Water Polo
AUSTRALIA

PRIVACY POLICY

January 2021

1. Purpose

- From time to time Water Polo Australia Limited ("WPA") is required to collect, hold, use and/or disclose personal information relating to individuals (including, but not limited to its customers, contractors, suppliers and employees) in the performance of its business activities.

- The information collected by WPA will, from time to time, be accessible to certain individuals employed or engaged by WPA who may be required to use the information in the course of their duties.

- This document sets out WPA's policy in relation to the protection of personal information, as defined, under the Privacy Act 1988 (Cth) the ("Act"), which includes the Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) and the Australian Privacy Principles ("APP"). The APPs regulate the handling of personal information.

- The obligations imposed on WPA under this policy are also imposed on any individual employed or engaged by WPA.

- This policy outlines WPA's requirements and expectations in relation to the handling of personal information.

2. Scope

This policy applies to all employees, independent contractors, consultants and other persons engaged by WPA and who have access to personal information in the course of performing their duties on behalf of WPA ("employees").

3. The Privacy Officer

The Privacy Officer can be contacted by email at privacy@waterpoloaustralia.com.au or by mail to Level 2, Building B, 6 Figtree Drive, Sydney Olympic Park NSW 2127.

4. What is Personal Information?

- 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 material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

5. What is not Personal Information?

- This policy does not apply to the collection, holding, use or disclosure of personal information that is an employee record as they are exempt from the APPs.

- An employee record is a record of personal information relating to the employment of an employee. Examples of personal information relating to the employment of the employee include, but are not limited to, health information and information about the engagement, training, disciplining, resignation, termination, terms and conditions of employment of the employee.

- Employees (such as those engaged in a supervisory, operations or human resource capacity) will have access to employee records.

- Employees who have access to employee records must ensure that the information is handled confidentially and for a proper purpose only.

- Employee records are only permitted to be collected, used and disclosed where the act of doing so is directly related to a current or former employment relationship.

- Employees who have access to employee records and who may have a question about the use or disclosure of employee records, should contact the Privacy Officer.

6. Kinds of information that WPA collects and holds

- WPA collects personal information that is reasonably necessary for one or more of its functions or activities or if WPA has received consent to collect the information. If WPA collects sensitive information (as defined below), WPA must also have obtained consent in addition to the collection being reasonably necessary.

- The type of information that WPA collects and holds may depend on an individual's relationship with WPA, for example:

a) Candidate: if a person is a candidate seeking employment with WPA, WPA may collect and hold information about that candidate including the candidates name, address, email address, contact telephone number, gender, age, employment history, references, resume, medical history, emergency contact, taxation details, qualifications and payment details.

b) Athlete: if a person is an athlete associated with WPA, WPA may collect and hold information including the athlete's name, address, email address, contact telephone number, gender, age, participation and playing history in the sport of water polo and other sensitive information.

c) Supplier: if a person or business is a supplier of WPA, WPA may collect and hold information about the supplier including the supplier's name, address, email address, contact telephone number, business records, billing information and information about goods and services supplied by the supplier.

d) Referee: if a person is a referee of a candidate being considered for employment by WPA, WPA may collect and hold information including the referee's name, contact details, current employment information and professional opinion of candidate.

e) Sensitive information: WPA will only collect sensitive information where an individual consents to the collection of the information, the collection is required or authorised by law, the collection is necessary to prevent or lessen a serious and imminent threat to the life or health any individual where the person about whom the sensitive information is collected is physically or legally incapable of giving consent or physically cannot communicate consent, or the information is reasonably necessary for one or more of WPA's functions or activities. Sensitive information includes, but is not limited to, information or an opinion about racial or ethnic origin, political opinions, religious beliefs, philosophical beliefs, membership of a trade union, sexual preferences, criminal record, health information, medical and anti-doping testing and investigations or genetic information.

7. How WPA collects and holds personal information

- WPA (and the employees acting on WPA's behalf) must collect personal information only by lawful and fair means.

- WPA may collect personal information in a number of ways, including without limitation:

    - through application forms (e.g. job applications, VIP and loyalty program applications);

    - by email or other written mechanisms;

- over a telephone call;

- in person;

- through transactions;

- through WPA website;

- through engagement with WPA's social media channels;

- through lawful surveillance means such as a surveillance camera;

-by technology that is used to support communications between individuals and WPA;

- through third-parties (which may include the Australian Sports Anti-Doping Authority, Sports Australia, Fédération Internationale de Natation and state and territory governing bodies);

- through publicly available information sources (which may include telephone directories, the internet and social media sites); and

- direct marketing database providers.

