PRIVACY POLICY

AUSTRALIAN PARAMEDICAL COLLEGE RTO 32513

Purpose

Industry Pathways (ABN 65 153 814 192) operating as Australian Paramedical College (APC) is committed to providing quality services in accordance with the Standards for Registered Training Organisations (2015) and Australian Legislation. Australian Paramedical College is required to comply with Federal law regarding the privacy and confidentiality of all individuals.

The purpose of this policy is to outline and identify APC's commitment to comply with the Privacy Act 1988 and the associated Australian Privacy Principles (APPs). The intent of the policy additionally includes the responsibility of the organisation to report breaches of the Privacy Act as defined by Office of the Australian Information Commissioner (OAIC) and the Notifiable Data Breaches scheme.

Policy Statement

APC is committed to complying with their obligations specifically in the way it collects, uses, stores and discloses personal information.

APC is committed to safeguarding any confidential information obtained by the Registerd Training Organisation (RTO) and will ensure:

a. Maintenance and access to a current Privacy Policy;
b. Information gathered by APC will only be for the purpose of training and assessment matters. Information will not be disclosed to a third party unless prior written consent is provided by the individual concerned, except in the instances where the disclosure of information is required by law;
c. The secure storage of all records and data;
d. The confidentiality of all information maintained on records.

Policy Principles

1.1 Legislation

APC shall abide by the Privacy Act (1988) and the Australian Privacy Principles (APPs) contained in Schedule one of the Act.

The APPs set out standards, rights and obligations for the handling, holding, accessing and collection of personal and sensitive information.

Specifically, APC will operate in accordance with the following:

a. Conduct open and transparent management of personal information inclusive of having a privacy policy.
b. An individual having the option of transacting anonymously or using a pseudonym where practicable.
c. The collection of solicited personal information and receipt of unsolicited personal and sensitive information including giving notice about collection.
d. How personaland sensitive information can be used and disclosed.
e. Maintaining the quality of personal and sensitive information.

f. Keeping personal and sensitive information secure.
g. Right for individuals to access and correct their personal and sensitive information.

1.2 Underpinning Principles

a. **Personal Information** is defined in the Privacy Act 1988 to mean "information or an opinion about an identified individual, or an individual who is reasonably identifiable:
   i. Whether the information or opinion is true or not; and
   ii. Whether the information or opinion is recorded in a material form or not.

b. **Sensitive Information** is defined in the Privacy Act 1988 to mean "information or an opinion about an individual's" that is also personal information, such as:
   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 orientation or practices; or
   ix. Criminal record.

1.3 Consideration of personal and sensitive information and privacy

a. To support the open and transparent management of personal and sensitive information APC will:
   i. Ensure that personal information is managed in an open and transparent way.
   ii. Take reasonable steps to implement practices and procedures that will facilitate dealing with enquiries or complaints from individuals regarding compliance with the APPs.
   iii. Ensure that it maintains an up-to-date policy about the management of personal information.
   iv. Ensure that this Privacy Policy identifies and supports compliance with regard to the following:
      - The kind of information that is collected and held;
      - How the information is collected and held;
      - The purposes for which information is collected, held, used and disclosed;
      - How an individual may access their personal information that is held and seek correction of such information as necessary;
      - How the individual may make a complaint about a breach of the APPs and how APC will deal with such a complaint;
   v. Shall provide the Privacy Policy free of charge and in such form as appropriate, and as reasonable.

b. Anonymity and pseudonymity:
   With regard to anonymity and pseudonymity APC will:
   i. Respect that individuals may not wish to identify themselves when making enquiries for products and services;
   ii. However, require full personal details as required by law and for identification purposes if enrolled.

1.4 Collection of personal and sensitive information

a. APC will not collect personal information unless that information is necessary for one or more of its functions or activities or is required by law.
b. APC will identify and advise that it is required by law to collect, hold, use and supply personal information, in accordance with the National VET Provider Collection Data Provision Requirements.
c. APC will take reasonable steps prior to the time of collection to ensure that you are aware of:
    i. Who we are and how to contact us;
    ii. How to gain access to your own information;
    iii. The purpose for which the information is being collected;
    iv. Any organisation to which we would normally disclose information of that kind;
    v. Any law that requires the particular information to be collected;
    vi. The main consequences for the individual if all or part of the information is not provided.
d. APC collects information in the following ways:
    i. Registration of interest online, application for enrolment, request of certain services or products, or otherwise contact or do business with us.
    ii. Information may be collected from enrolment forms, certified documents, telephone calls, faxes, emails, letters sent by you.
    iii. Information may be collected from third parties, such as other training providers, regarding confirmation of training and ongoing professional development as permitted by staff members and/or students.

