DARTS AUSTRALIA Inc.

INFORMATION PRIVACY PLAN

INFORMATION PRIVACY PLAN

1. Policy Statement

Darts Australia [DA] collects and holds personal information for the purposes of facilitating its business. It is important that the use of this information is confined to the purposes for which it is

acquired. DA is committed to protecting the privacy of our players, officials, directors, delegates, contractors and consultants.

The Privacy Act 1988 [National] provides for the protection of personal information and for the protection of the privacy of individuals. The IPA requires all public sector agencies to prepare, implement and review their Privacy Management Plan. This plan outlines how DA complies with the legislative requirements of the IPA and Privacy Act 1988 [National] and the Privacy Code of Practice 2003 [National].

1.1 Policy

PART 1 – INTRODUCTION

Federal Government agencies are required to comply with 13 Information Privacy Principles (IPPs) contained in the Privacy Act 1988 (the IP Act) which cover the responsible collection, storage, use and disclosure of personal information held by government agencies.

1.2 Framework

The 13 APPs can be broadly categorised into the following five groups:

Manner and Purpose of Collection of information

APP 1. **Collection of personal information (lawful and fair)**
APP 2. **Anonymity and Pseudonymity**
APP 3. **Collection of solicited information (personal)**
APP 4. **Dealing with unsolicited personal information**

Storage and security of information

APP 5 **Specifies certain matters about which an agency must generally make an individual aware at the time of, or as soon as practicable after, the agency collects their personal information.**

Use of Personal Information

APP 6 **Use and disclosure of personal information**

These include where the use or disclosure is reasonably necessary:

- To assist in locating a missing person
- To establish, exercise or defend a legal or equitable claim, or o For the purposes of a confidential alternative dispute resolution.

Direct Marketing

APP 7 **Direct marketing**

purposes where the individual has either consented to their personal information being used Generally, organisations may only use or disclose personal information for direct marketing for direct marketing, or has a reasonable expectation that their personal information will be used for this purpose, and conditions relating to opt -out mechanisms are met.

APP 7 permits contracted service providers for Commonwealth contracts to use or disclose personal information for the purpose of direct marketing if certain conditions are met.

Cross Border Disclosures APP 8 Cross-border disclosures

Before an agency discloses personal information to an overseas recipient, the agency must take reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to that information. In some circumstances an act done, or a practice engaged in, by the overseas recipient that would breach the APPs, is taken to be a breach of the APPs by the agency. There are a number of exceptions to these requirements.

Adoption, use or Disclosure of Government Related Identifiers APP 9 Adoption, use or disclosure of government related identifiers

APP 9 prohibits an organisation from adopting, using or disclosing a government related identifier unless an exception applies. APP 9 generally replicates the restrictions in National Privacy Principle 7 for organisations.

Exceptions generally refer to situations where the adoption, use or disclosure is required or authorised by law, a 'permitted general situation' (as outlined in s 16A) exists, or the use or disclosure is reasonably necessary:

- To verify the identity of the individual
- To fulfil obligations to an agency or State or Territory authority
- For one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Quality of Personal Information

APP 10 Quality of personal information

Under APP 10, an agency must take reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete.

An agency must also ensure that the personal information that it uses or discloses is accurate, up-to-date and complete and relevant, having regard to the purpose of the use or disclosure.

Security of Personal Information

APP 11 Security of personal information

APP 11 requires an agency to take reasonable steps to protect the personal information it holds from interference, in addition to misuse and loss, and unauthorised access, modification and disclosure.

APP 11 imposes a new requirement on agencies to take reasonable steps to destroy or deidentify information if the agency no longer needs the information for any authorised purpose, unless:

- It is contained in a Commonwealth record, or
- The agency is required by or law or a court/tribunal order to retain the information.

Access to Personal Information

APP 12 Access to personal information

Like IPP 6, APP 12 requires an agency to give an individual access to the personal information that it holds about that individual, unless the agency is required or authorised to refuse to give access by or under the Freedom of Information Act 1982 or any other Commonwealth or Norfolk Island legislation that provides for access by persons to documents.

Where access is given under the Privacy Act, APP 12 introduces a new requirement for agencies to respond to requests for access within 30 days. Agencies must give access in the manner requested by the individual if it is reasonable and practicable to do so, and must not charge.

If an agency refuses to give access, or to give access in the manner requested, it must take reasonable steps to give access in a way that meets the needs of the agency and the individual. This could include the use of a mutually agreed intermediary.

If an agency decides not to give an individual access it must generally provide written reasons for the refusal and the mechanisms available to complain about the refusal.

Correction of Personal Information

APP 13 Correction of personal information

Like IPP 7, APP 13 requires an agency to take reasonable steps to correct personal information to ensure that, having regard to a purpose for which it is held, it is accurate, up to-date, complete, relevant and not misleading, if either:

- The agency is satisfied that it needs to be corrected, or
- An individual requests that their personal information is corrected.

APP 13 contains similar provisions to IPP 7 in relation to associating a statement with the personal information if the agency refuses to correct the information and the individual requests a statement to be associated.

An agency must also respond to a correction request or a request to associate a statement by the individual within 30 days, and must not charge the individual for making the request, for correcting the personal information, or for associating the statement with the personal information.

When refusing an individual's correction request, an agency must generally provide the individual with written reasons for the refusal and notify them of available complaint mechanisms.

If an agency corrects personal information about an individual that it previously disclosed to another entity, APP 13 generally requires the agency to take reasonable steps to notify the other entity that a correction has been made, if the individual requests it to do so.
The primary intent of the Privacy Act is to protect the privacy of personal information that is collected and used in the delivery of government services and the conduct of government business.

1.3 Principles

Information Privacy act contain sets of principles which govern conduct to protect personal information.
They are: Australian Privacy Principles (APPs); and

These principles set out legal obligations for:

- Collection;
- Storage;
- Access and accuracy;
- Use; and
- Disclosure of personal and health information.

1.4 Objectives

The objective of this plan is to:

- Establish practices and procedures to protect the privacy rights of individuals with respect to all forms of personal information held by Darts Australia.
- Specify how Darts Australia handles the personal information it collects, stores, accesses, uses and discloses in the course of its business activities.
- Ensure Darts Australia complies with the principles and requirements of Privacy Act 1988 (NPA).

1.5 Responsibility

The overall responsibility for privacy at Darts Australia rests with the President. All DA staff is responsible for ensuring that they comply with the Privacy Act.

At the organisational level, responsibility for IP is described as follows:

- DA and Executive Management - Review, support, endorse and ensure accountability within the Information Privacy Plan.
- Manage and Administer the Information Privacy Plan.
- All members and officials - Use and apply DA Policies and Procedures, act with the purpose of continuous improvement.

2. Implementation

The Information Privacy Plan will be implemented through Darts Australia, through the following mechanisms.

- Prepare and monitor the implementation of this Privacy Management Plan
- Conduct internal reviews of complaints and ensure that all complaints about privacy breaches are dealt with properly.
- Monitoring and review by DA Executive/Privacy Officers