Office of Sport

Privacy Management Plan

March 2025

Summary

To document how the Office of Sport (the Office) manages personal information in line with the Privacy and Personal Information Protection Act 1998 (NSW) (PPIPA) and health information under the Health Records and Information Privacy Act 2002 (HRIPA). With this plan we also acquit our compliance with Part 6A and section 33 of the PPIPA.

Document information

Title:	Privacy Management Plan
Version:	V3.0
Approved date:	20 March 2025
Approver:	Chief Executive
Owner:	Executive Director – Corporate
Contact:	Privacy Officer
Publishing:	This document can be published on the intranet and internet
Review:	Every 2 years or as required from time to time
Next Review:	March 2027
Related Documents and Forms:	Centres, Venues & Regions Privacy Statement Combat Sports Privacy Statements Email Marketing Privacy Statement Internal Eligible Data Breach Register Internet Privacy Statement Office of Sport Privacy Statement Public Data Breach Notification Register Privacy Management Procedure Privacy Data Breach Response Plan Privacy Risk Assessment Procedure Privacy Impact Assessment Report Template Privacy Information Register Privacy Audit Survey Privacy Audit Report Privacy Internal Review Request Form
Related Internal Policies/Procedures:	Access to Information and Continuous Disclosure Policy Allergen Free Meals Standard Operating Procedure Code of Conduct and Ethics Complaints Handling Policy Child Safe Professional Standards Cyber Security Policy Framework Disability Inclusion Action Plan 2023 -2026 Enterprise Risk Management Policy & Procedure Exchange of Child Protection Information Policy and Procedure Incident Investigation Procedure, Safety Management System Incident Management and Reporting Procedure Records Management Policy Incident Investigation Procedure, Safety Management System Incident Management and Reporting Procedure Identification and Visitor Policy IM&T Access Control Policy and Procedure IM&T Acceptable Use Policy and Procedure IM&T Cyber Security Roles and Responsibilities Policy

	IM&T Cyber Security Framework NSW Government Cyber Security Guide Public Interest Disclosure Policy Prevention and Management of Unacceptable Workplace Behaviours Policy and Procedure Records Management Policy Records Destruction Procedure Reporting Concerns About Child Safety Working with Children Check Policy and Procedure
Related External Policies or Links:	Child Protection (Working with Children) Amendment (Statutory Review) Act 2018 Data Sharing (Government Sector) Act 2015 Government Information (Public Access) Act 2009 Health Records and Information Privacy Code of Practice 2005 Health Records and Information Privacy Act 2002 Health Records and Information Privacy Regulation 2022 Information and Privacy Commission New South Wales website Mandatory Notification of Data Breach (MNDB) Scheme NSW Government Cloud Policy NSW Cyber Security Policy Payment Card Industry Data Security Standard Privacy Act 1988 (Cwlth) Privacy Code of Practice (General) 2003 Privacy and Personal Information Protection Act 1998 Privacy and Personal Information Protection Regulation 2019 State Records Act 1998 (NSW) State Records Regulation 2015 Workplace Surveillance Act 2005 (NSW) Workplace Surveillance Regulation 2022 European Union General Data Protection Regulation United Kingdom General Data Protection Regulation

Version	Amendments**	Prepared by title, unit	Date	Record No.
V1.0	Initial release – approved by the Chief Executive (and submitted to the Information and Privacy Commission)	Sally Ryan, Manager Corporate Planning and Performance, Executive Services	18 Dec 2018	CDOC18/73642
V1.1	2024 Review	Michelle McNamara, Liss Gringhuis, Ministerial Support Officer	24 Jan 2024	D24/1784
V2.0	Major update – to be reviewed by IPC and approved by Core Executive	Sharon Paudel, Manager EMS	4 Oct 2024	D24/1784
V2.1	Staff Consultation amendments	Michelle McNamara, Ministerial Support Officer	31 Jan2024	D24/1784
V3	Final – approved by Core Executive	Michelle McNamara, Ministerial Support Officer	20 Mar 2025	D24/1784

Table of contents

Policy

1 Purpose Statement

The Office takes the privacy of our clients, stakeholders and staff seriously and will protect privacy in accordance with this Privacy Management Plan.

