ANARE CLUB Inc. **Attachment A**

Extract from the Victorian Privacy and Data Protection Act 2014 No. 60 of 2014

Summary *(In Brief)* of relevant parts of listing the Information Privacy Principles (IPPs) Schedules

In these Principles— *sensitive information* means information or an opinion about an individual's—
(a) racial or ethnic origin;
or (b) political opinions;
or (c) membership of a political association;
or (d) religious beliefs or affiliations;
or (e) philosophical beliefs;
or (f) membership of a professional or trade association;
or (g) membership of a trade union;
or (h) sexual preferences or practices;
or (i) criminal record— that is also personal information; unique identifier means an identifier (usually a number) assigned by an organisation to an individual uniquely to identify that individual for the purposes of the operations of the organisation but does not include an identifier that consists only of the individual's name and does not include an identifier within the meaning of the Health Records Act 2001.

Schedule 1—The Information Privacy Principles Privacy and Data Protection Act 2014 No. 60 of 2014

1.Principle 1—Collection

1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.

1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of—

(a) the identity of the organisation and how to contact it; and
(b) the fact that the individual is able to gain access to the information; and
(c) the purposes for which the information is collected; and
(d) to whom (or the types of individuals or organisations to which) the organisation usually discloses information of that kind; and
(e) any law that requires the particular information to be collected; and
(f) the main consequences (if any) for the individual if all or part of the information is not provided.

1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual

1.5 If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in IPP 1.3 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.

2. Principle 2—Use and Disclosure

2.1 An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless—

(a) both of the following apply—
(i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;
(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or
(b) the individual has consented to the use or disclosure; or
(c) if the use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest, other than for publication in a form that identifies any particular individual—

3. Principle 3—Data Quality

3.1 An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up to date

4. Principle 4—Data Security

4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.

5. Principle 5—Openness

5.1 An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.

5.2 On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

6. Principle 6—Access and Correction

6.1 If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that—

(a) providing access would pose a serious threat to the life or health of any individual; or

(b) providing access would have an unreasonable impact on the privacy of other individuals; or

(c) the request for access is frivolous or vexatious; or Sch. 1 cl. 6.1(a) amended by No. 23/2017 s. 22(2). Authorised by the Chief Parliamentary Counsel Schedule 1—The Information Privacy Principles Privacy and Data Protection Act 2014 No. 60 of 2014 138

(d) the information relates to existing legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery or subpoena in those proceedings; or

(e) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(f) providing access would be unlawful; or

(g) denying access is required or authorised by or under law; or

7. Principle 7—Unique Identifiers

7.1 An organisation must not assign unique identifiers to individuals *unless* the assignment of unique identifiers is necessary to enable the organisation to carry out any of its functions efficiently.

7.2 An organisation must not adopt as its own unique identifier of an individual a unique identifier of the individual that has been assigned by another organisation unless—

(a) it is necessary to enable the organisation to carry out any of its functions efficiently; or Authorised by the Chief Parliamentary Counsel Schedule 1—The Information Privacy Principles Privacy and Data Protection Act 2014 No. 60 of 2014 141

(b) it has obtained the consent of the individual to the use of the unique identifier; or

(c) it is an outsourcing organisation adopting the unique identifier created by a contracted service provider in the performance of its obligations to the organisation under a State contract.

7.3 An organisation must not use or disclose a unique identifier assigned to an individual by another organisation unless—

(a) the use or disclosure is necessary for the organisation to fulfil its obligations to the other organisation; or (b) one or more of IPP 2.1(d) to

(g) applies to the use or disclosure; or

(c) it has obtained the consent of the individual to the use or disclosure.

7.4 An organisation must not require an individual to provide a unique identifier in order to obtain a service unless the provision of the unique identifier is required or authorised by law, or the provision is in connection with the purpose (or a directly related purpose) for which the unique identifier was assigned.

8. Principle 8—Anonymity

8.1 Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering into transactions with an organisation.

