

**PRIVACY POLICY OF THE**  
**GUNNEDAH AND DISTRICT CHAMBER OF COMMERCE AND INDUSTRY INC**  
**(Hereinafter referred to as “The Chamber”)**

There are 13 Australian Privacy Principles “APPS” with which it is necessary for us to comply:-

This policy has been established AND ADOPTED on the \_\_\_\_\_ 2014 as a result of changes to the legislation which have taken effect from the 12<sup>th</sup> March 2014.

An act done or practice engaged in by a person employed by, or in the service of the Gunnedah AND District Chamber of Commerce and Industry Inc, in performing the duties of the person’s employment is taken to be an act done or practice engaged in by the Gunnedah and District Chamber of Commerce and Industry Inc to whom this policy applies.

Information disclosed to a person employed by, or in the service of the Gunnedah and District Chamber of Commerce and Industry Inc is also taken to be information disclosed to the Gunnedah and District Chamber of Commerce and Industry Inc.

**APP 1 – Open and transparent management of personal information – outlines the requirements for an APP entity to manage personal information in an open and transparent way.**

- The Chamber will take all steps necessary, to ensure any information it receives on its members, for it to be managed in an open and transparent way.

Information collected on members will include but will not be limited to:-

Name, Business address, Postal address (if different from business address), Phone number (Landline or Mobile), Email address and your preferred method of accessing information which must be made available to you from time to time. Details of which are electronically stored to enable access through our website.

All of this information (both electronic and hard copy) is stored on site and is not outsourced in any way.

- The Chamber will take all steps necessary to implement any practices, procedures and systems that will ensure it complies with the APPs and any binding APP code and will deal with related enquiries and complaints.
- The Chamber will endeavour to have the policy clearly expressed and up-to-date regarding how it manages personal and business information.
- The Chamber will provide the Policy, upon request, free of charge and in the appropriate form (including on its website).
- Individuals may, upon request and after satisfactory identification, access their personal information held by the Chamber during normal office hours.

**APP 2 – Anonymity and Pseudonymity – provides that individuals must have the option of dealing anonymously or by pseudonym with an APP entity.**

- Anonymity requires that an individual may deal with an APP entity without providing any personal information or identifiers.

- Pseudonymity requires that an individual may Deal with an APP entity by using a name, term or descriptor that is different to the person's actual name.

APP 2 provides that individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter. Since most matters that would be dealt with by the Chamber, would relate to members and would need to be dealt with in terms of our constitution, identification of those parties necessary to achieve a result would need to be obtained. No further information than that necessary to achieve a result would be gathered and all information regarding the matter would only be privy to the Management Committee and any parties involved in the resolution of the said matter.

**APP 3 – Collection of solicited personal information – outlines when an APP entity may collect solicited information.**

- All information collected in terms of this section must be collected by lawful and fair means.
- Information collected in terms of this section would be restricted to that required for us to reasonably conduct the business and functions related to any services that we provide in the normal course of our business.
- This section would also refer to any future services which we may introduce.
- No sensitive information would be solicited or collected without the written permission of the individual so giving it.
- All information collected in terms of this section prior to and upon completion of any event is stored in a secure manner without access by the public.

**APP 4 – Dealing with Unsolicited information – outlines the steps an entity must take if it receives unsolicited personal information.**

- Unsolicited information is personal information received by an APP entity where the entity has taken no active steps to collect the information.
- Information received in terms of this section must be identified as to whether or not it could have been collected under Section 3 of this policy or has been received as unsolicited and should be destroyed or de-identified as soon as practicable, unless it is contained in a "Commonwealth record" or it is unlawful or unreasonable to do so.

**APP 5 – Notification of the collection of personal information – An APP entity that collects personal information about an individual must take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters.**

- The matters include:
  - i) the APP entity's identity and contact details
  - ii) the fact and circumstances of collection
  - iii) whether the collection is required or authorised by law
  - iv) the purposes of the collection
  - v) the consequences if personal information is not collected
  - vi) the entity's usual disclosures of personal information of the kind collected by the entity
  - vii) information about the entity's APP Privacy Policy
  - viii) whether the entity is likely to disclose personal information to overseas recipients, and if practicable, the countries where they are located.
- Personal information held by the Chamber, may be accessed by the member to whom that personal information relates, upon request and after identification to the satisfaction of the Chamber.