The Office of Sport is committed to ensuring that personal information is:

- only collected where directly required for an activity or service provided, and when doing so the purpose, intended recipients and whether it is required by law or is voluntary, any right of access to, and correction of, that information, and the name and address of the Office (being the agency that is collecting and holding that information) is clearly stated
- only collected directly from the individual to whom the information relates, unless the individual has authorised the collection from someone else or the information relates to a person under the age of 16 years and has been provided by that person's parent or guardian
- ensure collection points only collect purpose relevant information
- protected with necessary safeguards against loss, unauthorised access, misuse, modification or disclosure
- not kept for longer than necessary and is disposed of securely
- accessible, open to amendment and, where appropriate, erasure, on request from the individual on whom the information is held.

2 Scope

The plan applies to all business areas within the Office of Sport and contractors/suppliers who use Office of Sport personal and health data.

3 Office of Sport functions and activities

The Office is responsible for planning, managing, and delivering high quality venues, facilities and sport and active recreation development programs, high performance sport and sports integrity and safety. It is also the driver for NSW sport policy and strategy, formation and dissemination of insights and information, and the promotion of partnerships.

The Office operates Sport and Recreation Centres and Sporting Venues that provide programs, facilities and accommodation for school, sporting clubs and the community and administers various legislation, including the *Motor Vehicle (Public Safety) Act 1985* (NSW) and *Combat Sports Act 2013* (NSW).

4 Definitions

Personal Information	Information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. This can include but not limited to information about our staff, sport and recreation clients, combatant, grant contacts and other contacts. It can include details such as name, address, phone number, email address, date of birth, tax file number or health information.

Health Information	Is a specific type of personal information that is defined in section 6 of HRIPA as:
	• Personal information that is also information or an opinion about:
	  ○ An individual's physical or mental health or disability
	  ○ An individual's express wishes about the future provision of health services to themselves
	  ○ A health service provided, or to be provided, to an individual.
	• Other personal information collected to provide a health service
	• Other personal information about an individual collected in connection with the donation of an individual's body parts, organs or body substances
	• Genetic information that is or could be predictive of the health or a person or their relatives or descendants
	• Healthcare identifiers.

Office	Refers to the Office of Sport.
PPIPA	*Privacy and Personal Information Protection Act 1998* (NSW)
HRIPA	*Health Records and Information Privacy Act 2002* (NSW)
IPPs	*Information Protection Principles* in the PPIPA
HPPs	Health Privacy Principles in the HRIPA
Code	Refers to the Office of Sport Code of Ethics and Conduct policy.
Employees	Any person working in a casual, temporary or permanent capacity in the Office. This includes volunteers, consultants, contractors and any person performing a public official function whose conduct could be investigated by an investigating authority.
Data Breach	An incident in which there has been unauthorised access to, unauthorised disclosure of, or loss of, personal information held by (or on behalf of) Office of Sport or any accidental or unlawful destruction or alteration of personal information held by (or on behalf of) Office of Sport in relation to individuals in the European Union.
Collected	The process of obtaining personal information.

Held	Under section 59C of the PPIPA, personal information is 'held' by a public sector agency if: a) The agency is in possession or control of the information, or b) The information is contained in a state record for which the agency is responsible under the *State Records Act 1998* (NSW).
MNDB	Mandatory Notification of Data Breach scheme under Part 6A of the PPIPA.
Eligible Data Breach	For a data breach to constitute an 'eligible data breach' under the MNDB Scheme there are two tests to be satisfied: 1. There is an unauthorised access to, or unauthorised disclosure of, personal information held by a public sector agency or there is a loss of personal information held by a public sector agency in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of, the information, and 2. A reasonable person would conclude that the access or disclosure of the information would be likely to result in serious harm to an individual to whom the information relates.
Contained	Involves one or more of the following: • Stopping unauthorised practices. • Recovering or limiting dissemination of records without authorisation. • Shutting down compromised systems.
Unauthorised access	Occurs when personal information held by an agency is accessed by someone who is not permitted to do so.
Unauthorised disclosure	When an agency (intentionally or accidentally) discloses personal information in a way that is not permitted by the PPIPA or HRIPA.
EU GDPR	The European Union General Data Protection Regulation. If you are collecting personal or health information from individuals living in the European Union (EU) with an intention of providing goods and services to them, you might be subject to EU's GDPR.
UK GDPR	The United Kingdom General Data Protection Regulation. If you are collecting personal or health information from individuals living in the United Kingdom with an intention of providing goods and services to them, you might be subject to UK's GDPR.

