PRIVACY POLICY

Section 1 - Purpose and Scope

Purpose

(1) This Policy sets out the College's commitment to protecting the privacy of personal information and health information.

Scope

(2) This Policy applies to:
- (a) all staff;
- (b) all students (including prospective and former students);
- (c) all contractors, consultants and agents of the College when collecting and / or dealing with personal information on behalf of the College.

Section 2 – Definitions

(3) In this Policy:

(a) **Approved third party/ies** means any organisation or individual with which ACPE has entered into a Memorandum of Understanding (MOU) or other formal contractual agreement. External service providers (such as course facilitators, publishers and printers, government agencies, clinicians, suppliers, legal advisers (for example, lawyers, investigators), international education agents and other similar service providers) are included in this definition.

(b) **Australian Privacy Principles (APPs)** means the thirteen (13) principles set out in the *Privacy Act 1988* (Cth), governing standards, rights and obligations around:
- the collection, use and disclosure of personal information;
- an organisation's governance and accountability;
- integrity and correction of personal information; and
- the rights of individuals to access their personal information

(c) **Health information** is a specific type of 'personal information' which may include information about a person's physical or mental health or disability. See section 6 HRIPA for the full definition.

(d) **HRIPA** means the *Health Records and Information Privacy Act 2002 (NSW)*. The Health Privacy Principles (HPPs) are a set of principles in Schedule 1 of HRIPA.

(e) **Eligible data breach** has the meaning given in Part IIIC of the Privacy Act.

(f) **Personal information** is defined in the *Privacy Act 1988* as meaning 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.

See also clause 6 for the types of personal information (also referred to as personal data) that may be collected by the College.

(g) **Privacy breach** means when personal or health information held by the College is lost; or subjected to, or likely to be subjected to, unauthorised access, modification or disclosure.

(h) **Sensitive information** is a type of personal information and defined in the Privacy Act as:

(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 orientation or practices; or
ix. criminal record

(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 purpose of automated biometric verification of biometric identification; or
(e) biometric templates.

Section 3 – Policy Statement

(4) The College will collect, store, provide access to, use and disclose personal and health information in accordance with:

(a) The *Privacy Act 1988* (Cth) (the Privacy Act) and the Australian Privacy Principles in relation to personal information; and
(b) The *Health Records and Information Privacy Act 2002 (NSW*) (HRIPA) in relation to health-related (personal) information where applicable.
(c) The *European Union General Data Protection Regulation 2016* (GDPR) where applicable.

(5) The College, in acknowledging its responsibility to protect people's personal information, seeks to:

(a) Only collect relevant personal information which is necessary to provide products and services.

(b) Ensure that all personal information collected, used or disclosed is accurate, complete and up-to-date.
(c) Obtain individuals' consent prior to collecting sensitive information (unless a statutory exemption applies).
(d) Take reasonable steps to make individuals aware of:
    i. why the College is collecting information about them;
    ii. with whom this information will be shared; and
    iii. other specified matters.
(g) Destroy or permanently de-identify personal information once it is no longer needed.
(h) Ensure individuals are aware of:
    i. The 'Opt-In' approach which permits the College to specifically utilise contact information for outlined and appropriate promotional contact. In providing personal information to the College, it is deemed that the individual has 'Opted in'.
    ii. The Opt-Out option, which the College commits to provide at any time. (Refer to the *Privacy Procedure* for more details about the way ACPE handles personal information in relation to direct marketing activities.)

(6) Personal information that is commonly collected by ACPE may include:
(a) Contact details (that is: name; gender; date of birth; email / postal / street address; social media contact details; telephone numbers (mobile / landline).
(b) Identity and immigration documentation (for example: passport; visa details; driver's licence; identity card)
(c) citizenship;
(d) ethnic origin;
(e) banking and credit card details;
(f) tax file number;
(g) emergency contact details;
(h) photographs or video recordings, including CCTV footage;
(i) student application forms and supporting documentation;
(j) student CHESSN (Commonwealth Higher Education Student Support Number)
(k) and/or USI (Unique Student Identifier) numbers (or their equivalents) associated with Commonwealth HELP loans;
(l) academic records, transcripts, enrolment data and assessment details;
(m) IT and Moodle access logs;
(n) metadata from use of online services and facilities;
(o) records of financial transactions;
(p) social media account details;
(q) information in regard to use of ACPE's website, social media platforms/pages, products and services;
(r) other information collected from students during their studies at ACPE (for example, management of complaints, special consideration requests, counselling referrals etc); and/or

(s) information required for new employees and data that is handled during the the ongoing employment relationship.

