from harm or threat.

Legal Action - a judicial proceeding brought by one party against another; one party prosecutes another for a wrong done or for protection of a right or for prevention of a wrong

Disclosure – The action of making new or secret information known.

Australian Privacy Principles (APPs) – the APPs replace the National Privacy Principles for organisations from the 12th March 2014. There are 13 APPs in the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth). The APPs apply to both organisations and agencies. In some cases the APPs can impose specific obligations that apply to only organisations or only to agencies.

Personal Information – 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.

File Name: ORG002 SOP Privacy and Confidentiality	Version: 1.0	Release Date: 28/04/16
Date of Review: 28/04/17	Responsibility: Chief Executive Officer	Page 1 of 20

Sensitive Information – Information or an opinion about an individual’s:

- Racial or ethnic origin
- Political association or opinions
- Religious beliefs or affiliations
- Philosophical beliefs
- Membership of a professional or trade association
- Membership of a trade union
- Sexual preferences or practices
- Criminal record (this can be classed as personal information as well)
- Generic information about an individual that is not health information
- Health information about an individual
- Biometric information that is used for automated biometric verification or biometric identification
- Biometric templates

4. References

- National Vocational Education and Training Regulator Act 2011
- Privacy Act 1988 and the Privacy Amendment (Enhancing Privacy Protection) Act 2012
- Privacy Act 1988 as amended
- Standards for Registered Training Organisations (RTOs) 2015
- RTO010 Policy Unique Student Identifier (USI)
- RTO010 SOP Unique Student Identifier (USI)
- ORG007 Form Confidentiality and non-Disclosure Agreement for Staff
- ORG001 Form HIMAA Copyright Licence for Publications, Presentations, Papers, Abstracts and Publicity
- ORG002 SOP Privacy and Confidentiality
- RTO002 Work Instruction AVETMISS Reporting
- RTO008 Policy Quality Assurance of RTO Operations
- RTO008 SOP Quality Assurance of RTO Operations
- RTO001 Policy Training and Assessment Strategies and Practices
- RTO001 SOP Training and Assessment Strategies and Practices
- RTO011 Policy Providing Accurate and Accessible Information and Advertising and Marketing
- RTO011 SOP Providing Accurate and Accessible Information and Advertising and Marketing

File Name: ORG002 SOP Privacy and Confidentiality	Version: 1.0	Release Date: 28/04/16
Date of Review: 28/04/17	Responsibility: Chief Executive Officer	Page 2 of 20

- RTO013 Policy Complaints and Appeals
- RTO013 SOP Complaints and Appeals
- RTO014 Policy Governance and Administration
- RTO014 SOP Governance and Administration
- RTO015 Policy Cooperating and Communicating with Regulation
- RTO015 SOP Cooperating and Communicating with Regulation
- RTO003 Work Instructions Recording AVETMISS Data
- ORG003 Form Privacy Complaint
- RTO024 Form Consent to Release Information
- RTO005 Form Complaints
- RTO010 Form Access to records Request
- RTO009 Policy Issuing, Maintaining and Acceptance of AQF Certification and Providing Access to Records
- RTO009 SOP Issuing, Maintaining and Acceptance of AQF Certification and Providing Access to Records
- RTO017 Form Change of Personal Details
- RTO018 Form Credential Request
- RTO019 Form Consent from a Learner for HIMAA to APPLY for a Unique Student Identifier (USI)
- RTO024 Form Consent to Release Information
- RTO012 Policy Learners Informed and Protected
- RTO012 SOP Learners Informed and Protected
- Google
- Free Dictionary by Farlex

5. Procedure

5.1 Privacy

The following guidelines are to be used when collecting, storing and releasing data.

- 5.1.1** Only information necessary for HIMAA to conduct its business is to be collected.
- 5.1.2** Information is collected lawfully and fairly and not in an intrusive way.
- 5.1.3** Information is to be collected directly from the individual if possible. If information is to be collected from a third party the individual whose information is being collected must be informed.
- 5.1.4** The individual must explicitly consent to the collection of any personal information.
- 5.1.5** The individual must complete a consent form before HIMAA collects or discloses any sensitive information about them.
- 5.1.6** Sensitive information is personal information about:
 - Racial or ethnic origin
 - Political opinions and associations
 - Religious beliefs

File Name: ORG002 SOP Privacy and Confidentiality	Version: 1.0	Release Date: 28/04/16
Date of Review: 28/04/17	Responsibility: Chief Executive Officer	Page 3 of 20

- Affiliations or philosophical beliefs

5.1.7 Information must be:

- Accurate
- Complete
- Relevant
- Up to date

5.1.8 All information must be kept /stored securely at all times.

5.1.9 HIMAA will enable an individual's access to their own records, unless giving access will infringe on privacy of others or be unlawful.

