

## Privacy Policy

---

**Policy Code:** GOV-001      **Version:**      **Effective Date:** 20 March 2017

### Purpose:

The College recognises the importance of privacy and security of personal details of all students, staff, clinic clients and customers. The Privacy Policy indicates the minimum privacy standards for handling personal information, in relation to internal and external practices. The policy aims to protect and provide absolute privacy and quality assurance for all people who are involved with the College.

The College is committed to following the guidelines, requirements and spirit of the Commonwealth [Privacy Act](#) 1988 and the [Australian Privacy Principles](#) as described in the [Privacy Amendment \(Enhancing Privacy Protection\) Act 2012](#).

**Definition of “College”** – *The Australian College of Natural Medicine Pty Ltd (ACNM) trades as Endeavour College of Natural Health, College of Natural Beauty, FIAFitnation and Wellnation. For the purpose of this policy, any reference to ‘College’ or ‘the College’ should be considered a reference to each or any of these respective trading names.*

### Scope:

- All campuses
- All staff
- All students
- All clinic clients
- All governance
- All third parties who may have dealings with the College or a College representative.

# Policy Statement:

## Overview

The College handles personal information in relation to staff, students, clinic clients and customers, hereafter referred to as 'stakeholders'. This policy is an essential measure in delivering superior customer service and ensures appropriate infrastructure is in place to effectively manage privacy requirements.

The College's Privacy Policy seeks to:

- Ensure personal information is collected, stored, and used in accordance with the [Privacy Act](#) 1988
- Acknowledge the responsibility of the College in ensuring that stakeholder information is protected
- Protect the privacy of stakeholders by ensuring that only relevant personal information, which is necessary to provide products and services, is collected
- Ensure that all personal information collected, used or disclosed is accurate, complete and up-to-date
- Obtain consent to collect sensitive information
- Take reasonable steps to make an individual aware of
  - Why we are collecting information about them
  - Who else we might give it to; and
  - Other specified matters.
- Destroy or permanently de-identify personal information if we no longer need it for any purpose for which we may use or disclose information
- Ensure privacy is protected by the use of an 'Opt-In' approach which permits the College to specifically utilise contact information for outlined and appropriate promotional contact. As such, in providing personal information to the College, it is deemed that the individual has 'Opted in' under the College's Privacy Policy. The College also commits to provide the individual with an 'Opt-Out' option at any time
- The College does collect statistical information which cannot be related to any specific individual for continuous improvement purposes and does not provide personal information to external parties for marketing purposes
- The College may be required to provide personal information to designated authorities including the Australian Government as required by law. This may include, but is not limited to sharing information with the Department of

Immigration and Citizenship (DIAC); Department of Education, Employment and Workplace Relations (DEEWR); Australian Council for Private Education and Training (ACPET); the Tuition Assurance Scheme and ESOS Assurance Fund Manager; state and national regulatory bodies including VETAB (NSW), DETE (QLD), TERC (QLD), VRQA (VIC), Board of Studies (NSW), TEQSA and ASQA

- Personal information about international students may be shared with College representatives/agents in order to provide overseas students with services. This information includes personal contact details, course enrolment details and changes and the circumstances of any suspected breach by the student of a student visa condition (National Code 2007, Standard 3.1).

## Terminology

**Personal information** means "personal information" as defined in the [Privacy Act](#). This information may include details such as an individual's name, address, billing information, contact telephone number, email address or photograph.

**Products and services** means any product or service, provided to students, staff or other stakeholders in the normal course of the College's functions and activities.

This can be an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the person performing it to:

- Assess, record and maintain personal contact details for marketing of upcoming courses or events to students, staff and other stakeholders, including and outside service providers
- Develop and continue our relationship with students, staff and other stakeholders, including outside service providers.

**Approved Third Parties** are other Colleges trading under the entity of Australian College of Natural Medicine (Endeavour College of Natural Health, College of Natural Beauty, or FIAFitnation) or any institution with which we have entered into a Memorandum of Understanding (MOU). External service providers (including course facilitators, publishers and printers, government agencies, clinicians, suppliers, legal advisers (e.g. lawyers, investigators) and other similar service providers) are also included in this definition. The College must take reasonable steps to ensure that its approved third parties only handle personal information in accordance with the Australian Privacy Principles.

**Opt-In** means that by providing personal information to the College, the individual recognises the right that they have provided consent for the College to make contact with

them regarding College services.

