Australian College of Nursing

A.3 Privacy Policy

January 2021

This policy encompasses the Australian College of Nursing Ltd (ACN 154 924 642), The College of Nursing (ACN 000 106 829), Royal College of Nursing, Australia (ACN 004 271 103), Australian College of Nursing Foundation (ABN 55 745 393 419) – collectively referred to as the ACN Group.

1. Definitions and Interpretation

1.1 Definitions

In this Policy, unless the context otherwise requires:

a. **ACN** means Australian College of Nursing Ltd (ACN 154 924 642);

b. **APP**s means Australian Privacy Principles, set out in Schedule 1 to the Privacy Act;

c. **Chief Operating Officer** means the chief operating officer of the Company;

d. **Executive Director** means an executive Director of the Company;

e. **GDPR** means the EU General Data Protection Regulation;

f. **Personal Information** has the meaning given to that term by the Privacy Act;

g. **Personnel** means employees, Directors, volunteers and contractors of a Company;

h. **Policy** means this privacy policy;

i. **Privacy Act** means Privacy Act 1988 (Cth);

j. **RCNA** means Royal College of Nursing, Australia (ACN 004 271 103);

k. **Sensitive Information** has the meaning given to that term by the Privacy Act; and

l. **TCON** means The College of Nursing (ACN 000 106 829).

1.2 Interpretation

a. The following companies:

i. ACN;

ii. TCON; and

iii. RCNA,

in their own capacity, and as the trustee of any trusts, are referred to collectively throughout this Policy as the "**ACN Group**".

b. Although this Policy applies to the ACN Group as a whole, any reference to a "**Company**" is a reference to an individual company within the ACN Group, and includes when it acts in a trustee capacity. Similarly, any reference to "**Staff**, a "**Director**", "**Secretary**" or a "**Board**" is a reference to staff, a director, secretary or board of the relevant Company.

c. Any obligation imposed by this Policy on a Director is also taken to be an obligation imposed on a member of any committee of the Board of that Company.

2. Policy

This Policy applies to Personal Information collected and held by the Company. The Policy provides a succinct overview of how the Company collects, stores and disposes of your Personal Information.

3. Purpose

3.1 Purpose

The Policy outlines the Company's legal obligations and ethical expectations in relation to privacy.

3.2 Scope and Application

This Policy applies to the Company as a body corporate and to all of its employees and Directors as individuals.

3.3 Understanding and Commitment

a. The Company recognises the need to be consistent, cautious and thorough in the way that information about interested parties who have provided the Company with Personal Information or data is recorded, stored and managed. As such, the Company and its Directors are committed to protecting the privacy and confidentiality of the interested parties in the way information is collected, stored and used, to ensure that it is done so in an ethical and responsible manner.

b. All individuals, including:

i. interested parties who have provided the Company with Personal Information and data;

ii. Personnel; and

iii. Directors, have legislated rights to privacy of Personal Information. In circumstances where the right to privacy may be overridden by other considerations (for example, child protection concerns), Personnel are to act in accordance with the relevant policy and/or legal framework.

c. All Personnel are to have an appropriate level of understanding about how to meet the Company's legal and ethical obligations to ensure privacy and confidentiality.

3.4 Outcomes

a. The Company provides quality services in which Personal Information is collected, stored, used and disclosed in an appropriate manner that complies with both legislative requirements and ethical obligations.

b. All Personnel understand their privacy and confidentiality responsibilities in relation to Personal Information and organisational information. This understanding is demonstrated in all work practices.

4. Company's Obligations

The Company will:

a. make available to all relevant persons this Policy related to the collection, use, maintenance and disposal of Personal Information;

b. take reasonable steps to ensure that Personal Information that is held is relevant, not excessive, accurate, up to date, complete and that the collection does not unreasonably intrude on the personal affairs of individuals;

c. retain Personal Information for no longer than is necessary and will then dispose of it lawfully and securely;

d. protect Personal Information from loss, unauthorised access, use, modification, disclosure or other misuse;

e. ensure that all reasonable steps are taken to ensure that Personal Information is not used or disclosed without authorisation by external service providers;

f. not apply to any Personal Information an identifier code that has been assigned by any other organisation or agency; and

g. not disclose Personal Information in any other circumstances other than those detailed in this Policy.

5. Legislation

5.1 Privacy Act

The privacy of Personal Information requirements is defined by legislation. At all times, the Company must act in accordance with its legal requirements, which underpin this Policy.