5.1.10 If the individual disputes the accuracy of the information, notes will be added to the record accordingly.

5.1.11 HIMAA will disclose internal controls, systems and procedures for collecting and managing personal information on individual request.

5.1.12 HIMAA will inform an individual on request of ways in which they can supply personal information anonymously, and any consequences of doing so.

5.1.13 HIMAA uses personal information collected from learners for the following regulatory requirements reports:

- Obtaining and verification of Unique Student Identifiers (USIs) for learners who enrol into our courses
- AVETMISS reporting requirements
- Quality indicator reports
- Course enrolment

5.1.14 HIMAA uses personal information collected from its members for:

- Membership renewal
- Conference information
- Journals
- E-Alerts and newsletters
- Delivery of other membership service entitlement resulting from the payment of membership fees

5.1.15 This information is kept securely and members can ask at any time to unsubscribe to any unwanted information that HIMAA sends by informing the Membership Officer.

5.2 Confidentiality

5.2.1 Confidentiality agreements must be signed by all staff upon commencement of employment with HIMAA. This ensures that staff are under obligation to keep all HIMAA information including documents and client information confidential.

5.2.2 All signed confidentiality agreements are to be filed in the appropriate staff member's human resource file with the Manager of Financial and Corporate Services (MFCS).

5.2.3 HIMAA staff are not to disclose any confidential information to anyone outside the HIMAA organisation or to a HIMAA staff member who is not authorised to know the confidential information.

File Name: ORG002 SOP Privacy and Confidentiality	Version: 1.0	Release Date: 28/04/16
Date of Review: 28/04/17	Responsibility: Chief Executive Officer	Page 4 of 20

- 5.2.4** HIMAA will take disciplinary or legal action against any staff member who has been found disclosing confidential information.
- 5.2.5** Disciplinary action can be in the form of a warning letter on file for minor breaches of confidentiality to instant dismissal and legal action for major breaches.
- 5.2.6** It is at the discretion of the Chief Executive Officer's (CEO) as to what form the disciplinary action will take.

5.3 Australian Privacy Principles

- 5.3.1** HIMAA follows the Australian Privacy Principles when collecting personal information about its Board Members, clients, members, staff, stakeholders and learners.
- 5.3.2** HIMAA would like all Board Members, staff, stakeholders, members and learners to be aware of how HIMAA uses and discloses personal information.
- 5.3.3** This Standard Operating Procedure describes HIMAA practices in collecting personal information regarding course enrolments, membership, staff, Board Members and stakeholder's information.
- 5.3.4** By using HIMAA's services you agree to the terms of this privacy policy and Standard Operating Procedure.
- 5.3.5** HIMAA obtains consent for using personal information on the enrolment form for learners and the membership application and renewal application for members and using RTO024 Form Consent to Release Information.
- 5.3.6** HIMAA is bound by the Privacy Act 1988, the Privacy Amendment (Enhancing Privacy Protection) Act 2012 and the Australian Privacy Principles (APPS).
- 5.3.7** HIMAA will take all precautions to ensure that all personal information is protected and accurate.
- 5.3.8** Information HIMAA collects. HIMAA collects personal information that is needed to provide our services and for business operations. This information can include but not limited to:

5.3.8.1 Learners

1. Name
2. Date of birth
3. Address
4. Phone
5. Email
6. Gender
7. Race
8. Previous qualifications
9. School level
10. Language spoken
11. Employment
12. Disability status
13. Indigenous status
14. Citizenship

File Name: ORG002 SOP Privacy and Confidentiality	Version: 1.0	Release Date: 28/04/16
Date of Review: 28/04/17	Responsibility: Chief Executive Officer	Page 5 of 20

15. Language Literacy and Numeracy levels
16. Credit Card Details (if paying by credit card)

5.3.8.2 Membership Clients

1. Name (minimum)
2. Address (minimum)
3. Phone (minimum)
4. Email (minimum)
5. Date of birth
6. Gender
7. Degree (if applying for full HIM membership)
8. Schooling (if applying for full HIM membership)
9. Overseas member
10. Occupation
11. Credit card details – (Online direct debit)

5.3.8.3 Staff Members

1. Name
2. Address
3. Date of birth
4. Phone
5. Email
6. Bank details
7. Superannuation details
8. Taxation details
9. Next of kin or emergency contact details
10. Medical information e.g. medical certificates etc.