**Opt-Out** is whereby the College commits to make the option freely available to unsubscribe at any time.

## Breaches of Privacy

All incidents of breach in relation to this policy must be reported to the Privacy Officer in the first instance. If no resolution is reached, details of the alleged breach will be forwarded to the Chief Executive Officer for further action.

## Discipline for Breach of the Privacy Policy

Breach of this policy by College staff (including contract and academic contract staff) will result in disciplinary action, and/or termination of employment.

Breach of this policy by College students will be treated as student misconduct, and investigation and subsequent action will be as per the [Student Misconduct Policy](#). This may result in cancellation of enrolment and exclusion from the College.

## Confidentiality

Unauthorised disclosure of College information, including human resources data, student records, clinic client health information or the misuse of intellectual property belonging to the College, is prohibited and may result in termination of employment (for staff) or exclusion from the College (for students). All records and information referencing personal information must be managed in accordance with the [Records Management Policy](#).

## Australian Privacy Principles (APP)

### Australian Privacy Principle 1 – Open and transparent management of personal information

#### **Kinds of information collected**

All information collected by the College is for the purpose of providing a high quality service to all stakeholders.

The kinds of information collected and held by the College on stakeholders may include:

- Full name
- Date of birth
- Contact details such as residential address, postal address, phone number and email

- Educational background

**For students**, this information may be collected when speaking with a Student Adviser or Admissions Adviser directly, when filling out the enrolment form, or when using the online application form on the College website.

**For staff**, this information may be collected when speaking with a Human Resources Officer directly or when using the online application form on the College website.

**For clinic clients**, this information may be collected when speaking with a clinic student or staff member directly, or when using the online booking form on the College website.

**For customers**, this information may be collected when speaking with a retail staff member directly, or when using the online store.

When enrolling into accredited programs and when gaining employment at the College, the College is obligated to obtain data for government reporting.

Government reporting data includes who participants are, where they study or work and what they study or their role. This includes:

- age, sex and other demographic information
- Indigenous and disability information
- geographic location
- type of provider (for example, government or private)
- location of training delivery
- enrolments in units of competency, as part of a qualification, and modules as part of courses
- how it was studied (for example, classroom, workplace or online)
- how it was funded
- the results obtained for unit/module (outcome)
- role at the College
- educational background relevant to working at the College
- experience relevant to working at the College.

This information is collected only through the means outlined above. Where a stakeholder is unable to complete the relevant form this way, it can be completed over the phone.

Attendance at events or training/education sessions and progress through study is also kept on record.

When collecting personal information, the College will take reasonable steps to inform the individual of the following:

- the identification of the College and its contact details;
- how the individual may obtain access to his or her personal information;
- purposes for which the personal information is collected;
- to whom the personal information will be disclosed;
- Consequences (if any) if the individual does not provide all of their personal information requested.

College stakeholders may be portrayed in photographs, electronic images and video recording of events. Stakeholders may be demonstrating an implied approval of course and events by their presence. Stakeholders shall be asked if they wish to be photographed in such situations, and where events are recorded, a suitable sign shall be prominently displayed at entry to the events indicating that they may be recorded and if appropriate the session/event documentation should indicate that recording may occur.

### Australian Privacy Principle 2 – Anonymity and pseudonymity

The provision of personal information is voluntary, and as such potential and current stakeholders may choose to remain anonymous or use a pseudonym.

The College will provide individuals with the option of not identifying themselves when it is lawful and practicable to do so. For example, searching or enquiring about our courses, gaining background information about the College as an organisation and while exploring the public features of any of the College's websites without making an identity known to us.

The College may not however be able to provide appropriate products or services which a stakeholder customer may request without the required and correct personal information.

### Australian Privacy Principle 3 – Collection of solicited personal information

#### **The College's information collection principles**

- All information collected by the College is for the purpose of providing a high quality service for all College staff, students and clients.
- Only personal information necessary to provide one or more of its services or activities is collected.
- The collection of personal information should be conducted in a lawful and fair

manner (approach taken is open and not misleading), and in a way that is not unreasonably intrusive.

- If it is reasonable and practicable to do so, collect personal information about an individual only from that individual.
- If personal information is collected about an individual from someone else, take reasonable steps to ensure that the individual is or has been made aware of the matters listed in 1 above.
- The College does not actively collect personal information which is "sensitive information" (as defined in the Privacy Act 1988) but may collect sensitive information by consent if it is volunteered.