9. Principle 9—Transborder Data Flows

9.1 An organisation may transfer personal information about an individual to someone (other than the organisation or the individual) who is outside Victoria only if— Authorised by the Chief Parliamentary Counsel Schedule 1—The Information Privacy Principles Privacy and Data Protection Act 2014 No. 60 of 2014 142

(a) 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 Information Privacy Principles; or
(b) the individual consents to the transfer; or
(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of precontractual 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 organisation and a third party; or
(e) all of 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 that consent, the individual would be likely to give it; or
(f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Information Privacy Principles. Authorised by the Chief Parliamentary Counsel Schedule 1—The Information Privacy Principles Privacy and Data Protection Act 2014 No. 60 of 2014 143

10. Principle 10—Sensitive Information

10.1 An organisation must not collect sensitive information about an individual unless—
(a) the individual has consented; or
(b) the collection is required or authorised under law; or
(c) the collection is necessary to prevent or lessen a serious threat to the life or health of any individual, where the individual whom the information concerns—
(i) is physically or legally incapable of giving consent to the collection; or (ii) physically cannot communicate consent to the collection; or
(d) the collection is necessary for the establishment, exercise or defense of a legal or equitable claim. 10.2 Despite IPP 10.1, an organisation may collect sensitive information about an individual if—
(a) the collection—
(i) is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services; or
(ii) is of information relating to an individual's racial or ethnic origin and is collected for the purpose of providing government funded targeted welfare or educational services; and
(b) there is no reasonably practicable alternative to collecting the information for that purpose; and Sch. 1 cl. 10.1(b) amended by No. 60/2017 s. 34(2). Sch. 1 cl. 10.1(c) amended by No. 23/2017 s. 22(3). Authorised by the Chief Parliamentary Counsel Schedule 1—The Information Privacy Principles Privacy and Data Protection Act 2014 No. 60 of 2014 144 (c) it is impracticable for the organisation to seek the individual's consent to the collection

Dated July 2023

ANARE Club Inc. **Attachment B**

Extract from the Club's Constitution /Rules Regarding-

APPENDIX G ACCESS TO PERSONAL INFORMATION

58 Improper use of information recorded on register of members

(1) A person must not use information about another person obtained from the register of members of an incorporated association to contact or send materials to the other person.

Penalty: 20 penalty units.

(2) A person must not disclose information about another person obtained from the register of members of an incorporated association knowing that the information is likely to be used to contact or send materials to the other person.

Penalty: 20 penalty units.

(3) Subsections (1) and (2) do not apply if the use or disclosure of the information—

(a) is directly related to the management or the purposes of the association; and

(b) is not prohibited by the rules of the association.

Example Information from the register of members may be used to give notice to members of general meetings of the association or to distribute newsletters of the association.

59 Restriction of access to personal information

(1) A request may be made to the secretary of an incorporated association to restrict access to the personal information of a person recorded in the register of members of the association.

(2) A request under subsection (1) may seek to restrict access so that the personal information is available only to—

(a) the secretary and members of the committee; or

(b) the secretary and members of the committee other than a specified member or specified members of the committee.

(3) The request may be made by—

(a) the person; or

(b) if the person is a child—by a parent or guardian of the person.

(4) If the secretary is satisfied that there are special circumstances which justify doing so, the secretary must agree to the request.

(5) If the secretary refuses the request, the secretary must notify the person who made the request of the decision.

(6) The notice must—

(a) be in writing; and

(b) include the reasons for the decision.

(7) If the secretary refuses the request, the secretary must not release the personal information without the consent of the person unless—

(a) at least 28 days have elapsed since the secretary gave notice to the person under subsection (5); and

(b) either—

(i) the person has not sought a review of the decision; or

(ii) VCAT has upheld the secretary's decision to release the information.

(8) If a person is notified by the secretary that his or her request to restrict access to personal information has been refused, the person may, within 28 days after the notification, apply to VCAT for a review of the decision.

(9) If—

(a) a member of an incorporated association informs the secretary of the association that he or she wishes to circulate material to all members of the association relating to its management, activities or purposes; and

(b) access to the personal information of another member recorded on the register of members of the association is restricted under this section— the secretary must forward that material to that other member.