ACPE's Responsibilities in the Collection of Personal information (APP 3 and 5)

(7) When ACPE collects personal information, it undertakes to inform the individual why it is required.

(8) ACPE will not collect personal information unless it is reasonably necessary to enable it to undertake its business such as:
- (a) providing services to students/people enquiring about studying at ACPE;
- (b) processing applications for enrolment;
- (c) recruiting staff and generating staff contracts;
- (d) communicating with students, staff and alumni;
- (e) supporting students during their studies at ACPE;
- (f) maintaining appropriate academic and financial records;
- (g) performing other internal administrative functions; and
- (h) providing required data to the Commonwealth or State government departments and professional authorities to comply with ACPE's legal and regulatory obligations.

(9) Before or at the time of collecting personal information (or where that is not practicable, as soon as practicable after its collection), ACPE will take reasonable steps to provide a Privacy Statement to the individual.

(10) Personal information may be collected and held in different forms depending on the reason for the individual's interaction with the College. (See the *Privacy Procedure* for more details.)

Sensitive information

(11) The College collects sensitive information only if the individual has consented to its collection and the information is reasonably necessary to ACPE's business or activities unless ACPE is required to collect such information by Australian law or a court / tribunal order.

Note: ACPE collects minimal personal data classified as sensitive information.

(12) Sensitive information 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.

(13) All sensitive information handled by the College is collected and stored in compliance with other personal information and the Australian Privacy Principles.

Withdrawal of consent

(14) An individual may withdraw their consent for the use of their personal information at any time.

Unsolicited information (APP 4)

(15) The College will handle any unsolicited personal information it has received in line with APP 4. This includes destroying or de-identifying any information it determines it could not have collected.

Anonymity and pseudonymity (APP 2)

(16) The College recognizes there may be circumstances where an individual may wish to remain anonymous or use a pseudonym when accessing or using ACPE services.
   (a) ACPE may not be able to provide all or some of the relevant products, services or other support which an individual has requested or is seeking without the required and correct personal information.

Disclosure of Personal Data (APP 6)

(17) ACPE will take reasonable steps to ensure that personal information is not disclosed to a third party except in certain permitted situations, including:
   (a) Where ACPE has obtained the individual's consent.
   (b) Where disclosure is required or authorised by law or regulatory obligations, such as:
      i. to the Australian Tax Office;
      ii. through PRISMS to the Department of Home Affairs, in relation to immigration and student visa arrangements (including disclosure of suspected breaches of student visa conditions);
      iii. Services Australia;
      iv. disclosing information required by the Higher Education Support Act 2003 (Cth);
      v. for the purpose of administering entitlements to financial assistance (such as FEE-HELP); and
      vi. any other circumstance permitted by the Australian Privacy Principles.
   (c) It is necessary to provide the information to an approved third-party who provides services to or on behalf of ACPE.

(18) Third parties the College works with include:
   (a) education agents (see also clause 19);
   (b) IT companies supporting the ACPE website;
   (c) cloud storage companies;
   (d) customer relationship management application providers;
   (e) other education providers;
   (f) student accommodation providers;

(g) ACPE partners; and
(h) online webinar providers.

(19) The College has specific requirements between itself and contracted education agents in relation to the handling of a person's personal information. The directions and expectations are set out in the contract between the College and the education agent and includes:
(a) providing only the information they need to perform their specific services;
(b) setting out the purpose for which personal information is being shared;
(c) confirmation that they will make every reasonable effort to ensure that the individual's privacy is respected and protected; and
(d) they will inform the College immediately in the event of a suspected or actual breach being detected.

Cross-border disclosure of personal information (APP 8)

(20) The College will only transfer personal information about an individual to someone (other than within ACPE or the individual) who is in a foreign country if:
(a) ACPE 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 APPs; or
(b) the individual expressly consents to the transfer; or
(c) the transfer is necessary for the performance of a contract between the individual and the College, or for the implementation of pre-contractual measures taken in response to the individual's request; or
(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the College and a third party; or
(e) in situations where all the following apply:
i. the transfer is for the benefit of the individual;
ii. it is impracticable to obtain the consent of the individual to that transfer;
iii. if it were practicable to obtain such consent, the individual would be likely to give it; and
iv. ACPE 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.

Adoption, use or disclosure of government related identifiers (APP 9)

(21) The College, in assigning an identifier to individuals for the purpose of uniquely identifying them for its operations, does not adopt any government related identifier of an individual unless the adoption of the identifier is required or authorised by Australian law.