### **Sensitive information**

The College collects minimal data classified as sensitive information. Sensitive information as relating to health must be collected with the consent of the individual unless it is required by law or unless it is necessary to prevent or lessen a serious and imminent threat to the life or health of that individual.

All sensitive information is collected and stored in compliance with other personal information as it relates to the Australian Privacy Principles.

### **Australian Privacy Principle 4 – Dealing with unsolicited information**

If the College receives personal information and it did not solicit the information, the College will (within a reasonable period after receiving the information) determine whether or not the information could have been collected as outlined under Australian Privacy Principle 3.

Where it is determined that the information gathered could have been obtained through normal solicited means, then the information must be managed as per Australian Privacy Principle 3.

Where the College determines that it could not have collected the personal information (and the information is not contained in a Commonwealth record) the College will, 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.

### **Australian Privacy Principle 5 – Notification of the collection of personal information**

At or before the time or, if that is not practicable, as soon as practicable after, the College collects personal information about an individual, it must take such steps (if any) as are

reasonable in the circumstances to inform the individual of the following:

- The identification of the College and its contact details.
- If the College collects or has collected the personal information from someone other than the individual and the circumstances of that collection.
- If the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order – the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/ tribunal order, that requires or authorises the collection).
- Purposes for which the personal information is collected.
- Consequences (if any) if the individual does not provide all of their personal information requested.
- To whom any personal information will be disclosed.
- How to access this policy to ensure they are aware of their right to access their information, where and how that information is stored, how to complain if a person feels their privacy has been breached and if and to whom their information may go overseas.

## Australian Privacy Principle 6 – Use or disclosure of personal information

The following guidelines apply for use and disclosure of information:

- The 'primary' purpose for collection of data is always made clear.
- Consent for secondary purposes may be obtained at the same time of gathering information for the primary purpose or by future call / contact.

Personal information may be used for secondary purposes, which include direct marketing, follow-up, relationship development and promotion of the College and journal publication.

If the information is used for secondary purposes, the secondary purpose must relate to the primary purpose of collection, and if the personal information is sensitive information, directly relate to the primary purpose of collection; and

- The individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or
- The individual has consented to the use or disclosure; or
- If the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:
  - It is impracticable for the College to seek the individual's consent before



that particular use

- The individual has not made a request to the organisation not to receive direct marketing communications (opt out); and
- The College's procedures and guidelines on direct marketing are complied with.

### Australian Privacy Principle 7 – Direct marketing

As outlined under Privacy Principle 6, the College may use the personal information it gathers to direct market. This secondary use of information is made clear to each individual; the individual would therefore reasonably expect this contact and 'opt out' or unsubscribe opportunities are simple should they wish to opt out of this service at no charge to the individual.

### Australian Privacy Principle 8 – Cross-border disclosure of personal information

The College will only transfer personal information about an individual to someone (other than within the College or the individual) who is in a foreign country if:

- The organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles; or
- The individual consents to the transfer; or
- 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; or
- 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; or
- 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 such consent, the individual would be likely to give it; and
  - The College has taken reasonable steps to ensure that the information, which is transferred, will not be held, used or disclosed by the recipient of the information inconsistently with the Australian Privacy Principles.

## Australian Privacy Principle 9 – Adoption, use or disclosure of government related identifiers

The College does not adopt or disclose any government related identifier of an individual as its own identifier of the individual unless the adoption of the government related identifier is required or authorised by or under an Australian law or a court/tribunal order; if:

- The identifier is prescribed by the regulations; and
- The organisation is prescribed by the regulations, or is included in a class of organisations prescribed by the regulations; and
- The adoption, use or disclosure occurs in the circumstances prescribed by the regulations.

In this Privacy Policy, Identifier includes a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. However, an individual's name or ABN (as defined under Section 30 of the Australian Business Number Act 1999) is not an identifier.

The College does not employ as an identifier for an individual any identifier that has been assigned by:

- An agency; or
- An agent of agency acting in its capacity as agent.

## Australian Privacy Principle 10 – Quality of personal information

The College will take all reasonable steps to ensure that the personal information it collects, uses or discloses is, having regard to the purpose of the use or disclosure, is accurate, up to date and complete.

Procedures undertaken to ensure data quality include:

- Regular training of all relevant stakeholders in use of the online options to update personal information.
- Verification of personal information during contact.
- Audit of any undeliverable email or mail (including relevant contact and updating).