5 Roles and Responsibilities

5.1 Chief Executive

The Chief Executive is responsible for ensuring commitment to the Privacy Management Plan, and its' associated process, is maintained.

5.2 Executive Management

Executive Management is committed to:

- making privacy a standard agenda item in executive meetings,
- reporting on privacy issues in our annual report in line with the *Annual Reports (Departments) Act 1985* (NSW),
- confirming support for privacy compliance in the Code,
- identifying privacy issues when implementing new systems, and
- promoting the Privacy Management Plan as part of induction for new staff.

5.3 Office of Sport Privacy Officer

The Privacy Officer is the Office contact for privacy matters and is responsible for:

- responding to enquiries about how we manage personal and health information,
- responding to requests for access to and amendment of personal or health information,
- providing guidance on broad privacy issues, compliance, and application of the Privacy Management Plan and privacy principles across the Office,
- conducting internal reviews about possible breaches of the PPIPA and HRIPA (unless the subject of the review is the conduct of the Privacy Officer), and
- leading the Response Team for all data breaches, the business unit will manage the response, and EMS will provide advice/assistance only – see Data Breach Response Plan for process for responding to data breaches
- ongoing training and education of staff about their obligations under the PPIPA and HRIPA by:
    - ensuring this Plan remains up to date
    - informing staff of any changes to the Plan
    - conducting or arranging staff training sessions on privacy matters as required

5.4 Our Staff

Under the PPIPA, it is a criminal offence, punishable by up to two years' imprisonment for any employee (or former employee) to intentionally use or disclose any personal information about another person, to which the employee has or had access in the exercise of his or her official functions, except as necessary for the lawful exercise of his or her official functions.

The EMS team is responsible for identifying the proposing the training required to be undertaken by all staff. The People and Culture branch is then responsible for ensuring the training is included in the online induction for all new employees.

6 Personal and health information

6.1 Personal information

Personal information is defined in the PPIPA and is any information or opinions about a person where that person's identity is apparent or can be reasonably ascertained, using moderate steps, including by reference to other information. Personal information can include a person's name, address, family life, sexual preferences, financial information, fingerprints, and photos.

There are a number of exceptions to the definition of personal information. These include:

- information about someone who has been dead for more than 30 years,
- information about someone that is contained in a publicly available publication,
- information about someone that is contained in a public interest disclosure within the meaning of the Public Interest Disclosures Act 1994 or that has been collected in the course of an investigation arising out of a public interest disclosure,
- information or an opinion about a person's suitability for employment as a public sector official, and
- the personal information is not collected by a public sector agency if the information provided to an agency is unsolicited.

Health information is generally excluded from the definition of personal information as it is covered by the HRIPA.

6.2 Health information

Health information is a more specific type of personal information and is defined in the HRIPA.

Health information can include information or an opinion about a person's physical or mental health or disability or the provision of a health service to an individual. Put simply, the meaning of health information is:

- personal information about your health,
- information about a health service already provided, or to be provided, to you,
- any personal information about organ donation,
- genetic information about you or your relatives, and
- healthcare identifiers.

6.3 Relevant Policies

Privacy Management Procedure is an internal document that provides the Office's employees with information on how the principles and aims of the Office's PMP are

integrated into the agency's policies, operating plans, business processes and work practices.

