PRIVACY POLICY

of

PIPE BANDS AUSTRALIA INC

(A0035346S)

Update adopted 01 March 2014

Contents

Part A - PRIVACY POLICY

1. POLICY STATEMENTS

1.1. Pipe Bands Australia Inc. ["the association"] affirms the National Privacy Principles.
1.2. The association's primary purpose in collecting information is to pursue its purposes as set out in its Rules in accordance with relevant Acts of Parliament, regulations and its rules and procedures.
1.3. It collects personal information from members and intending members to the least extent reasonably enabling it to carry out its stated primary purpose.
1.4. It collects sensitive information as permitted to the least extent possible.
1.5. It manages personal and sensitive information held by it in accordance with National Privacy Principles. In particular, the Council directs all officers and members of the association that the disclosure of any such information to which an officer or member may become privy is permitted only to an officer or member of the association who has an immediate and direct need to have that information, and otherwise only with the consent of the person whose information it is or in accordance with the law.
1.6. Disclosure of any personal or sensitive information to a law-enforcement or other interested agency for investigation of prosecution of an illegality must be recorded in writing without delay, and a copy of that record passed to the Secretary for filing.
1.7. Disclosure of personal information in accordance with the primary purpose above shall be recorded in a register kept for the purpose.
1.8. The statutory rights of access to information and to its correctness and being up to date shall be faithfully observed by the association and its officers.
1.9. Personal and sensitive information shall be destroyed promptly upon it becoming out of date or of no continuing use in the operations of the association and the fulfilment of its purposes and a record shall be kept of the destruction of that information.

Part B – GUIDING STATEMENTS

2. General

2.1. The Commonwealth Privacy Act 1988 was amended in 2000 to cover commercial and other bodies in their collecting and handling of information about people.

2.2. These notes seek to indicate the nature of the restrictions affecting the association's collection and release of information, and a mention of privacy issues arising from security surveillance of association premises and property.

3. Definitions

3.1. "personal information" means information or an opinion (including information or an opinion forming part of a database) whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. [Section 6 (1)]

3.2. "Sensitive information" means

3.2.1. information or an opinion about an individual's

3.2.1.1. racial or ethnic origin; or
3.2.1.2. political opinions; or
3.2.1.3. membership of a political association; or
3.2.1.4. religious beliefs or affiliations; or
3.2.1.5. philosophical beliefs; or
3.2.1.6. membership of a professional or trade association; or
3.2.1.7. membership of a trade union; or
3.2.1.8. sexual preferences or practices; or
3.2.1.9. criminal record

that is also personal information; or

3.2.2. health information about an individual.

4. National Privacy Principles (NPP #)

The amended Act requires organisations such as the association to follow the National Privacy Principles, which are set out in the Act, and breach of which is treated as a breach of the Act itself. These are considered briefly below.

4.1. NPP 1 – Acquiring information

4.1.1. An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities, and only in legal and fair means, and not unreasonably intrusive. As far as possible, information about a person should be collected from that person only.

4.1.2. Notes:

a) If information is collected from a third party, the organisation must as far as possible notify the subject person – the exception is unlikely to concern the association.

b) Upon or, if you please, before collecting a person's personal information, the organisation must take "reasonable steps" to ensure that the person is aware of:-

- the identity of the organisation and how to contact it;
- that the person may have access to the information;
- the purposes for which the information is collected;

- the organisations, or kinds of organisations, to which the organisation usually discloses information of that kind;
- any statute requiring collection of particular information; and
- the main consequences for an individual if the information is not provided.

4.2. NPP 2 – Use of information

4.2.1. An organisation must not use or disclose personal information about a person except for the primary purpose for which it is collected unless the secondary purpose is related to the primary purpose, and for sensitive information, directly related to the primary purpose, 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.