## Australian Privacy Principle 11 – Security of personal information

The College has implemented the following security safeguard and procedures to ensure individuals' personal information are restricted from:

- Misuse
- Loss; or

- Unauthorised access, modification or disclosure.

All data is stored in either secure hard copy format in locked cabinets with limited and registered access, or electronically where access is restricted and password protected.

Security safeguards presently in place include:

- Network access classes defined on a per user basis, with access level based on a 'need to know' basis.
- General ledger access specified.
- Ability to lock-out all users.
- Physical server is offsite in a locked, temperature controlled room.
- Confidential documents are stored nightly in a lockable area.
- Data is archived securely.
- Unique individual passwords for students and staff.

All records must be kept securely and confidential information must be safeguarded. Records must be kept to avoid fire, flood, termites or any other pests and be available when requirement by statutory authorities. A backup of all records must be kept.

All records are retained as per the College's [Records Retention and Disposal Schedule](#) and personal information is destroyed on expiry under that schedule.

## Australian Privacy Principle 12 – Access to personal information

The College understands that open communication with individuals in relation to access to personal information is necessary to gain trust and to build a relationship.

In relation to the College Privacy Policy, giving access means that on request, and if none of the APP exceptions apply, the College must give an individual access to information it holds about the individual that falls within the definition of personal information. This includes information it has collected from third parties and information it has received unsolicited and added to its records.

According to the College [Privacy Policy](#) when individuals request information:

- They are not required to provide a reason
- All official requests for information must be in writing
- An identity check is undertaken
- Information is checked to ensure no information should be withheld (according to the Privacy Act 1988). Where access to certain details is to be withheld, reasons for this decision will be provided to the individual.
- Once the personal information is prepared and cleared for access, the

information can be provided in the form most appropriate to the situation. This will take into account the intention expressed by the individual in his or her original request, and the de-identification of personal information relating to other parties where necessary.

The total time for processing a request for access to information should take no longer than 28 days from the time a request is received.

### Australian Privacy Principle 13 – Correction of personal information (Review and access)

Where the College holds personal information about an individual and finds that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; the College will take reasonable steps to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading.

## Queries

Any Privacy-related queries should be addressed to:

**The Privacy Officer**

Endeavour College of Natural Health

Level 2, 269 Wickham Street,

Fortitude Valley

Queensland, 4006

Email: [privacy@endeavour.edu.au](mailto:privacy@endeavour.edu.au)

## Related Procedures:

Not Applicable

## Further Information:

**Defintions:**

**Student** – is an individual person who is formally enrolled to study at the College. The individual person is that who appears on the College's documents such as enrolment, admission and payment documents, and who is assigned an individual student ID.

**Related Policies:** [Student Misconduct Policy](#)  
[Records Management Policy](#)

**Benchmarking:** AIM QLD & NT

**Supporting Research and Analysis:** Not Applicable

**Related Documents:** [Australian Privacy Principles](#)  
[Records Retention and Disposal Schedule](#)

**Related Legislation:** [Privacy Act 1988](#) (Commonwealth)

<b>Policy Author:</b>	Quality Coordinator
<b>Policy Owner:</b>	Director, Admissions and Marketing
<b>Contact:</b>	Privacy Officer privacy@endeavour.edu.au
<b>Approval Body:</b>	CEO (for ratification by College Council) Approval date: 24 April 2014
<b>Ratifying Body:</b>	College Council Ratification date: TBA
<b>Policy Status:</b>	Revised
<b>Responsibilities for Implementation:</b>	Director, Admissions and Marketing National HR Business Partner
<b>Key Stakeholders:</b>	Director, Admissions and Marketing Director of Education Director, Student Services and Retention National HR Business Partner National Compliance Manager
<b>Date for Next Review:</b>	December 2015

<b>Version History</b>			
<b>Version</b>	<b>Date</b>	<b>Author</b>	<b>Details</b>
0.1	28Oct10	N Chaperon	Draft Document
0.2	25Feb11	N Chaperon	Incorporating feedback; addition of administration details.
1.0	04Mar11	N Chaperon	Approved document Office of CEO
1.1	23Aug11	S Englart	New header including FIAFitnation logo
1.2	20Mar12	D Hoey	Policy Review
1.3	12Oct12	L Sharkey	Compliance Review
2.0	07Dec12		College Council Approved
1.0	23Jun13	C Smalbil	College changed to new version control system within Sharepoint (refer to The Source for further version history).