5.3.8.4 Board Members

1. Name
2. Address
3. Phone
4. Email
5. Fit and Proper Persons Declaration (used for supplying the National VET Regulator with information on the high managerial agent)

5.3.8.5 Other Stakeholders

1. Name
2. Address
3. Phone
4. Email
5. Business or organisation name

5.3.9 How HIMAA uses personal information, including purpose, collection and storage.

5.3.9.1 Learners

- 5.3.9.1.1 Learner's personal information is used for the purpose of:
 1. Reporting to the registering and contractual bodies (Australian Vocational Education and Training Management Information Statistical Standard AVETMISS)

File Name: ORG002 SOP Privacy and Confidentiality	Version: 1.0	Release Date: 28/04/16
Date of Review: 28/04/17	Responsibility: Chief Executive Officer	Page 6 of 20

2. Course enrolment in Business Applications
3. Complying with the registering and contractual bodies
4. National Centre for Vocational Education Research (NCVER) reporting requirements Statement of Attainment purposes
5. Enrolment into a HIMAA course. Information is also collected from assessments are submitted for marking, email correspondence and the final examination undertaken by the learner
6. HIMAA ensures that learner's personal information is held securely in Business Applications database which has limited access and is individually password protected only to staff members who have access to the system. Older learners may have a hard copy file but all data is stored in Business Applications for future use such as if a learner needs a reprint of their Statement of Attainment.
7. HIMAA destroys securely all learners' credit card details. These are blacked out then shredded.
8. HIMAA uses Business Applications to store learners' personal information in an electronic format on servers located in Sydney.
9. Business Applications uses the Cloud to store learners' personal information that has been collected by HIMAA. Business Applications servers are located in Sydney (see email response from Business Applications filed in Australian Privacy Principles), though they do have business sites in other countries. These sites do not have access to HIMAA as a client or any of our learners' information.
10. HIMAA has taken reasonable steps to ensure that Business Applications complies with the Australian Privacy Principles when storing learners' personal information. This includes an email requesting information on where Business Applications servers are located and if the country complies with Australian Privacy Principles when dealing with learners and HIMAA clients personal information. As well as having policies and procedures in place for managing learners records and archiving.
11. HIMAA follows the VET Regulators and contractual requirements regarding the length of time that we must hold learner's information, which is 30 years. This information is used to reissue Statements of Attainment (SOA) to learners if the SOA has been lost or stolen. Checks are made to confirm the learners' identity. The learner needs to complete the RTO018 Form Credential Request and submit it to the Student Support and Administration Officer with the applicable fee.
12. HIMAA complies with the VET Act 2011, Privacy Act 1988 and the Privacy Amendment (Enhancing Privacy Protection) Act 2012, Australian Privacy Principles, Standards for NVR Registered Training Organisations 2012, Data Provision Requirements, and the VET

File Name: ORG002 SOP Privacy and Confidentiality		Version: 1.0	Release Date: 28/04/16
Date of Review: 28/04/17	Responsibility: Chief Executive Officer		Page 7 of 20



Quality Framework for the collection and reporting requirements for the Australian Skills Quality Authority (ASQA).

13. All learner information is kept for the required period of time and then destroyed securely by shredding all hard copy documentation. Electronic information is kept on Business Applications and is accessible for the purpose of reprinting Statements of Attainment.

File Name: ORG002 SOP Privacy and Confidentiality		Version: 1.0	Release Date: 28/04/16
Date of Review: 28/04/17	Responsibility: Chief Executive Officer		Page 8 of 20

5.3.9.2 Members Personal Information

- 5.3.9.2.1 HIMAA collects personal information from members by completion of forms such as:
1. Membership registration
 2. Membership renewal
 3. Invoices/remittance advice
 4. Direct debit forms
- 5.3.9.2.2 This information is currently collected by the Membership Officer and is used to create or renew membership for HIMAA. Renewal notices are sent to clients or members and payment taken with the members consent.
- 5.3.9.2.3 HIMAA uses client's information for membership purposes such as:
1. To provide information on membership services to members
 2. Collection of fees
 3. Networking groups and committees
 4. Enrolment in membership activities
 5. Purchase of membership products and services
 6. Gathering of feedback
 7. Membership benefits, rewards and privileges
 8. Organisational governance
- 5.3.9.2.4 HIMAA also uses the information to send to its members regarding but not limited to:
1. Conferences
 2. HIMAA courses
 3. Journals
 4. Industry information
 5. Newsletters
 6. E-Alerts
- 5.3.9.2.5 Existing members can update their information into the database EventsAir. HIMAA members can do this at any time or by contacting the Membership Officer.
- 5.3.9.2.6 For new members they can apply for membership online but the Membership Officer needs to issue a password and login details before they can use the system.
- 5.3.9.2.7 HIMAA ensures that member's personal information is held securely. The database program EventsAir is stored in the cloud and the software is stored only on four computers within the HIMAA office. The Software is guaranteed by Microsoft. The program is also login and password protected for members security.
- 5.3.9.2.8 HIMAA destroys securely all members' credit card details. These are blacked out then shredded.
- 5.3.9.2.9 HIMAA ensures that all members' personal information is protected and only responsible staff have access to the information.