(22) The College will only use or disclose a person's government related identifier in line with the requirements of APP 9.2. This includes ACPE using or disclosing such identifiers for the purpose of fulfilling its obligations to federal government agencies.

Note: Examples of government related identifiers include a person's Medicare number or tax file number.

Quality of personal information (APP 10)

(22) ACPE 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, accurate, up to date and complete.

(23) Procedures undertaken to ensure data quality include:
- (a) regular training of all relevant stakeholders in using the online options to update personal information;
- (b) verification of personal information during contact; and
- (c) audit of undeliverable email or mail (including relevant contacts and updating where applicable).

Holding and securing personal information (APP 11)

(24) ACPE takes reasonable steps to protect personal information from misuse, loss, unauthorised access, modification or disclosure. This includes:
- (a) securing access to all transactional areas of the ACPE website using 'https' technology;
- (b) restricting access to records of personal information;
- (c) securing access to sensitive information via password protection and encryption;
- (d) except where required by law, personal information is securely destroyed or permanently de-identified when no longer required; and
- (e) where personal data is stored digitally, it is located within Australia only, on site and in a secure back-up database off campus.

Access to, and correction of, personal information (APP 12 and 13)

(25) The College will provide individuals, who request it, with access to their personal information.
- (a) Individuals seeking access to their personal information should contact the Registry team (students) or HR (staff) in the first instance. See the *Privacy Procedure* for the process for accessing personal information.

(26) The College reserves the right to withhold access to all or part of the personal information where the disclosure is restricted by law, is the subject of legal action, or may compromise the privacy of another person.

(27) An individual has the right to have their personal information corrected at no charge if there is evidence of any errors.

Note: Students and staff should keep ACPE informed of changes to their personal information, especially in regard to name and contact details.

Eligible Data Breach

(28) In accordance with the Privacy Act, an eligible data breach happens if:
- (a) there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity (that is, the College); and
- (b) the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.

(29) The College must give a notification if it has reasonable grounds to believe that an eligible data breach has happened (or is otherwise directed to do so by the Privacy Commissioner).

(30) The Chief Executive Officer (CEO), with the support of the Compliance Officer and relevant Executive Team member/s, is responsible for responding to eligible data breaches.

Complaints and breaches of Policy

(31) Unauthorised access, use or disclosure of personal information, such as human resources data, student records or health information or the misuse of intellectual property belonging to the College, is prohibited.

(32) Individuals who are concerned about a potential privacy breach, or other breach of this Policy or related procedure are required to contact HR in the first instance.
- (a) If no resolution is reached, details of the alleged breach will be forwarded to the CEO for further action including investigation.
- (b) Breach of this Policy by any staff member may result in disciplinary action, and/or termination of employment.
- (c) Breach of this Policy by students will be treated as student misconduct, and investigation and subsequent action will be in accordance with the *Student Misconduct (Non-Academic) Policy*. This may result in cancellation of enrolment and exclusion from the College.

(33) If the College does not respond to a privacy complaint within 30 days or the individual is not happy with the response, they may lodge a privacy complaint with the Office of the Office of the Australian Information Commissioner:
- https://www.oaic.gov.au
- 1300 363 992 (enquiries only)

(34) Concerns about the handling of health-related personal information may also be referred to the Information and Privacy Commission NSW (https://www.ipc,nsw.gov.au)

Section 4 - Procedures

- Privacy Procedure

Related documents

This Policy should be read in conjunction with but is not limited to:

College policies and procedures:

- Privacy Procedure
- Student Misconduct (Non-Academic) Policy
- Grievances, Complaints and Appeals Policy
- Cookies Statement
- Staff Code of Conduct
- Student Code of Conduct
- ACPE Values

Legislation:

- *Privacy Act 1988* (Cth) and the Australian Privacy Principles (APPs)
- Australian Privacy Principles Guidelines Office of the Australian Information Commissioner (combined December 2022)
- *Health Records and Information Privacy Act 2002* (NSW) (where applicable)
- *European Union General Data Protection Regulation 2016* (where applicable)

Document Administration

Policy Name	Privacy Policy
Policy Owner	CEO
Approval Authority	Board of Directors
Approval Date	29 June 2023
Effective Date	As at Approval Date
Next Review #	Three years from the Approval Date
Amendment history	
Version 3:	V1April 2020: Document developed and implemented. V2 Updated to include College responsibilities about the collection of personal information, Facebook data deletion instructions. V3 April-May 2023: Updated to new template; compliance check with Privacy Act 1988 (Cth) and associated requirements.

 # Unless otherwise indicated, this Policy will still apply beyond the Review date.