The Code assist us to understand who we are, what the Office stands for and how the Office operates with our colleagues and stakeholders. The Code also outlines employees' responsibilities in protecting privacy in the course of their duties. Employees are required to comply with the Code.

Risk Management Policy and Procedures provides detailed information to support consistent processes for identifying, analysing, treating, responding, monitoring, escalating, recording and reporting on risk. All employees are responsible for managing risk.

Data Breach Policy provides details of the procedures the Office will take in the event of an eligible data breach.

6.4 Why we collect personal and health information

The Office collects and uses personal information to process applications for grants or financial assistance, enrolments in sport and recreation programs, seeking feedback on workshops and programs that we run as well as for dealing with general requests for information or enquiries.

The collection of such information enables us to carry out our business, build up a profile of clients who use our products and services and to remain client focused in the delivery of products and services.

In some instances, where the information is provided in the course of applying for a grant, it is necessary for us to disclose that information to the Minister or Members of Parliament for approval purposes.

Generally, personal information is collected directly from the individual to whom the information relates or from their parent or guardian. There are occasions where it is necessary to collect information from third parties. These occasions may include nominations for awards or enrolment into a program via a third party such as a school or sporting club or organisation. We may collect and update information over the phone, over the internet, in person, in writing (including by email) or through a customer survey.

The Office also collects and uses personal and health information of combatants and industry participants involved in certain combat sports in NSW. The Office does this in the course of providing administrative services to the Combat Sports Authority for the purposes of the operation of the Combat Sports Act 2013 (NSW). The information is held on registers and may be viewed by NSW Police for the purposes of the exercise of their functions under the Combat Sports Act 2013 (NSW).

6.5 Personal and health information held by the Office of Sport

The types of personal and health information the Office holds include:

- records of participants in school, holiday and community programs and activities including:
    - participant details such as age and gender
    - emergency contact details for next of kin, parents or guardians or other appropriate persons
    - medical consent forms (showing allergies, dietary requirements or special needs for accommodation or care)
    - media consent forms and risk waivers for participation in activities
- records of participants in workshops, training or other events, including evaluation feedback
- records of subscriber, mailing and contact lists
- previous records of First Lap voucher program (closed on 30 June 2024)
- previous records of Active Kids program (transferred to Department of Customer Service in February 2024) recipients including:
    - name, e-mail, address and contact phone number
    - date of birth
    - Medicare card or other Australian document identity number (for identity verification purposes)
    - personal details of the specified child in relation to Active Kids Voucher applications, including name, age, school, residential postcode, indigenous status, disability status, language spoken at home, weight, height and activity level
    - provider business details
- correspondence records including:
    - contact details of people who have phoned or written to a business unit
    - details of the nature of their correspondence
    - records of who (if anyone) correspondence referred to
- financial information (including credit card details) for types of payments made for services (such as bookings, venue hire, participation in programs)
- information obtained during investigations, applications or reviews, including names of people involved, contact details, proof of identification
- personal and health information provided in response to an incident at an Office facility, centre or venue
- personal information of employees in personnel files which may include:
    - address, phone number, emergency contact details, tax file number and bank details

    - records of race, sex, marital status, and impairment of employees for equal employment opportunity purposes
    - proof of identity
    - medical assessments, certificates and reports
    - attendance, pay and leave records
    - performance and disciplinary records
    - next of kin
    - education and training
    - family and care arrangements
    - secondary employment
    - conflicts of interest and pecuniary interest disclosures
    - work health and safety records
    - investigation reports
    - outcome of criminal records checks or working with children checks.
- recruitment records when people apply for jobs
- visitors to Office premises
- information obtained when individuals request information, brochures or make general enquiries
- information about individuals and organisations obtained during tender processes
- information about individuals and State Sporting Organisations obtained in the course of seeking feedback on organisational health
- information about individuals obtained in the course of developing and managing business relationships and entering into and maintaining contractual relationships
- information obtained in the course of complaint handling
- information obtained about individuals and organisations during the grant application process
- information (including health information) obtained from combatants and industry participants involved in combat sports for the purposes of registration and determinations etc under the Combat Sports Act 2013 (NSW) (in the course of the Office of Sport providing administrative support to the Combat Sports Authority).