File Name: ORG002 SOP Privacy and Confidentiality		Version: 1.0	Release Date: 28/04/16
Date of Review: 28/04/17	Responsibility: Chief Executive Officer		Page 9 of 20

5.3.9.2.10 All members' documentation is kept for the required period of time and then destroyed securely by shredding.

5.3.9.3 Staff Personal Information

5.3.9.3.1 HIMAA collects personal information from staff by the staff member completing documents such as:

1. Superannuation
2. Tax file number
3. Bank details
4. Employee's personal details
5. Employee's emergency contact details
6. Contract signed by the CEO and staff member

5.3.9.3.2 HIMAA uses the personal information gained from staff members to:

1. Pay superannuation contributions for the staff member
2. Pay the staff member for their work contribution
3. Pay the Australian Taxation Office (ATO) monies on behalf of staff members
4. Contact their next of kin in case of an emergency
5. Ensure that HIMAA can contact the staff member
6. Record the staff members' personal leave entitlements

5.3.9.3.3 Staff are to update their details with the Manager of Financial and Corporate Services (MFCS) if details have changed.

5.3.9.3.4 HIMAA MFCS holds all staff records in secure filing cabinets.

5.3.9.3.5 All staff records are kept for the period required by legislation then destroyed by shredding.

5.3.9.4 Board Members Personal Information

5.3.9.4.1 HIMAA collects Board Member's personal information by the completion of documents such as:

1. Board Member Nomination Form usually completed by another person but can be a self-nomination)
2. Fit and Proper Person Requirements Declaration (ASQA document)
3. Membership registration forms
4. Invoices/remittance advice

5.3.9.4.2 HIMAA uses the personal information gained from Board Members for:

1. Australian Skilled Quality Authority (Fit and Proper Persons) and governance of HIMAA as an RTO
2. Membership purposes
3. Conference and events
4. Committee purposes
5. Journals, newsletters and promotional materials

5.3.9.4.3 Board members' personal information is kept by the MFCS and the Fit and Proper Person's Requirements declaration by the Quality and Compliance Officer. Both are kept in secure locked cabinets.

File Name: ORG002 SOP Privacy and Confidentiality	Version: 1.0	Release Date: 28/04/16
Date of Review: 28/04/17	Responsibility: Chief Executive Officer	Page 10 of 20

5.3.9.4.4 Board Members' personal information is kept for the required period of time then destroyed securely by shredding.

5.3.9.5 Other Stakeholders Personal Information

5.3.9.5.1 HIMAA collects other stakeholders' personal information but not limited to, by the completion of:

1. Conference Registration form
2. Invoices/remittance advice
3. Event registration
4. Membership form
5. Letter/fax/email
6. Business cards
7. Acceptance for presentation and publication of papers or abstract form

5.3.9.5.2 HIMAA uses the personal information gained from stakeholders for:

1. Conference and events
2. Committee purposes
3. Journals, newsletters and promotional materials

5.3.9.5.3 All information that stakeholders provides to HIMAA is protected by the Membership Officer, Marketing and Events Coordinator and MFCS.

5.3.9.5.4 This is protected in locked filing cabinets, databases and on G drive (HIMAA's internal drive) to which only the appropriate staff member has access.

5.3.9.5.5 All stakeholders' information is kept for the required period of time then destroyed securely by shredding.

5.3.10 How information is accessed and updated for Board Members, staff, stakeholders, members and learners

5.3.10.1 HIMAA has a process in place for Board Members, staff, stakeholders, members and learners to be able to access, review, correct or update their information.

5.3.10.2 Board Members, staff, stakeholders, members and learners can request this information by completing a RTO010 Form Access to Records or if information has changed by completing the RTO017 Form Change of Personal Details.

5.3.10.3 All information is updated onto the Business Applications database and on the membership database by the relevant staff member for Board Members, stakeholders, members and learners. For staff it is updated on the personnel file by the staff member informing the MFCS of the change.