5.2 APPs

The 13 APPs are:

a. APP 1 — open and transparent management of Personal Information;

b. APP 2 — anonymity and pseudonymity;

c. APP 3 — collection of solicited Personal Information;

d. APP 4 — dealing with unsolicited Personal Information;

e. APP 5 — notification of the collection of Personal Information;

f. APP 6 — use or disclosure of Personal Information;

g. APP 7 — direct marketing;

h. APP 8 — cross-border disclosure of Personal Information;

i. APP 9 — adoption, use or disclosure of government related identifiers;

j. APP 10 — quality of Personal Information;

k. APP 11 — security of Personal Information;

l. APP 12 — access to Personal Information; and

m. APP 13 — correction of Personal Information.

5.3 Commitment

Personnel are committed to implementing practices, procedures and systems that will ensure compliance with the APPs.

5.4 EU

If a person is a user of the Company's products and/or services in the European Union, then the Company's processing of that person's Personal Information must be in accordance with the GDPR.

6. Open and Transparent Management of Personal Information (APP 1)

6.1 Availability of Policy

a. The Company makes this Policy and other material available to Personnel and stakeholders to inform them of the Company's policies on management of Personal Information, free of charge.

b. Information on how to access this Policy will be made available to all interested parties. At a minimum, the Company will make this Policy available on its website.

6.2 Details of Personal Information held

Upon request, Personnel will let interested parties who have provided Personal Information/data know, generally, what sort of Personal Information the Company holds, for what purposes, and how the Company collects, holds and discloses that Personal Information.

7. Anonymity and Pseudonymity (APP 2)

7.1 Anonymity and Pseudonymity

Individuals or other interested parties have the right to be dealt with by the Company anonymously or by using a pseudonym, provided that this is lawful and practicable.

7.2 Impracticality

a. It may be impracticable for the Company to deal with parties anonymously when they have provided the Company with information or data.

b. Senior management of the Company will need to decide whether it is likely to be practical or possible to deal with a party anonymously.

8. Collection of Solicited Personal Information (APP 3)

8.1 Details and Consequences of Collection

a. The Company will ensure that each third party providing Personal Information to the Company is informed about and understands the purpose of collecting the Personal Information, to whom and under what circumstances their Personal Information may be disclosed to another party, and how they can access the Personal Information held about them.

b. The Company will ensure that interested parties who have provided information/data, including Personal Information, to the Company, understand the consequences, if any, of providing incomplete or inaccurate information.

8.2 Reason for Collection

a. The Company will only collect Personal Information about an individual from that individual directly, unless it is unreasonable or impractical to do so.

b. The Company will only collect Personal Information for purposes that are reasonably necessary for, or are directly related to, the functions or activities of the Company. These purposes include:

i. responding to enquiries about education courses/ educational services;

ii. events, workshops, and meetings attendance;

iii. administrative activities, including human resources management;

iv. sector development activities;

v. professional development activities;

vi. complaint handling; and

vii. scholarships.

c. When collecting Personal Information, the Company must provide parties who have given the Company that Personal Information with information:

i. the purpose for collecting information;

ii. how the information will be used;

iii. to whom information may be transferred and under what circumstances;

iv. limits to privacy of Personal Information;

v. how a party can access or amend that party's Personal Information; and

vi. how a party can make a complaint about the use of that party's Personal Information.

d. The Company will only collect Sensitive Information from a person:

i. in accordance with **clause 8.2(b)**; and

ii. with the consent of the person,

unless a legal exception otherwise allows that information to be collected.

8.3 Type of Collection

a. The type of information collected by the Company generally includes name, date of birth, address, email address, telephone number, ethnicity, demographics, next of kin, and emergency contact details.

b. Other information collected and held by the Company include job applications, personnel files and referee information. Data collected is considered Personal Information and will only be used for the purpose for which it was collected, or with prior consent from the party from whom the Personal Information was collected, and will be managed in accordance with the APPs.

9. Dealing with Unsolicited Personal Information (APP 4)

9.1 Unsolicited Information

Unsolicited Personal Information is Personal Information received by the Company where the Company has taken no active steps to collect the information.

9.2 Treatment of Unsolicited Information

a. In some instances, the Company may have difficulty deciding whether Personal Information it receives falls within the terms of a Company request and is, therefore, solicited Personal Information. Where it is unclear whether the information is solicited or unsolicited information, the Company will err on the side of caution and treat the Personal Information as unsolicited information.

b. If the Company determines that it could not have lawfully received that unsolicited information, then it shall destroy or de-identify that information as soon as is practicable.