- When WPA collects personal information about an individual through publicly available information sources, it will manage such information in accordance with the APPs.

- At or before the time or, if it is not reasonably practicable, as soon as practicable after, WPA collects personal information, WPA must take such steps as are reasonable in the circumstances to either notify the individual or otherwise ensure that the individual is made aware of the following:

- the identity and contact details of WPA;

- that WPA has collected personal information from someone other than the individual or if the individual is unaware that such information has been collected;

-that collection of personal information is required by Australian law, if it is;

- the purpose for which WPA collects the personal information;

- the consequences if WPA does not collect some or all of the personal information;

- any other third party (such as state and territory water polo governing bodies, member associations and Sport Australia) to which WPA may disclose the personal information collected by WPA;

- WPA's privacy policy contains information about how an individual may access and seek correction of personal information held by WPA and how an individual may complain about a breach of the APPs; and

- whether WPA is likely to disclose personal information to overseas recipients, and the countries in which those recipients are likely to be located.

- Unsolicited personal information is personal information that WPA receives which it did not solicit. Unless WPA determines that it could have collected the personal information in line with the APPs or the information is contained within a Commonwealth record, it must destroy the information to ensure it is de-identified unless WPA determines that it is acceptable for WPA to have collected the personal information.

8. Use and Disclosure of Personal Information

- The main purposes for which WPA may use and/or disclose personal information may include but are not limited to:

-recruitment functions;

- athlete management;

- compliance with rules, regulations and policies implemented by WPA and other organisations such as the International Olympic Committee and Fédération Internationale de Natation;

- customer service management;

- training and events;

- surveys and general research; and

- business relationship management.

- WPA may also collect, hold, use and/or disclose personal information if an individual consents or if required or authorised under law.

- Direct marketing:

- WPA may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing (for example, advising a customer about new goods and/or services being offered by WPA);

- WPA may use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose; and

- an individual can opt out of receiving direct marketing communications from WPA by contacting the Privacy Officer in writing or if permissible accessing WPA's website and unsubscribing appropriately.

9. Disclosure of Personal Information

- WPA may disclose personal information for any of the purposes for which it is was collected, as indicated under clause 0 of this policy, or where it is under a legal duty to do so.

- Disclosure will usually be internally and to related entities or to third parties such as contracted service suppliers.

- If an employee discloses personal information to a third party in accordance with this policy, the employee must take steps as are reasonable in the circumstances to ensure that the third party does not breach the APPs in relation to the information.

a) Cross-border disclosure of personal information.

- WPA may be likely to disclose personal information to overseas recipients. Before an employee on behalf of WPA discloses personal information about an individual to an overseas recipient, the employee will take steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs in relation to the information.

- The country or countries in which overseas recipients are likely to be located include, without limitation, Switzerland.

10. Access to personal information

- If WPA holds personal information about an individual, the individual may request access to that information by putting the request in writing and sending it to the Privacy Officer. WPA will respond to any request within a reasonable period, and a charge may apply for giving access to the personal information where WPA incurs any unreasonable costs in providing the personal information.

- There are certain circumstances in which WPA may refuse to grant an individual access to personal information. In such situations WPA will provide the individual with written notice that sets out:

    - the reasons for the refusal; and

    - the mechanisms available to you to make a complaint.

- If you receive such a request, please contact the Privacy Officer.

11. Correction of personal information

- If WPA holds personal information that is inaccurate, out-of-date, incomplete, irrelevant or misleading, it must take steps as are reasonable to correct the information.

- If WPA holds personal information and an individual makes a request in writing addressed to the Privacy Officer to correct the information, WPA must take steps as are reasonable to correct the information and WPA will respond to any request within a reasonable period.

- There are certain circumstances in which WPA may refuse to correct the personal information. In such situations WPA will give the individual written notice that sets out:

    - the reasons for the refusal; and

    - the mechanisms available to the individual to make a complaint.

- If WPA corrects personal information that it has previously supplied to a third party and an individual requests WPA to notify the third party of the correction, WPA will take such steps as are reasonable to give that notification unless impracticable or unlawful to do so.

- If you receive such a request, please contact the Privacy Officer.