6.6 How we store information

The Office stores information in secure application specific databases in our electronic document and records management system or access-controlled paper-based files. We have taken steps to ensure the protection of personal information from misuse, loss, unauthorised access and modification or disclosure.

The Office also take steps to destroy or de-identify information (including CCTV footage) that we no longer require in accordance with the State Records Act 1988 (NSW).

Where the Office provides services to individuals in the EU or the UK, the Office can take steps required under the relevant GDPR to protect the privacy of those individuals, including when requested, erasure of information. The Office uses secure Cloud Services for the provision of software, platform, and infrastructure. Prior to the deployment of a Cloud service a risk assessment is undertaken in accordance with the requirements of the NSW Government Cloud Policy.

6.7 Use of cookies

Cookies are a small data file from a website that is stored within a web browser that can be retrieved at a later time. Cookies tell a server that users have returned to a particular website. The Office uses cookies to provide our stakeholders with a seamless experience. If you do not wish a website to store cookies there is a simple process in each browser type to turn this feature off.

6.8 Links to other sites

The Office provides links to third party websites to provide as additional information and support to stakeholders. These links may not be under the control of the Office and as such the Office is not responsible for the content and privacy practices employed by these websites. The Office encourages you to read the privacy information and terms and conditions on any other website prior to providing personal information.

6.9 How we ensure privacy integrity

The Office maintains privacy integrity by:

- Implementing and maintaining cyber security.
- Conducting regular audits on data collection, use, storage and sharing.
- Ensuring privacy is contained within all relevant business policies and practices.
- Applying best practice as outlined by the IPC
- Regularly reviewing relevant legislation and the Office's policies and procedures.
- Conducting training sessions for staff that cover:
    - Awareness of Office privacy requirements
    - How to identify a data breach
    - How and who to report data breaches to
    - Outline roles and responsibilities

- Additional training for staff that directly collect, handle & use private information

6.10 Privacy and Health information data breaches

Data can be put at risk by cyberattacks, ransomware, spear phishing, malware, system and process failure, employee mistakes, deliberate misconduct, lost or stolen devices or hard copy files and other risks, such as verbal conversations. Not every information security incident will create a privacy risk; for example, a Denial of Service attack may impact our functions without risking the data we hold. However, when an incident involves the potential exposure of 'personal information', it also becomes a privacy incident and possibly a notifiable 'data breach'.

In 2023 the NSW Government amended the PPIPA to include mandatory data breach reporting, under the Mandatory Notification of Data Breach (MNDB) scheme, by government departments and agencies. The Mandatory Notification of Data Breach (MNDB) scheme also applies to the HRIPA and is administered by the NSW Privacy Commissioner. From 28 November 2023 all NSW government departments and agencies are required to comply with Part 6A – Mandatory notification of data breaches of the PPIPA. Under Part 6A the Office is obligated to:

- assess suspected data breaches to determine whether an eligible data breach has or is likely to have occurred
- undertake steps to contain an eligible data breach
- undertake steps to mitigate the effects of an eligible data breach in order to reduce the risk of serious harm to affected individuals
- notify the Privacy Commissioner that an eligible data breach has occurred
- notify affected individuals that an eligible data breach has occurred
- prepare and publish a data breach policy
- keep and maintain a register of eligible data breaches.

A definition of an eligible data breaches as outlined in Part 6A 59D is provided below:

*(1) For the purposes of this Part, an **eligible data breach** means —*

(a) there is unauthorised access to, or unauthorised disclosure of, personal information held by a public sector agency and a reasonable person would conclude that the access or disclosure of the information would be likely to result in serious harm to an individual to whom the information relates, or

(b) personal information held by a public sector agency is lost in circumstances where —

(i) unauthorised access to, or unauthorised disclosure of, the information is likely to occur, and

(ii) if the unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to an individual to whom the information relates.

