AIHE
Australian Institute of Healthcare Education

AUSTRALIAN INSTITUTE OF HEALTHCARE EDUCATION

Privacy and Confidentiality Policy

Date	Version	What changes	Approval
July 2016	1.0	Creation of document	CEO

Introduction

It is a requirement that all Students are given sufficient information to make informed decisions for themselves in relation to the course. They are also given information in relation to collection of information and the fact that it remains private and confidential.

Supporting Documents

- Complaints and Appeals Policy
- Student Information Guide v 6.0
- Student Absentee Policy v 3.0
- Course outline AIHE v1
- FAQ Graduate Diploma v3
- AIHE brochure v5
- Privacy Policy

Policy guidelines

1. AIHE expects that students who attend the Graduate Diploma courses will already have received information about the course, including training and assessment, expected hours of work and other areas as required through information as indicated in the Supporting Documents (above).

2. AIHE recognizes the need for students to be able to feel confident that all information is private and kept confidential. This information must be provided to students before commencement of the course in writing. It should also be contained in the Student Information Guide.

The following issues are not considered within the scope of this policy:

- Information about staff
- Academic matters

Confidentiality

In accordance with the institute privacy policy, all parties involved in the grievance procedure will maintain complete confidentiality –unless approval to disclose is granted – and respect for the policy of others.

Privacy Policy

AIHE, including its operation as a Registered Training Organisation, has made it's Privacy Policy clearer to reflect recent changes to Australian Privacy Laws and to ensure we are committed to and compliant with the Australian Privacy Principles (APPs) which came into effect on 12 March 2014.

AIHE complies with the Privacy Act 1988 (Commonwealth) and subsequently in accordance with the thirteen APP's outlined in Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act

2012, which prescribe and mandate the way organisations must collect, manage, use, secure, disclose and dispose of personal and sensitive information.

AIHE is committed to protecting the privacy of client's personal information and we treat any information collected and retained with the respect and importance it deserves. AIHE will be honest and transparent in relation to the way we manage client's information.

Our Privacy Policy explains how we handle clients personal information, including how it is used and potentially disclosed, importantly how it is stored and secured and additionally how clients can access and update clients personal information.

This policy only applies to our databases and files and does not cover any State, Territory or Commonwealth Government database or file. Clients are advised to contact the relevant government agency for a copy of their privacy policy.

Why we collect personal information?

We collect personal information in order to provide the client, with access to our training and associated services, and so we can better understand how we can improve our provision of services now and into the future. Additionally, a large component of what we do as an RTO in particular, requires us to collect personal information for mandatory statistical data as prescribed by government regulators.

AIHE will only collect personal information that is required for the purposes of employment or education, or in meeting government reporting requirements and it will only be used for the specific purposes for which it was collected.

What types of information do we collect in general?

So we can provide our range of services to clients, we may have to collect personal information deemed necessary for us to supply clients with the service clients have requested.

The information we collect is defined under the current legislation as ***personal*** and ***sensitive,*** and information collected by AIHE may fall into both categories. The following specific guidelines as defined in the Privacy Act are as follows:

- *Personal information*: "information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not."
- *Sensitive information*: "(a) information or an opinion about an individual's: (i) racial or ethnic origin, or (ii) political opinions, or (iii) membership of a political association, or (iv) religious beliefs or affiliations, or (v) philosophical beliefs, or (vi) membership of a professional or trade association, or (vii) membership of a trade union, or (viii) sexual preferences or practices, or (ix) criminal record, that is also personal information; or (b) health information about an individual; or (c) genetic information about an individual that is not otherwise health information; or (d) biometric information that is to be used for the purposes of automated biometric verification or biometric identification; or (e) biometric templates".

In general terms, information collected will include:

- Solicited information: contact information such as name, organisation, position, address, telephone, and email, employment and educational histories, referees reports, date of birth and marital status.
- Information collected by AIHE which may be regarded as sensitive:

- ‘Disability’ and ‘long-term impairment status’ (health); and ‘indigenous status’, ‘language spoken at home’, ‘proficiency in spoken English’, ‘country of birth’ (implies ethnic/racial origin). This information is specified in NCVER statistical data elements and is collected for national data reporting requirements.
- ‘Dietary requirements’ (health-related) are collected for event catering purposes only.
- Biographical information, which may contain information on ‘affiliations’ and ‘membership of a professional or trade association’ are obtained from key note speakers for event marketing purposes and for training consultants involved with service delivery for the AIHE.
- ‘Health and work injury information’ relating to the impact for clients self as a client using AIHE services and our ability to provide a service to clients without breaching a Duty of Care.

No sensitive information will be collected without express consent.

What information do we collect using technology?

Our website is designed to give useful information in relation to our services and events. To track the use of our website and to continually develop it to meet client needs, we may collect information about who has accessed our site and which pages were viewed so as to determine overall use patterns. We only use such information collected for statistical purposes and do not attempt to identify individual users.