**APP 6 – Use or disclosure of personal information – outlines when an APP entity may use or disclose personal information.**

- An APP entity can only use the personal information for the purpose for which it was collected (known as the primary purpose), or for a secondary purpose if an exception applies.
- The exceptions include where:
  - i) The individual has consented to a secondary use or disclosure
  - ii) The individual would reasonably expect the APP entity to use or disclose their personal information for the secondary purpose, and that purpose is related to the primary purpose of collection , or , in the case of sensitive information, directly related to the primary purpose
  - iii) The secondary use or disclosure is required or authorised by or under an Australian law or a court/tribunal order
  - iv) A permitted general situation exists in relation to the secondary use or disclosure
  - v) The APP entity reasonably believes that the secondary use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

**APP 7 – Direct marketing – provides that an organisation must not use or disclose personal information it holds for the purpose of direct marketing unless an exception applies.**

- Direct marketing involves the use or disclosure of personal information to communicate directly with an individual to promote goods or services
- Where an organisation is permitted to use or disclose personal information for the purpose of direct marketing, it must always:
  - i) Allow an individual to request not to receive direct marketing communications (also known as opting out), and
  - ii) Comply with that request.

**APP 8 – Cross-border disclosure of personal information – before an APP entity discloses personal information to an overseas recipient, the entity must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information.**

- No personal information which the Chamber holds will be released (unless required by law) to any third party especially any international one.

**APP 9 – Adoption, use or disclosure of government related identifiers – restricts the adoption, use and disclosure of government related identifiers by organisations.**

- An identifier is a number, letter or symbol, or a combination of any or all of those things, that is used to identify the individual or to verify the identity of the individual.
- Where an identifier, including a government related identifier, is personal information, it must be handled in accordance with the APPs.
- An organisation must not adopt a government related identifier of an individual as its own identifier of the individual, unless an exception applies.
- An organisation must not use or disclose a government related identifier of an individual, unless an exception applies.
- An individual cannot consent to the adoption, use or disclosure of their government related identifier

**APP 10 – Quality of personal information – an APP entity must take reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete.**

- Personal information is inaccurate if it contains an error or defect.
- Personal information is out-of-date if it contains facts, opinions or other information that is no longer current
- Personal information is incomplete if it presents a partial or misleading picture, rather than a true or full picture

**APP 11 – Security of personal information – an APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.**

- An APP entity must take reasonable steps to destroy or de-identify the personal information it holds once the personal information is no longer needed for any purpose for which the personal information may be used or disclosed under the APPs
- An APP entity “holds” personal information if the entity has possession or control of a record that contains the personal information
- If sensitive information is held then the level of security would need to be greater

**APP 12 – Access to personal information – requires an APP entity that holds personal information about an individual to give the individual access to that information on request.**

- Personal information is defined as 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 material form or not”.
- Personal information of one individual may also be personal information of another individual.
- This section requires an APP entity to provide access to all of an individual’s personal information it holds, even if that information is also the personal information of another individual, unless a ground to refuse access applies.
- An APP entity must be satisfied that a request for personal information under APP 12 is made by the individual concerned, or by another person who is authorised to make a request on their behalf, for example, as a legal guardian or authorised agent.
- The steps appropriate to verify an individual’s identity will depend on the circumstances.

**APP 13 – Correction of personal information – requires an APP entity to take reasonable steps to correct personal information and to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading.**

- Following on from APP 10 the Chamber endeavours to maintain the most up-to-date records of the business information it can, however, businesses are bought and sold and transfers and change of address transpire without the Chamber being advised. In this event we must wait until contact is made by the member in question for us to be able to update the information on that member. If it were common knowledge of a new address for a member the Chamber would assume it would be a reasonable step for it to amend its records accordingly.
- Input of personal information can sometimes lead to the incorrect information being held on a member. As soon as we become aware of the inconsistency in the data it should be remedied.
- Only relevant personal information is held on members and individuals g functions/seminars.