*(2) An individual specified in subsection (1)(a) or (1)(b)(ii) is an **affected individual**.*

(3) To avoid doubt, an eligible data breach may include the following —

(a) a data breach that occurs within a public sector agency,
(b) a data breach that occurs between public sector agencies,
(c) a data breach that occurs by an external person or entity accessing data held by a public sector agency without authorisation.

A Privacy Data Breach Response Plan has been developed in line with the MNDB scheme and the Office's IMT *Data Breach Policy* procedures. More information on the MNDB scheme can be found on the NSW Information and Privacy Commission's website: https://www.ipc.nsw.gov.au/privacy/MNDB-scheme

It is all employees, contractors and suppliers' responsibility to report suspected data breaches as soon as possible.

In all cases, employees, contractors and suppliers must report the suspected data breach immediately:

- Either in person or by phone call, to the Office of Sport Privacy Officer: Telephone: 131302 or 02 8754 8796
- You must then confirm your report in writing, by email to: privacy@sport.nsw.gov.au

Once notification has been received the Privacy Officer will follow the procedure as outlined in the Privacy Data Breach Response Plan.

If the data breach contains information from individuals in the EU or UK, the Office must notify the supervisory authority in accordance with the relevant the GDPR.

7 Privacy Principles

Privacy Principles refer to the combination of the Information Protection Principles set out in the PPIPA and the Health Privacy Principles in the HRIPA, which are summarised here as a set of principles.

When developing new services, business processes, online forms or other material or resources, our staff will refer to the Information & Privacy Commission's (IPC) *Privacy for NSW public sector agency staff checklist* (available on www.ipc.nsw.gov.au).

7.1 Information Protection Principles (IPPs)

7.1.1 Collection

- The Office collects personal information only for a lawful purpose that is directly related to our functions and activities.
- The personal information is collected directly from the person concerned unless:
    - they have authorised information to be collected from someone else, or

- the information relates to a person under the age of 16 and has been provided by their parent or guardian

- The Office informs people why their personal information is being collected, what it will be used for, and to whom it will be disclosed. We tell people how they can access and amend their personal information and any possible consequences if they decide not to give their personal information to us.
- The Office ensures that personal information is relevant, accurate, is not excessive and does not unreasonably intrude into the personal affairs of people.
- If you are collecting personal information from people living in the EU or UK with an intention of providing goods and services to them, you might be subject to EU GDPR or UK GDPR in which case you should make sure your collection meets the requirements of Articles 13-14 of the EU GDPR and UK GDPR. This includes if you are collecting information about, and tracking, web-based behaviour, where the behaviour is coming from the EU or UK.

This principle also applies to the installation and use of CCTV surveillance in public places. Refer also to the "NSW Government policy statement and guidelines for the establishment and implementation of closed circuit television (CCTV) in public places".

Combat Sports registration is currently transitioning to a new system which will sit within Licence NSW. The new system and Privacy Collection Notice is expected to go live to the public in early 2025. The new Privacy Collection Notice will be available to the public via a link on the Office webpage.

Following is a list of privacy statements used by the Office:

Appendix A	Office of Sport Privacy Statement
Appendix B	Internet Privacy Statement
Appendix C	Email Marketing Privacy Statement
Appendix D	Centres, Venues & Regions Privacy Statement
Appendix E	Combat Sports Privacy Statements

7.1.2 Storage

- The Office stores personal information securely, keep it no longer than necessary and destroy it appropriately. We protect personal information from unauthorised access, use or disclosure.
- Personal information will be kept for no longer than is reasonably necessary and will be stored, used, retained and disposed of in accordance with the *State Records Act 1998* (NSW) and approved retention and disposal authorities.

7.1.3 Access and accuracy

- The Office is transparent about the personal information we store about people, why we use the information and about the right to access and amend it. We allow people to access their own personal information without unreasonable delay or expense. The Office enables people access to update, correct or amend their personal information where necessary by making a request to the Privacy Officer.
- The Office ensures that personal information is relevant and accurate by confirming the data with the individual prior to using it.