5.3.11 Opting out

5.3.11.1 HIMAA's Board Members, staff, stakeholders, members and learners can opt out of receiving HIMAA updates such as:

1. Conferences
2. HIMAA courses

File Name: ORG002 SOP Privacy and Confidentiality	Version: 1.0	Release Date: 28/04/16
Date of Review: 28/04/17	Responsibility: Chief Executive Officer	Page 11 of 20

3. Journals
4. Industry information
5. Newsletters
6. e-Alerts

- 5.3.11.2 This can be done at membership commencement or when membership is to be renewed, by advising on the membership form that they would not like to receive emails or a hard copy of the journal, or by the opt-out link on every eAlert and Newsletter to unsubscribe for the eAlert or Newsletter only. Important information will still be mailed or emailed to the Board Member, staff, stakeholders and learners about HIMAA's upcoming events.
- 5.3.11.3 If at a later stage the Board Members, staff, stakeholders, members and learners wish to opt-out from receiving all updates, journals, industry information, newsletters or e-Alerts they can request in writing to do so by emailing membership@himaa.org.au at any time.
- 5.3.11.4 Doing so will mean the individual will no longer receive some or all of the items in 5.3.11.1
- 5.3.11.5 Board Members, staff, stakeholders, members and learners can also block or delete cookies through their browser settings; however they may not be able to continue to use some websites. In addition this may not be sufficient to block or opt-out of all activities which track the usage of a device or which deliver targeted content. Recent browsers have a "do not track" feature that may be used.

5.3.12 Other important information

- 5.3.12.1 Any information that HIMAA has received from a third party and not a Board Member, staff, stakeholder, member or learner is destroyed. HIMAA does not retain information that the organisation has not collected in the first instance or from a third party.
- 5.3.12.2 Where information has been collected from a third party, HIMAA will take reasonable steps to notify the person concerned about the collection and the disposal of the information as soon as possible after securing the information.
- 5.3.12.3 HIMAA does not disclose personal information without consent. HIMAA has a form to obtain a person's consent to having their details or photo published within the HIMAA Journal or marketing material. HIMAA also has a form to obtain consent for use a person's work including presentations, abstracts and papers at HIMAA conferences and events. HIMAA informs Board Members, staff, stakeholders, members and learners' where and how the information will be used
- 5.3.12.4 When collecting personal information from Board Members, staff, stakeholders, members and learners for cross border disclosure HIMAA ensures that the Board Members, staff, stakeholders, members and learners are aware of why, how and where this information is used as well as

File Name: ORG002 SOP Privacy and Confidentiality		Version: 1.0	Release Date: 28/04/16
Date of Review: 28/04/17	Responsibility: Chief Executive Officer		Page 12 of 20

- ensuring that the recipient of this information follows HIMAA's policy on the Australian Privacy Principles by giving the person access to HIMAA's policy and procedure. By doing this HIMAA ensures that the person has measures of security in place that is equal to those held by HIMAA.
- 5.3.12.5 HIMAA does not disclose government related identifiers. An identifier is a number, letter or symbol or a combination of any or all of these that can be used to identify an individual. An individual cannot consent to the use or disclosure of their government related identifier.
- 5.3.12.6 HIMAA's Board Members, staff, stakeholders, members and learners take reasonable steps to ensure that all personal information that has been collected is current and accurate. HIMAA requests that any change of details for any of its Board Members, members, staff, stakeholders and learners is updated as soon as practicable and that all correspondence is kept either on Business Applications, in the Membership database or on G drive.
- 5.3.12.7 HIMAA secures all collected personal information in the Business Applications database, MYOB, Membership database as well as in secure filing cabinets with limited access.
- 5.3.12.8 HIMAA takes reasonable steps to ensure that personal information collected is accurate, up-to-date, complete and relevant to the use and not misleading. HIMAA Board Members, members, staff, stakeholders and learners can update or correct this information at any time.
- 5.3.12.9 HIMAA updates policies and procedures on at least an annual basis. If changes are made to policies and procedures the Document Management System (DMS) automatically archives the superseded version of the document. All documents are made available through links on the HIMAA website as well as on PDF documents being available to staff members on the G drive.
- 5.3.12.10 When HIMAA collects personal information by a payment service (eWay for online payments) an email stating the amount that it has been paid is sent to Accounts and IT departments. This information does not contain credit card details. For the direct debit system a form is completed by the person who is to be direct debited for Membership. This information is held by the Manager of Financial and Corporate Services in secure filing cabinets. Members are informed prior to the renewal of membership that a fee will be debited from their account.
- 5.3.12.11 HIMAA retains all personal information for the period as required by law, such as Vocational Education and Training (VET) information (30 years).
- 5.3.12.12 HIMAA in some cases must request sensitive information for the purpose of AVETMISS reporting for VET. NCVER generates statistics from this information on age groups, ethnic backgrounds, gender and locality.
- 5.3.12.13 HIMAA notifies Board Members, staff, stakeholders, members and learners the reason for collecting their personal information and where it will be used.