10. Notification of the Collection of Personal Information (APP 5)

a. The Company will take all reasonable steps to ensure parties who have provided the Company with Personal Information:

i. have access to this Policy at or before the time of collection of Personal Information, or as soon as practicable afterwards; and

ii. are informed of the purposes for the collection of the Personal Information, and the ways in which the Company will use that Personal Information.

b. **Clause 10(a)** applies to all Personal Information 'collected' about an individual, either directly from the individual or from a third party.

11. How the Company Collects, Uses and Discloses Personal and Confidential Information (APP 6)

11.1 Purpose of use of Personal Information

a. The Company will ensure that Personal Information will only be used for the purpose for which it was collected, or that would reasonably be expected by the party providing the information.

b. If the identified Personal Information is to be used for a secondary or unrelated purpose, such as data analysis or research, the Company will obtain informed consent from the individual to whom the information relates, unless that individual would reasonably expect that information to be used for another purpose.

c. Parties who have provided the Company with Personal Information will be given the opportunity to refuse such use or disclosure referred to in **clause 11.1(b)**.

11.2 Disclosure to Third Parties

Personal Information may be provided to government agencies, other Companies or individuals if:

a. the party from whom the information was collected has consented;

b. it is required or authorised by law;

c. it will prevent or lessen a serious and imminent threat to somebody's life or health;

d. the disclosure is directly related to the primary purpose for collection;

e. in an emergency situation, where release of information is necessary to aid medical treatment; or

f. the Company is required by law to disclose the information (such as reporting of communicable diseases).

11.3 Confidential Information

a. Information held by the Company other than Personal Information may be regarded as confidential, pertaining either to an individual or the Company. The most important factor to consider when determining whether information is confidential is whether the information should be accessed by the general public.

b. If they are unsure whether information held by the Company is confidential, Personnel are to refer to an Executive Director or the Chief Operating Officer.

c. Personnel will not disclose confidential information about a third party without third party consent/ agreement. The manner in which Personnel manage third party confidential information will be clearly articulated in any contractual agreements that the Company enters into with a third party.

12. Direct Marketing (APP 7)

The Company will only use or disclose Personal Information for direct marketing purposes where the individual has either:

a. consented to their Personal Information being used for direct marketing; or

b. has a reasonable expectation that their Personal Information will be used for this purpose,

and all requirements under the Privacy Act relating to opt-out mechanisms are met.

13. Cross-border Disclosure of Personal Information (APP 8)

13.1 Cross-border Disclosure of Personal Information

The Company will take steps to protect Personal Information if it is sent interstate or outside Australia.

13.2 Requirements for Cross-border Disclosure of Personal Information

Transfer of Personal Information overseas will only occur if the Company is satisfied that the overseas recipient will treat the Personal Information in a manner that is consistent with the Privacy Act.

14. Anonymity, Adoption, Use or Disclosure of Government Related Identifiers (APP 9)

The Company will not use Medicare or Veterans Affairs numbers or other identifiers assigned by a Commonwealth or State Government agency (that is, government-assigned individual identifier number, such as a Medicare number) to identify individuals, unless required to do so by law.

15. Quality of Personal Information (APP 10)

15.1 Accuracy of Personal Information

The Company will take all reasonable steps to ensure that Personal Information kept, used or disclosed by the Company is accurate, complete, and as up to date as practicable.

15.2 Maintaining and Updating Personal Information

These steps include maintaining and updating Personal Information when the Company is advised by individuals that the information has changed (and at other times as necessary), and checking that information provided about an individual by another person is correct.

16. Security of Personal Information (APP 11)

16.1 Security of Personal Information

a. The Company must take all reasonable steps to protect Personal Information collected from misuse or loss. Such steps include computer password access, access restrictions to work areas, office and building security systems, and adequate computer system virus protections and fire wall, and electronic back-up of Personal Information.

b. When the Personal Information that the Company collects is no longer required, it will be destroyed or deleted in a secure manner.

c. The Company may store Personal Information in both hard copy and on computer. The storage, use and where necessary, transfer, of Personal Information will be undertaken in a secure manner that protects third party privacy. Hard copy information is kept under lock and key. Information stored on computer is password protected.