Should APC collect information from a third party they will take all reasonable steps to ensure that an individual is or has been made aware of the matters listed above, except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

1.5 Dealing with personal and sensitive information

APC will not use or disclose personal or sensitive information for any purpose other than what it was collected for, unless the relevant person has provided written consent to use or disclose that information in circumstances that are different to those for which it was collected.

a. Exceptions

The circumstances where an exception may occur are:

i. Where the use or disclosure of this information is required or authorised by or under an Australian law or a court/tribunal order;
ii. The individual would reasonably expect to use or disclose the information for the secondary purpose;
iii. A permitted health situation exists in relation to the use or disclosure of the information by APC;
iv. A permitted general situation exists in relation to the use or disclosure of the information by APC;
v. APC reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

b. Collection of student information

APC collects a student's personal information to:

i. Process applications;
ii. Manage your enrolment;
iii. Record and maintain your details;
iv. Administer training programs;
v. Record and maintain details of your ongoing training and assessment;
vi. Provide you with details regarding client services, benefits, and training
vii. opportunities;
viii. Notify you about upcoming events and opportunities;
ix. Gain feedback from you;
x. Communicate with you;
xi. Report to relevant authorities as required by law.

c. Direct Marketing

i. APC may use personal information (specifically name and relevant contact details) and your preferences for direct marketing (ie the communication channels which you prefer for receiving direct marketing from us and the types of products and services in which you are interested in) to let you know about our services and benefits, where we have your consent.
ii. Provides an opt-out and/or unsubscribe method that is easily accessible for individuals to request not to receive direct marketing communications.

d. Adoption, use or disclosure of government related identifiers

i. APC is required by law (Student Identifier Act) to collect, maintain and report to relevant Government agencies the individual's Unique Student Identifier (USI) number in accordance with the National VET Provider Collection Data Provision Requirements.
ii. Will not disclose the Unique Student Identifier (USI) number for any other purpose, including on any Certification documents you receive.
iii. Must not adopt the Unique Student Identifier (USI) number as its own identifier of the individual.

1.6 Integrity of personal and sensitive information

a. With regard to the quality of personal and sensitive information APC will take reasonable steps to ensure that the personal information it collects is accurate, up to date, complete and relevant.
b. With regard to security of personal and sensitive information APC will take reasonable steps to:
   i. Protect the information from misuse, interference and loss as well as unauthorised access, modification or disclosure.
   ii. Destroy the information or ensure that the information is de-identified.

1.7 Access to and collection of personal and sensitive information

a. APC provides all clients with electronic access to their own personal records, where the individual can update and maintain their own personal information.

b. APC will never disclose personal or sensitive information (inclusive of the above or any other information pertaining to the individuals) or assessment results to any 3rd parties without consent.
c. Any requests for personal or sensitive information to be disclosed will need to be approved by the individual.
d. APC at no time will be able to provide students or ex-students with information regarding other student's or ex-students, personal details or assessment results.
e. In the following circumstances, we will not permit access to an individuals personal or sensitive information. These may include
    i. Where giving access to the information would pose a serious threat to the life, health or safety of the individual, or to public health or public safety.
    ii. Giving access would have an unreasonable impact on the privacy of other individuals
    iii. The request for access is frivolous or vexatious
    iv. The information relates to existing or anticipated legal proceedings between and the individual, and would not be accessible by the process of discovery in those proceedings
    v. Giving access would reveal intentions in relation to negotiations with the individual in such a way as to prejudice those negotiations
    vi. Giving access would be unlawful
    vii. Denying access is required or authorised by or under an Australian law or a court/tribunal order; or where the following apply:
        - Reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to functions or activities has been, is being or may be engaged in.
        - Giving access would be likely to prejudice the taking of appropriate action in relation to the maters.
        - Giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body.
        - Giving access would reveal evaluative information generated within in connection with a commercially sensitive decision-making process.
f. When dealing with requests for access to personal or sensitive information, APC will:
    i. Respond to the request for access within 30 days of receival from an individual or an organisation.
    ii. Provide access to the information in the manner requested, if it is reasonable and practicable to do so.
    iii. Shall not charge a fee for access to personal information. The exception to this is reprints of certification documentation previously supplied.
g. With regard to the collection of personal or sensitive information held, APC
    i. where information be inaccurate, out of date, incomplete, irrelevant or misleading, will take such steps as reasonable to correct the information and ensure that updated information is accurate, up-to-date, complete, relevant and not misleading.
    ii. should APC refuse to collect information, will give written notice to the individual that sets out:
        - The reason for refusal
        - The mechanisms available to complain about the refusal; and
        - Any other matter prescribed by the regulations.

Complaints and Breaches of the Privacy Policy

If an individual believes that APC may have breached privacy concerns, they may access the Complaints and Appeals Policy and Procedure available via the APC website or on request.

Where an employee is identified as responsible for a breach of the Privacy Policy and/or complaints are found to be warranted, the following will occur:

a. Employees will be managed internally through the variable consequences as per various APC Policies.
b. Reportable offences can result in serious consequences for the organisation and the Employee. Organisations are required to report breaches as identified by Office of the Australian Information Commissioner (OAIC).

For example, data breach may include, but is not limited to the following incidents:

i. A device containing customers' personal information is lost or stolen
ii. A database containing personal information is hacked
iii. Personal information is mistakenly provided to the wrong person.

APC will address the reportable breaches in accordance with the processes identified by the AOIC and available for information through the following link: Notifiable Data Breaches (AIOC)

Responsibilities

The Managing Directors of APC ensure that all employees are made aware of this policy, its underpinning legislative requirements and consequences. APC supports compliance with this policy at all times.

The Managing Directors ensure that all employees, students and stakeholders have access to and are aware of this policy at all times.

Version	Purpose/amendments	Release date
V1.1_18	Initial implementation	10 Mar 2018
V1.2_18	Review to ensure APP's are in accordance with regulation	02 Nov 2018
V1.3_19	Annual Review & Minor additions (e.g. policy/statement additions)	07 Jan 2019
V1.4_19	Update of policy and minor amendments	03 Dec 2019
V1.5_21	Minor amendment	25 Jan 2021
V1.6_21	Review and minor amendments	08 Nov 2021