7.1.4 Use

- The Office only uses personal information for the purpose we collected it for unless the person consents to us using it for an unrelated purpose, the other purpose is directly related to the purpose for which the information was collected and if the other purpose is necessary to prevent or lessen serious and imminent threat to the life or health of the individual the personal information relates to.
- If the information you collected and intend to use is subject to the EU GDPR or UK GDPR, make sure that consent for that use (if required) is specific, informed, and freely given. There is a difference between positive opt-in and compulsory acceptance of standard terms and conditions.
- The EU GDPR and UK GDPR permits personal data to be processed if necessary for the purposes of the legitimate interests of the data controller (that is, the entity holding the data) subject to the interests or fundamental rights and freedoms of the data subject (that is, the person to whom that data relates). Similarly, under NSW privacy law, use or disclosure is permissible for a directly related secondary purpose within the reasonable expectations of the data subject.

7.1.5 Disclosure

- The Office only discloses personal information with people's consent unless they were already informed of the disclosure when we collected the personal information.
- The Office does not disclose sensitive personal information without consent, e.g. ethnicity or racial origin, political opinions, religious or philosophical beliefs, health or sexual activities or trade union membership. The Office must not disclose personal information to a person or body outside NSW or to a Commonwealth agency without the person's consent unless a relevant privacy law that applies to the personal information concerned is in force in that jurisdiction or the disclosure is permitted or required by an Act or other law.
- If the information you collected and intend to disclose is subject to the EU GDPR or UK GDPR, make sure that consent for that disclosure (if required) is

specific, informed, and freely given. There is a difference between positive opt-in and compulsory acceptance of standard terms and conditions.

7.1.6 Exemptions to the IPPs

- The Office does not regularly use exemptions. Accordingly on any occasions where an exemption is used, the Office will be clear of its use and our reasons for using it.
- There are limited circumstances when the privacy codes of practice and the public interest directions can modify the IPPs for any NSW public sector agency. Further information on the public interest directions is available on the Information and Privacy Commissioners website www.ipc.nsw.gov.au
- There are limited exceptions to IPPs to enable law enforcement or investigative functions.
- Non-compliance with the IPPs may be expressly or impliedly authorised in other legislation.
- Disclosure may also be authorised or required by a subpoena, warrant or statutory notice to produce.
- In certain circumstances personal information may be exchanged between public sector agencies including for the purposes of dealing with correspondence from a Minister or Member of Parliament. This exemption does not apply to health information.

7.1.7 Public Registers

The Office provides the following information to the public:

- Office of Sports GIPA Disclosure Log
- Successful Grant Recipients
- Register of Contracts Awarded
- Combat Sports Public Register

7.1.8 Offences

It is an offence for the Office to:

- intentionally disclose or use personal information accessed in doing our jobs for an unauthorised purpose
- offer to supply personal information that has been disclosed unlawfully
- hinder the Privacy Commissioner or a member of the Commissioner's staff from doing their job

7.2 Health Privacy Principles (HPPs)

7.2.1 Collection

- The Office collects health information only for a lawful purpose that is directly related to our functions and activities.

- The Office ensures that health information is relevant, accurate, is not excessive and does not unreasonably intrude into the personal affairs of people.
- The Office collects health information directly from the person concerned.
- The Office informs people why their health information is being collected, what it will be used for, and to whom it will be disclosed. We tell people how they can access and amend their health information and any possible consequences if they decide not to give their health information to us.

7.2.2 Storage

- The Office stores health information securely, keep it no longer than necessary and destroy it appropriately.
- The Office protects health information from unauthorised access, use or disclosure.
- The Office uses relevant information management systems, including paper-based filing system, to store private information.

7.2.3 Access and accuracy

- The Office is transparent about the types of health information we store about people, why we use the information and about the right to access and amend it.
- The Office allows people to access their own health information without unreasonable delay or expense.
- The Office allows people to update, correct or amend their health information where necessary.
- The Office makes sure that health information is relevant and accurate before using it.

7.2.4 Use

- The Office only uses health information for the purpose we collected it for unless the person consents to us using it for an unrelated purpose.