File Name: ORG002 SOP Privacy and Confidentiality		Version: 1.0	Release Date: 28/04/16
Date of Review: 28/04/17	Responsibility: Chief Executive Officer		Page 13 of 20

5.3.13 Complaints

- 5.3.13.1 If any Board Member, staff, stakeholder, member and learner feels that HIMAA has in any way breached the Privacy Act or any other applicable privacy laws they may register a complaint. A complaint can be submitted by completing ORG003 Form Privacy Complaint. An individual can request this form to be emailed to them to complete and submit by email, fax or post to:
Health Information Management Association Australia Limited
Attn: Chief Executive Officer
Locked Bag 2045 North Ryde NSW 1670
Email: ceo@himaa.org.au
Fax: 02 9887 5895
- 5.3.13.2 The RTO013 Policy and Procedure for Complaints and Appeals and the ORG004 Induction Policy and SOP under the heading Personal Grievance will be followed for the process to respond to the complaint. The complainant will be informed of the outcome within the specified timeframe.

5.4 Release of Learners Information

- 5.4.1 HIMAA gathers learners' personal information on the enrolment form including but not limited to:
1. Name
 2. Address
 3. Date of Birth
 4. Contact Details
 5. Ethnicity
 6. Gender
 7. School Level
 8. Previous Qualifications
- 5.4.2 HIMAA informs learners on their enrolment where their personal information is sent and how it is used. This is to meet regulatory reporting requirements e.g. AVETMISS reporting to the National Regulator, Quality Indicator reports.
- 5.4.3 HIMAA collects this information to be compliant with the National VET Regulator.
- 5.4.4 HIMAA will not release information without the consent of the learner. If another Registered Training Organisation requests information about a learner to confirm a credential HIMAA will obtain consent to release the learner's information. This MUST be in writing using RTO024 Form Consent to Release Information.
- 5.4.5 HIMAA will under no circumstances release information without the consent form being submitted to HIMAA.

File Name: ORG002 SOP Privacy and Confidentiality		Version: 1.0	Release Date: 28/04/16
Date of Review: 28/04/17	Responsibility: Chief Executive Officer		Page 14 of 20

5.5 Clean Desk

- 5.5.1** Documents that are left on desks may pose a substantial risk to HIMAA.
- 5.5.2** Desks often display confidential papers to such as:
 - 1. Company reports
 - 2. Strategic plans
 - 3. Tactical plans
 - 4. Project statuses
 - 5. New innovations
 - 6. Privileged information
 - 7. Personal records (learners and members files)
 - 8. Credit card details
- 5.5.3** Unattended documents can pose a real potential threat for inappropriate disclosure.
- 5.5.4** HIMAA requires staff to place in secure filing cabinets any documents they are working on when their office is unattended during office hours and where possible must be securely stored overnight.
- 5.5.5** If a staff member requires documents to be left out after hours their office door must be locked.
- 5.5.6** User IDs and passwords should not be on or around a HIMAA staff member's desk and should be stored securely.

5.6 Records Management

5.6.1 Employee Records

- 5.6.1.1** All employee records contain personal information relating to:
 - 1. The engagement, training, disciplining, resignation or termination of employment
 - 2. Terms and conditions of employment
 - 3. Employees performance or conduct, hours of employment, salary or wages, personal and emergency contact details
 - 4. Employees membership
 - 5. Health
 - 6. Leave such as annual, personal/carers, maternity, paternity or long service
 - 7. Banking details, taxation and superannuation information
 - 8. Contract
 - 9. Qualifications
- 5.6.1.2** If an employee's details change in any way they need to inform the Chief Executive Officer (CEO) and Manager Financial and Corporate Services (MFCS) in writing.
- 5.6.1.3** An employee can have access to their own personal records providing the request meets the legislative requirements including:
 - 1. Time and wages records, including overtime (if applicable) and remuneration
 - 2. Records of leave including leave taken and available leave entitlement

File Name: ORG002 SOP Privacy and Confidentiality	Version: 1.0	Release Date: 28/04/16
Date of Review: 28/04/17	Responsibility: Chief Executive Officer	Page 15 of 20

3. Records of superannuation contributions
4. Workers compensation records (if applicable)
- 5.6.1.4 HIMAA has the right to keep confidential information that is judged sensitive or restricted because it may relate to other employees or comments not meant to be accessed by the employee in question.
- 5.6.1.5 HIMAA will provide a copy of personal financial records as requested by the employee within 7 days of the request being made.
- 5.6.1.6 Financial records will be presented to the employee at the HIMAA office. If the employee cannot attend the HIMAA office due to illness or injury, HIMAA may consider meeting the employee at an agreed meeting place.
- 5.6.1.7 HIMAA's CEO will either approve or deny an employee having access to their employment history record. The CEO will make their decision based on the confidentiality impact on others and the prospect of litigation arising from disclosing particular information. HIMAA will generally but not always grant access to the personal information held by HIMAA regarding the employee.
- 5.6.1.8 All medical information about employees must be kept strictly confidential. Medical information can include but is not limited to drug and alcohol screening.
- 5.6.1.9 Any breach of this policy could expose the company to serious legal liability and any breach of this policy could lead to disciplinary action being taken which can include termination of employment.
- 5.6.1.10 HIMAA's MFCS keeps all personnel and financial records in a locked filing cabinet. Electronic records of employee's time and wages are password protected and only accessed by the MFCS.