4.2.2. Notes:

a) There are other provisions relating to direct marketing use, from which it is suggested the association abstains, which avoids that issue, and in relation to statistics about public health or safety which seem remote from the association. An appropriate consent to use of information for such purposes on the original form probably sorts this out.

b) It is also permissible to use information in course of investigating suspected illegal activity or reporting it to proper authorities, and when required under law, and to protect public revenues and in relation to investigation of crime etc.

c) Should a situation arise where information is required by, for example, parent or guardian to help medical treatment then it may be given – the provision is cumbrous and should be checked if it is thought likely to be required.

d) The organisation must record, in writing, any use of information under this heading.

4.3. NPP 3 – Data Quality

4.3.1. Reasonable steps must be taken to ensure that information collected, used or disclosed is accurate, complete and up-to-date.

4.4. NPP4 – Data Security

4.4.1. Reasonable steps must be taken to protect personal information from misuse and from unauthorised access, modification or disclosure.

4.4.2. Information no longer needed for a proper purpose (under NPP 2 above) must be destroyed or “de-identified” (which ‘word’ presumably means making it impossible to tell to whom the information refers).

4.5. NPP 5 – Openness

4.5.1. 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.

4.6. NPP 6 – Access to and correction of information

4.6.1. An individual about whom personal information is held must be allowed access to that information unless it would put life or limb of another at risk, have an unreasonable impact on the privacy of other individuals, the request is vexatious or frivolous [e.g. making a daily request as an irritant], there is legal action or other negotiation between the organisation and the individual and the information is not available by

'discovery' in the course of an action at law, where access is unlawful, or would prejudice a criminal investigation or the like, or where a security organisation asks for non-disclosure. The last seems remote from the present inquiry, and the others not much less so. On occasion, information relating to commercially sensitive matters may be withheld. It is suggested that specific advice be sought when refusal of access is considered.

4.6.2. When access is refused, the organisation must, "if reasonable", consider whether access through an intermediary is satisfactory.

4.6.3. If information is believed inaccurate, the organisation must take "reasonable steps to correct it so that is accurate, complete and up-to-date. It the organisation and an individual disagree about the accuracy, completeness and up-to-dateness of information, presumably about an individual, the individual may ask that a letter or statement claiming that the information is not accurate etc be placed with the information, and the organisation must "take reasonable steps to do so".

4.6.4. If access or correction is refused, the organisation must give reasons for the refusal – presumably in writing, and filing a copy.

4.7. NPP 7 – Identifiers

4.7.1. It is proper for the association to use identifying numbers for members. Use of other organisation's identifiers for the same individuals is, generally, not permitted – though with exceptions. Again, should there be any specific problem in this area, specific advice should be sought.

4.8. NPP 8 – Anonymity

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

4.8.2. Note: In the association context, this seems of small relevance. To make a contract of any significance one must know the identity of the other party.

4.9. NPP 9 – Transborder data flows

4.9.1. Personal information must not be transferred outside Australia except in accordance with the Act, which in general spells out the need for the person's consent, or careful protection of the person's privacy rights by the recipient of the information to at least the extent provided by the Australian law. The existence of the restriction should be noted; if an apparent need to transfer information abroad arises, further specific advice should be sought. A band producing its registration papers overseas does not raise any problem for the association. The proposed consent below covers this point.

4.10. NPP 10 – Sensitive information

4.10.1. Sensitive information must not be collected without the consent of the person concerned, unless it is required by law, or to meet a threat to life and limb and consent cannot be obtained, or if necessary for the establishment, exercise or defence of a legal or equitable claim. [In practice, the inclusion of "equitable" adds nothing – this simply means dealing with, running or resisting a claim through the legal system.]

4.10.2. Notes:

a) A "not-for-profit organisation" has limited authority to collect sensitive information – but the section limits this to organisations with only racial, ethnic, political, religious, philosophical, professional, trade or trade union aims.

b) Information relating to medical and health conditions is defined as sensitive, and must not be disclosed except by consent of the person concerned or in accordance with the law.
c) Fortunately it will be rare indeed that we receive such information and rarer that we need to consider disclosing it. A possible instance is permission to breach dress requirements [for example] for a health reason.