d. The Company's data security policy is as follows:

i. The Company shall maintain an adequate level of security/data protection and privacy for the protection of information supplied by third parties;

ii. The Company shall maintain a commitment to the protection of third party supplied information;

iii. Where there are additional security and privacy requirements as part of contractual agreements, laws and regulations, the strictest requirements shall be implemented;

iv. Directors and the senior executive management team shall set direction for, and show commitment to, security. As a minimum, this Policy shall be applied enterprise-wide and assignment of overall responsibility for information/data security assigned to the Chief Operating Officer;

v. All Personnel and contractors shall be provided with guidance to help them understand the meaning of security, the importance of complying with security policies and their personal responsibilities for security, such as desired security behaviour including reporting witnessed and suspected security incidents;

vi. The Company shall, in a timely manner, report all security incidents to the Board and the relevant key interested parties, including, but not limited to, information or systems used for processing information, including malicious attacks, abuse or misuse of assets;

vii. The Company shall arrange for a security audit and gap analysis review by an externally qualified and competent auditor as required and findings shall be evaluated for possible improvement/corrective actions;

viii. The Company shall have a documented security incident management process – to detect and handle information/data security incidents;

ix. The Company shall have an emergency response process for dealing with serious information security incidents;

x. The Company shall document security incidents, weaknesses or suspicious activities, with reports emailed to the third party nominated representative, and the Company shall deal with these reports in order to ensure that provisions of this Policy concerning security always are complied with, and that the reputation of the person to whom the information relates is not harmed as a result of such events;

xi. The Company shall protect the information supplied by third parties by implementing applicable controls and shall make informed decisions as to if a specific control shall be implemented fully, partly, or not at all, or if alternative protection measures will be implemented. Such decisions shall always include ensuring that security is not compromised; and

xii. Records shall be kept, where possible, showing which information has been accessed, modified, disclosed or disposed.

16.2 Reasonable Physical Safeguards

Reasonable physical safeguards include:

a. locking filing cabinets and unattended storage areas;

b. physically securing the areas in which the Personal Information is stored;

c. not storing Personal Information in public areas; and

d. positioning computer terminals and fax machines so that they cannot be seen or accessed by unauthorised people or members of the public.

16.3 Reasonable Technical Safeguards

Reasonable technical safeguards include:

a. using passwords to restrict computer access and requiring regular changes to passwords;

b. establishing different access levels so that not all staff can view all information;

c. ensuring information is transferred securely (for example, not transmitting Personal Information via non-secure e-mail);

d. using electronic audit trails; and

e. installing virus protections and firewalls.

16.4 Reasonable Administrative Safeguards

Reasonable administrative safeguards include not only the existence of policies and procedures for guidance, but also training to ensure staff and Directors are competent in this area.

17. Access to Personal Information (APP 12)

17.1 Access to Personal Information

Individuals or other interested parties may request access to Personal Information held by the Company, and should contact the relevant person in clause 21 regarding access to and correction of that Personal Information. Access will be provided unless there is a sound reason under the Privacy Act.

17.2 Requests for Access

Requests for access should be made in writing, to the relevant person in clause 21. The Company needs to be satisfied that a request for Personal Information is made by the person to whom the information relates, or by another person who is authorised to make a request on that person's behalf. An identity document will need to be sighted to verify personal identity or, if a person is authorising another person to access on personal medical records on that person's behalf, then a letter of authority and confirmation of personal identity will be required before Personal Information is released.

17.3 Withholding Information

Situations in which access to information may be withheld include:

a. there is a threat to the life or health of an individual;

b. access to information creates an unreasonable impact on the privacy of others;

c. the request is clearly frivolous or vexatious;

d. access to the information has been granted previously;

e. there are existing or anticipated legal dispute resolution proceedings; or

f. denial of access is required by legislation or law enforcement agencies.

17.4 Decision

Where access to information is restricted, the reasons for denying access will be explained to the person requesting it.

17.5 Responses to Requests for Access

The Company will use its best efforts to take fewer than 14 days to respond to a request for access to, or amendment to, information.

18. Correction and Updating of Personal Information (APP 13)

18.1 Amending Personal Information

Where necessary, individuals can also request an amendment to any Personal Information in personal records should they believe that it contains inaccurate information. Such requests should be made in writing.

18.2 Decision

a. If the Company does not agree to change Personal Information in accordance with an individual's request, the individual will be notified.

b. Where access to information is restricted, the reasons for denying access will be explained to the person requesting it. The individual's request will be kept with that individual's personal records.