As part of this we may use 'cookies'. Cookies are used to track information about users of a website. They do not contain any information that could identify clients; they identify client’s computer to our servers. Clients may set clients browser to refuse cookies if clients do not wish to allow their use. Some areas of our website may not perform properly if clients not accept cookies.

How do we collect client’s information?

AIHE will make all endeavours where possible to collect personal information directly from clients. We will collect all personal information in writing in the first instance, either from an employment, registration, personal details or enrolment form that has come directly from clients.
AIHE will also collect personal information through direct marketing on its website via:

- General enquiries contact form

AIHE will not collect any additional personal information other than for the purpose of ensuring we can deliver our services to clients and information will only be collected in a fair and lawful manner. If AIHE receives personal information indirectly (unsolicited) from a party other than clients , AIHE will make a determination on whether the information needs to be retained in order to provide our services to clients as previously explained, or whether the information can lawfully be destroyed or de-identified.

Use and disclosure of personal information

AIHE will make every effort to ensure that client’s personal information remains confidential and secure and is only used for the primary purposes outlined in this document and only for any secondary purposes that clients have been made aware of and have agreed to.

AIHE will not disclose, reveal, sell, share or pass clients information onto a third party, without clients express permission. AIHE does not sell its mailing lists to third parties for marketing purposes.

In some specific instances however, clients information will need to be passed to a third party, these include:

- Australian Skills Quality Authority (ASQA)
- Commonwealth Department of Education
- Department of Immigration and Border Protection
- The National Centre for Vocational Education Research (NCVER)

Only personal information required to comply with Federal or State based legislation for our scope of operation or Commonwealth contractual obligations, will be passed to these third parties and at no time will AIHE disclose any of clients personal information to overseas recipients.

If required to do so, AIHE may disclose personal information to law enforcement authorities when required or authorised under an Australian law or a court/tribunal order, or where it is reasonable to do so if there has been a threat to life or AIHE believes a criminal act or unlawful activity has been committed. AIHE may also disclose information if a permitted health condition exists or a health condition eventuates that may require emergency medical care for clients.

Direct Marketing policy

AIHE does not sell its mailing lists to third parties for marketing purposes and will not use client's information for purposes of direct marketing unless clients have given clients permission for this to occur. AIHE may use client testimonials on its website but they will not identify clients by name unless clients express permission has been given.

AIHE will send out newsletters and corporate event information to existing and previous clients and to businesses aligned with the AIHE. Anybody receiving information from AIHE in error or who does not wish to receive such information, can contact AIHE and request to have their name removed from AIHE mailing lists.

Government related identifiers

AIHE does not adopt or disclose a government related identifier of an individual as its own identifier, unless AIHE is authorised by law and prescribed by regulations to do so.

In the course of our provision of services as an RTO, the AIHE may use a government related identifier, for example, AIHE uses contracted training staff who operate as sole traders and we will collect an Australian Business Number (ABN) for the purpose of contracting services.

AIHE may also need to collect government related identifiers, such as a Medicare Card number, passport details or a driver's licence in order to fulfil our obligations under Federal Law in the conduct of our operations as an RTO.

Management of clients personal information and its 'Quality'

AIHE endeavours to ensure client's personal information is accurate, up to date, complete and relevant. AIHE will as a matter of course, routinely update personal information in our Student Management system.

AIHE invites previous clients to keep their contact details up to date on our website and internal policy prescribes that anytime we contact clients, we will ask if clients personal information is up to date and accurate. We invite clients to contact AIHE at any time to provide us with updated personal information and clients can request access to client's personal information at any time.

AIHE does not charge a fee for accessing or correcting client's personal data.

Retention and disposal of clients information and information security

Client's personal information is held at AIHE in both electronic and paper format. AIHE takes all reasonable steps to protect client's personal information from misuse, loss and from unauthorized access or disclosure.
Specifically client's information is retained:

- In our Student Management System which hosts data externally with a third party and is secured in alignment with Commonwealth standards. The system is encrypted accordingly and secured with personalised user account passwords.
- For a period of time in hard copy archive, secured on site in a locked office.
- Periodically on AIHE's systems and databases which are secured with individual user account passwords and user access privileges.
- On hard copy backup drives which are retained in the event of system failure or loss. All backup copies of these drives are held securely on site.
- AIHE will adopt a clear desk policy at close of business for documents containing personal information.
- Paper documents containing personal information are disposed of in secure waste bins for destruction.

AIHE will retain personal information for as long as we are required to do so to conduct business activities in line with Commonwealth legislation or other legal requirements. This may include the retention of some personal information for up to 30 years.

As soon as client's personal information or components of it are no longer required, and it is lawful to do so, AIHE will take all reasonable steps to destroy and/or de-identify the information.