Summary of Australian Privacy Principles

(Schedule 1, Privacy Amendment (Enhancing Privacy Protection) Act 2012)

**Australian Privacy Principle 1: Open and Transparent Management of Personal Information**

APP entities must ensure that they manage personal information in an open and transparent manner. APP entities can achieve this by ensuring compliance with the Australian Privacy Principles, and implementing a clearly expressed APP privacy policy, which explains what kinds of information the APP entity collects and holds, how that information is collected and the purposes for which it is collected.

**Australian Privacy Principle 2: Anonymity and Pseudonymity**

When collecting personal information, APP entities must provide individuals with the option to not be identified or to use a pseudonym. This principle is subject to exceptions in circumstances where an individual must provide identifiable information by law, or circumstances where it is impracticable to deal with unidentified information.

**Australian Privacy Principle 3: Collection of Solicited Personal Information**

This Australian Privacy Principle provides that an APP entity or agency may collect solicited information if the information is directly related to one or more of the APP entity’s functions or activities. The principle applies a higher standard for sensitive information, which attaches the requirement to obtain an individual’s consent for the collection of such information.

**Australian Privacy Principle 4: Dealing with Unsolicited Personal Information**

This Australian Privacy Principle makes provision for cases where APP entities receive unsolicited personal information. In such cases, APP entities must determine whether they could have collected the personal information under Australian Privacy Principle 3 (APP 3). If APP 3 could not apply to the unsolicited information, then the APP entity must de-identify or destroy the data if it is lawful to do so.

**Australian Privacy Principle 5: Notification of The Collection of Personal Information**

APP entities are required to make individuals aware that their personal information is being collected. Among other requirements, this means APP entities are expected to disclose their contact details, the purpose for which the information is being collected, whether the personal information might be shared with other entities or agencies, and how an individual may access and correct personal information held about them.

**Australian Privacy Principle 6: Use or Disclosure of Personal Information**

An APP entity must not use personal information obtained from an individual for a particular purpose for a secondary purpose without obtaining the consent of the individual, except in limited circumstances.

**Australian Privacy Principle 7: Direct Marketing**

This principle provides that an APP entity must not use an individual’s personal information for the purposes of direct marketing, unless certain conditions can be satisfied, such as obtaining the consent of the individual to use their information for such a purpose.
Australian Privacy Principle 8: Cross-Border Disclosure of Personal Information

Under this principle, APP entities must take reasonable steps to ensure that if they disclose personal information to an overseas entity, that the overseas entity conforms with standards expected in accordance with the Australian Privacy Principles for the handling of such information.

Australian Privacy Principle 9: Adoption, Use or Disclosure of Government Related Identifiers

Australian Privacy Principle 9 precludes an APP entity from using government related identifiers of an individual for its own purposes, subject to limited exceptions, such as where that use is authorised by law or to fulfil the APP entity’s obligations to a Commonwealth, State or Territory authority.

Australian Privacy Principle 10: Quality of Personal Information

Under this principle, APP entities are obliged to take reasonable steps to ensure that the personal information they collect is accurate, up-to-date and complete, and that the information they disclose is also accurate, up-to-date and complete for the purposes of that disclosure.

Australian Privacy Principle 11: Security of Personal Information

An APP entity holding personal information must take reasonable steps to protect the information from misuse, interference, loss, unauthorised access, modification or disclosure. An APP entity must take reasonable steps to destroy or de-identify personal information that it no longer needs for any purpose allowed by the Principles, except where the information is contained in a Commonwealth record or if the APP entity is required by law or ordered by a court/tribunal to retain the information.

Australian Privacy Principle 12: Access to Personal Information

An APP entity must provide access to information that it holds about an individual if that individual requests it, subject to certain exceptions, such as where access is denied by legislation or court/tribunal order, or would impact on the life, health, safety or privacy of another person.

If an exception applies, the APP entity must take reasonable steps to give access in a way that meets the needs of the entity and the individual, or provide the individual with a written notice of the reasons for refusal. Charging for access is not permitted for agencies, and must not be excessive for organisations.

Australian Privacy Principle 13: Correction of Personal Information

An APP entity must take reasonable steps to correct the personal information it holds about an individual if the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, or upon request from the individual. Upon the individual’s request, the APP entity must take reasonable steps to notify any other APP entity to which it has previously disclosed the information being corrected.

An APP entity which refuses a request to correct information must provide a written notice of reasons to the individual and, if requested to do so, associate to the information a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, in a way which would be apparent to users of the information.