5.6.2 HIMAA Membership Records

- 5.6.2.1 The membership database contains information relating to a member:
 1. Home and /or business address
 2. Contact details
 3. Membership history
 4. Financial history relating to membership
 5. Educational history
 6. Professional credentialing information
- 5.6.2.2 HIMAA members can request to be excluded from mail outs of HIMAA advertising material. The database is updated with this information accordingly.
- 5.6.2.3 State branches of HIMAA have access to this information regarding the financial status of members in their state. This information is used for recruitment and retention purposes and to advise members of functions and workshops.
- 5.6.2.4 The CEO has access to statistical information for Board meeting reports. Other staff have access to information which relates to their work or job role.
- 5.6.2.5 HIMAA members have access to copies of receipts, invoices and other personal information that relate to the particular member at no cost.
- 5.6.2.6 HIMAA members can request username and password information which is supplied by Membership Services.

File Name: ORG002 SOP Privacy and Confidentiality	Version: 1.0	Release Date: 28/04/16
Date of Review: 28/04/17	Responsibility: Chief Executive Officer	Page 16 of 20

5.6.2.7 HIMAA Members' administration records are kept in the Membership Services department in lockable cabinets. The file contains membership application, copy of certificate awarded to the member, membership letters and payment information.

5.6.2.8 HIMAA's Membership database is password protected and maintained by Membership Services Department.

5.6.3 Learner Records

5.6.3.1 The Student Management System (SMS) Business Applications (BA) contains personal information relating to learners including:

1. Home and/or business address
2. Contact details
3. Prior learning
4. Course enrolment dates
5. Timetable selection
6. Assessment results
7. Course competency completion date
8. Payment information
9. Cultural background
10. AVETMISS details (see 001 Policy and SOP data provision requirements for details)
11. Issuance of credential

5.6.3.2 The Learning Management System (LMS) contains learner information relating to training and assessment.

5.6.3.3 Electronic versions of learner assessments are uploaded in the SMS/LMS.

5.6.3.4 The Summative Assessment Report is scanned and uploaded into the SMS/LMS.

5.6.3.5 All learners' records prior to the implementation of the SMS/LMS have been archived.

5.6.3.6 HIMAA learners can request photocopies of assessment results, Certificate of Achievement and/or Statement of Attainment at no cost. However, if another original is requested for a credential then RTO018 Form Credential Request must be completed by the learner this incurs a fee. (Please see RTO009 policy and procedure Issuing, Maintaining and Accepting Statements of Attainment and AQF Certification and Access to Records)

5.6.3.7 Learners must under no circumstances be given access to another learner's information.

5.6.3.8 Employers do not have access to specific information about learners who are in their employ or sponsored by their organisation unless written approval has been given by the learner.

5.6.3.9 Assessment information requested by another Registered Training Organisation (RTO) may be confirmed after authorisation of the learner involved and the Quality and Compliance Officer.

5.6.4 Maintenance of Records

File Name: ORG002 SOP Privacy and Confidentiality	Version: 1.0	Release Date: 28/04/16
Date of Review: 28/04/17	Responsibility: Chief Executive Officer	Page 17 of 20

- 5.6.4.1 HIMAA is required to keep personnel records for seven years from date on which an entry has changed or from termination of an whichever occurs first.
- 5.6.4.2 HIMAA's financial records must be maintained for a continuous period of seven years from the date the entry is made.
- 5.6.4.3 HIMAA's learners' records must be maintained for a continuous period of thirty years from the date the entry is made.
- 5.6.5 Disclosure of Employee's Personal Information**
- 5.6.5.1 Personal information concerning employees is confidential and will only be used for purposes for which information is relevant.
- 5.6.5.2 Exceptions may be used for personal information being used for purposes other than for which it was collected. These must have the consent of the person concerned and may include:
1. To prevent a serious threat to a person's health or life
 2. As required or authorised by law
 3. Where reasonably necessary for the enforcement of criminal revenue law.
- 5.6.5.3 When a request is made by a third party, such as a bank seeking information about an employee, the employee will be contacted and their written and signed permission, will be required before any information is released to the third party.
- 5.6.5.4 Theft of Intellectual property (designs and copyrighted material etc) is a serious breach of company policy and the law. This will be treated as a serious matter and depending on particular circumstances may justify dismissal.
- 5.6.6 Mailing Lists**
- 5.6.6.1 Member and learner mailing lists are the intellectual property of HIMAA and are to be protected by internal security arrangements as follows:
1. Under no circumstances are HIMAA lists to be given to any person or organisation except as required by the Board or CEO for internal organisational use e.g. State lists to State committees.
 2. All mailings to these lists will be conducted by HIMAA National Office authorised third parties after execution of a confidentiality agreement.
- 5.6.7 Protection against loss of electronic records**
- 5.6.7.1 Each employee's operational documents and data stored on their computer are backed up on a weekly basis using an automated system.
- 5.6.7.2 After each backup the automated system archives these files to an online, cloud-based repository operated by Amazon Web Services S3.
- 5.6.7.3 In the event of a catastrophic loss of data all files within the online archive are available to ensure the timely restoration of data.
- 5.6.7.4 The financial database (MYOB) is housed on a standalone drive and connected to users through the file server.
- 5.6.7.5 MYOB data is copied daily by the Accounts clerk or MFCS onto a USB memory device which is held securely offsite by the MFCS.