19. GDPR

Under the GDPR, in addition to any other right third parties have under this Policy, they have a right to:

a. request an explanation of the Personal Information that the Company has about them and how it uses that Personal Information;

b. request the deletion of their Personal Information under certain circumstances;

c. object to the Company's processing of its Personal Information, including for marketing purposes based on profiling and/or automated decision making; and

d. request a copy of the Personal Information the Company has collected about them, and access it in a structured, commonly used and machine readable format for the purposes of transferring it to another party.

19.2 Grounds for processing

a. In accordance with the GDPR, the Company processes Personal Information on the following legal grounds:

i. the processing of personal information is necessary for the performance of the Company's contract with third parties for the provision of goods and services;

ii. the processing is necessary for the Company to comply with its legal obligations including disclosing Personal Information to relevant law enforcement agencies;

iii. the processing is necessary for the Company's legitimate interests. This will include processing for the purpose outlined in this Policy, for direct marketing purposes and to enforce its contract with third parties; and/or

iv. the third party has consented to the processing. The third party may revoke its consent at any time, but if it revokes its consent it may limit the products and services that the Company is able to provide or which the third party is able to access.

b. The Company uses automatic decision making, such as profiling, to make decisions that may have a legal effect on third parties concerning their Personal Information.

20. Privacy Complaints and How the Company would Deal with a Privacy Complaint

20.1 Staff Complaints

If Personnel members are dissatisfied with the conduct of a colleague regarding privacy and confidentiality of information, the matter should be raised with the Personnel member's direct line manager. If this is not possible or appropriate, the Personnel member should follow the delegations indicated in the grievance resolution policy. Personnel members who are deemed to have breached privacy and confidentiality standards set out in this Policy may be subject to disciplinary action up to and including dismissal.

20.2 Third Party Complaints

a. If third parties are dissatisfied with the conduct of a Personnel member, a complaint should be raised in accordance with the compliments, complaints and feedback policy. Information about making a complaint will be made available to third parties who have provided the Company with information/data.

b. Individuals or other third parties should feel free to discuss any concerns, questions or complaints about issues related to the privacy of Personal Information with Personnel.

20.3 Complaint Culture

a. The Company is committed to improving its privacy practices and welcomes any comments or complaints from third parties who have provided Personal Information to the Company. Such feedback helps the Company to identify the things that the Company does well or needs to improve.

b. The Company recognises that, handled well, a complaint provides the Company with an opportunity to strengthen relationships with interested parties who have provided Personal Information to the Company.

c. The Company will respond to personal privacy concerns quickly and in accordance with the Company's complaints management procedure (a copy of which individuals are welcome to sight upon request) and keep individuals informed of actions and progress.

21. How to contact us Privacy Complaints

21.1 Privacy Complaints

Individuals who feel that the Company may have breached their privacy or this Policy, are to contact the Company in writing either by email, fax or letter addressed to:

Company Secretary
PO Box 219
DEAKIN WEST ACT 2600
Fax: 02 6282 3565
Email: company.secretary@acn.edu.au

21.2 General Information

For general information:

Canberra Office

1 Napier Close Deakin ACT 2600 or postal address PO Box 219, Deakin West ACT 2600

Free call 1800 061 660 *call may incur charges,
t 02 6283 3400,
f 02 6282 3565,
e acn@acn.edu.au

Membership - Free call 1800 061 660 *call may incur charges,
e membership@acn.edu.au

Scholarships - Free call 1800 117 262 *call may incur charges,
e scholarships@acn.edu.au

Sydney Office

9 Wentworth St, Parramatta NSW 2150

Free call - 1800 061 660 *call may incur charges,
t 02 6283 3400
f 02 6282 3565
e acn@acn.edu.au

Education - Free call 1800 265 534 *call may incur charges,
e customerservices@acn.edu.au

21.3 Privacy Officer

To contact the privacy officer:

Privacy Officer c/o Company Secretary
PO Box 219
DEAKIN WEST ACT 2600
Fax: 02 6282 3565
Email: company.secretary@acn.edu.au

21.4 External Complaint

a. Under the Privacy Act, individuals can make a complaint to the Office of Australian Information Commissioner (OAIC) about the handling of Personal Information.

b. For details please visit http://www.oaic.gov.au/privacy/privacy-complaints.

22. Review

a. This Policy will be revised from time to time considering any legislative or organisational changes.

b. If you have any queries about this Policy, please contact the Secretary.

23 History

Reviewed by Mills Oakley, October 2020

Responsibility for Review:	**Executive Leadership Team**
Ratification:	**Board**
Date of issue:	**December 2012**
Date last reviewed:	**October 2020**