12. Integrity and security of personal information

- WPA will take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that it collects is accurate, up-to-date and complete.

- Employees must take steps as are reasonable in the circumstances to protect the personal information from misuse, interference, loss and from unauthorised access, modification or disclosure.

- If WPA holds personal information and it no longer needs the information for any purpose for which the information may be used or disclosed and the information is not contained in any Commonwealth record and WPA is not required by law to retain the information, it will take such steps as are reasonable in the circumstances to destroy the information or to ensure it is de-identified.

- If you are unsure whether to retain personal information, please contact the Privacy Officer to discuss.

13. Data Breaches and Notifiable Data Breaches

- A **"Data Breach"** occurs where personal information held by WPA is accessed by, or is disclosed to, an unauthorised person, or is lost. An example of a Data Breach may include:

  - Lost or stolen laptops or tablets;

  - Lost or stolen mobile phone devices;

  - Lost or stolen USB data storage devices;

  - Lost or stolen paper records or documents containing personal information relating to the Employer's customers or employees;

  - Employees mistakenly providing personal information to the wrong recipient (i.e. payroll details to wrong address);

  - Unauthorised access to personal information by an employee;

  - Employees providing confidential information to WPA's competitors;

  - Credit card information lost from insecure files or stolen from garbage bins;

  - Where a database has been 'hacked' to illegally obtain personal information; and

  - Any incident or suspected incident where there is a risk that personal information may be misused or obtained without authority.

- If you are aware of or reasonably suspect a Data Breach, you must report the actual or suspected Data Breach to the Privacy Officer as soon as reasonably practicable and not later than 24 hours after becoming aware of the actual or suspected Data Breach.

- A **"Notifiable Data Breach"** occurs where there is an actual Data Breach, and:

  - a reasonable person would conclude that the unauthorised access or disclosure would likely result in serious harm to the relevant individual (including harm to their physical or mental well-being, financial loss, or damage to their reputation); or

  - in the case of loss (i.e. leaving an unsecure laptop containing personal information on a bus), unauthorised access or disclosure of personal information is likely to occur as a result of the Data Breach, and a reasonable person would conclude that the unauthorised access or disclosure would likely result in serious harm to the relevant individual (including harm to their physical or mental well-being, financial loss, or damage to their reputation).

- A Notifiable Data Breach does not include a Data Breach where WPA has been successful in preventing the likely risk of serious harm by taking remedial action.

a) Assessment

- If WPA is aware of any actual or suspected Data Breach, it will conduct a reasonable and expeditious assessment to determine if there are reasonable grounds to believe that the Data Breach is a Notifiable Data Breach or not.

b) Notification

- Subject to any restriction under the Act, in the event that WPA is aware of a Notifiable Data Breach, WPA will, as soon as practicable, prepare a statement outlining details of the breach and notify:

  - the individual whose personal information was part of the Data Breach; and

  - the Office of the Australian Information Commissioner.

14. Anonymity and Pseudonymity

- Individuals have the option of not identifying them self, or using a pseudonym, when dealing with WPA in relation to a particular matter. This does not apply:

  - where WPA is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or

  - where it is impracticable for WPA to deal with individuals who have not identified themselves or who have used a pseudonym.

- However, in some cases if an individual does not provide WPA with the personal information when requested, WPA may not be able to respond to the request or provide them with the goods or services that they are requesting.

15. Complaints

- Individuals have a right to complain about WPA's handling of personal information if the individual believes WPA has breached the APPs.

- If an employee becomes aware of an individual wanting to make such a complaint to WPA, the employee should direct the individual to first contact the Privacy Officer in writing. Complaints will be dealt with in accordance with WPA's complaints procedure and WPA will provide a response within a reasonable period.

- Individuals who are dissatisfied with WPA's response to a complaint, may refer the complaint to the Office of the Australian Information Commissioner.

16. Breach of this Policy

- An employee directed by WPA to do an act under this policy and which relates to personal information, must ensure that in doing the act they comply with the obligations imposed on WPA. An employee directed by WPA who fails to do an act in accordance with this policy will be deemed to have breached this policy and will be subject to formal counselling and disciplinary action, up to and including possible termination of the employee's employment.

Date Prepared / Reviewed:	By Whom:	Approved By:	Board Approval Date:	Next Review Date:
Nov 2020	360HR / CFO	Board	12-12-2020	Nov 2021