File Name: ORG002 SOP Privacy and Confidentiality	Version: 1.0	Release Date: 28/04/16
Date of Review: 28/04/17	Responsibility: Chief Executive Officer	Page 18 of 20

5.6.7.6 The membership database and financial database (MYOB) are copied onto a disc weekly and held by the Information Technology Support Officer in a secure location outside the office. A log is maintained of back up date and location of the databases.

5.6.7.7 Education Services learner administration and training and assessment records are stored in the Business Application (BA) System and are backed up by BA to three servers in three overseas countries on a continuous basis.

5.6.8 Username and Passwords

5.6.8.1 In the event of an unexpected absence of an employee it is vital that electronic documents can be accessed. This ensures HIMAA's daily operations are maintained.

5.6.8.2 All employees must:

1. Note their user name and passwords plus explanatory notes if appropriate for all systems they use or access. In some cases this is not applicable e.g. when a staff member terminates their employment and the passwords for the sites they use are to be in the new staff member's name.
2. Place the list in a sealed envelope with their name on the front of the envelope and double seal the back with a label bearing their signature and date of signature.
3. Pass the envelope to the CEO for safekeeping.

5.6.8.3 The sealed envelope will only be opened in an emergency by the CEO or his nominated substitute and the employee advised as soon as possible of this action. The employee will then be given the opportunity to change their user name and password and duplicate the process above.

5.6.8.4 In the event of the employee leaving the organisation a staff member nominated by the CEO will remove the employee's username and password access to HIMAA's internal and internet-based Systems.

5.7 Document Storage and Disposal

5.7.1 Storage of Documents

5.7.1.1 All confidential documents that are stored on computers on the G drive are to be password protected.

5.7.1.2 All clients' sensitive personal information such as credit card details are to be stored securely either in locked filing cabinets or if on the computer with password protection.

5.7.1.3 All computers that have sensitive information stored on them are to be password protected. The password is to be written and placed in a sealed envelope and given to the Manager of Financial and Corporate Services. This will be used in the event of an emergency if access to the information is required. If a password is changed the new password must be given to the Manager of Financial and Corporate Services and the old one shredded.

File Name: ORG002 SOP Privacy and Confidentiality	Version: 1.0	Release Date: 28/04/16
Date of Review: 28/04/17	Responsibility: Chief Executive Officer	Page 19 of 20

- 5.7.1.4 All personal information on Business Applications is stored securely and only HIMAA staff who has been provided with the relevant level of access to the system can access the documents and information.

5.8 Disposal of Documents

- 5.7.2.1 All documents stored on your computer that are confidential must only be deleted after permission is granted to do so by the Chief Executive Officer. This ensures documents are not deleted if they are still relevant.
- 5.7.2.2 No policies, procedures, forms etc are to be deleted. The document is saved using the new version number in the file name. This ensures that we have continuous improvement.
- 5.7.2.3 All paper-based documents that are confidential are to be shredded prior to being put in the recycling bin.
- 5.7.2.4 All sensitive or personal information is to be shredded. Personal and sensitive information includes but is not limited to:
1. Name of a person
 2. Signature
 3. Address
 4. Date of birth
 5. Any other identifying information
 6. Credit card details
 7. Gender
 8. Sexual preferences
 9. Ethnic background
- 5.7.2.5 Twice a year a secure bin will be ordered for disposal of large quantities of confidential documents. These documents will be shredded by the company who supplies the bin. Staff are to ensure that they have all the documents that need to be placed in the bin ready for disposal as the bin in only on HIMAA premises for 3-5 days. An email will be sent from the Manager of Financial and Corporate Services to state when the bin will be arriving.

File Name: ORG002 SOP Privacy and Confidentiality	Version: 1.0	Release Date: 28/04/16
Date of Review: 28/04/17	Responsibility: Chief Executive Officer	Page 20 of 20