7.2.5 Disclosure

- The Office only discloses health information with people's consent unless they were already informed of the disclosure when we collected the health information.

7.2.6 Identifiers and anonymity

- The Office does not use unique identifiers for health information, other than where we need them to carry out our functions – for example, wrist bands allocated to identify participants who have food allergies for the purposes of catering at school camps.
- The HPPs provide for people to stay anonymous where it is lawful and practical. However, we generally collect health information for the purposes of a person participating in a sport and recreation program or combat sport fight

and in those circumstances, it is essential for the relevant health information to be linked to the identifiable participant in case the participant needs medical attention.

7.2.7 Transfers and linkage

- The Office does not usually transfer health information outside of NSW. Where we are using data management and software services provided by organisations with data centres outside of NSW but within Australia, they are subject to either the Privacy Act 1988 (of the Commonwealth) or equivalent Australian state or territory privacy laws or binding policies.
- The Office does not currently use a health records linkage system and do not anticipate using one in the future. The sharing of health care identifiers is subject to the same disclosure rules as other health care information. HPP 11 in Schedule 1 of the HRIPA sets out the principles governing disclosure of health information.
- Any transfers or linkages are done in accordance with the HRIPA, NSW Government Cloud Policy and Data Sharing (Government Sector) Act 2015.
- Additionally, any data sharing involving computerised linkage of health records must comply with HPP. HPP 15 requires expressed patient consent if data sharing involves computerised linkage of health records.

7.2.8 Exemptions to the HPPs

- The Office does not regularly use exemptions, on any occasions where an exemption is used, the Office will be clear of its use and our reasons for using it.
- The secondary purpose exceptions are set out in HPP 10 (use) and HPP 11 (disclosure) of Schedule 1 of the HRIPA and include:
  - The management of health services
  - Law enforcement purposes
  - To lessen or prevent a serious and imminent threat to life, health or safety of the person or another
  - Training or research purposes
  - To locate a missing person
- Exceptions to HPP 10 and 11 only operate in specific circumstances and should only be considered after seeking advice from the Privacy Officer or legal unit before relying on the exceptions within the provisions. The sharing of health care identifiers is subject to the same disclosure rules as other health care information. HPP 11 in Schedule 1 of the HRIPA sets out the principles governing disclosure of health information.
- Health privacy codes of practice and public interest directions can modify the HPPs for any NSW public sector agency. These are available on the Information and Privacy Commissioner's website www.ipc.nsw.gov.au.

7.2.9 Offences

It is an offence for the Office to:

- intentionally disclose or use health information accessed in doing our jobs for anything else other than what we are authorised to do
- offer to supply health information that has been disclosed unlawfully
- attempt to persuade a person to refrain from making or pursuing a request for health information, a complaint to the Privacy Commissioner or the NSW Civil and Administrative Tribunal (NCAT), or an application for internal review under the PPIPA, or to withdraw such a request, complaint or application

8 Other laws that affect how we comply with the IPPs and HPPs

This section contains information about the other laws that affect how we comply with the Information and Health Privacy Principles (IPPs and HPPs).

8.1 Crimes Act 1900

Under this law we must not access or interfere with data in computers or other electronic devices unless we are authorised to do so.

8.2 *Government Information (Public Access) Act 2009* (GIPA Act) and *Government Information (Public Access) Regulation 2009*

Under this law people can apply for access to government information held by the Office. Sometimes this information may include personal or health information which will usually be redacted from the information provided. If a person has applied for access to someone else's personal or health information the Office will consult with affected third parties. If a decision is made to release a third party's personal information, it will not be disclosed until the third party has had the opportunity to seek a review of our decision.

When accessing government information of another NSW public sector agency about a review, the Information Commissioner must not disclose this information if the agency claims that there is an overriding public interest against disclosure.

8.3 *Government Information (Information Commissioner) Act 2009* (GIIC Act)

Under this law the Information Commissioner has the power to access government information held by other NSW public sector agencies for conducting a review, investigation or dealing with a complaint under the GIPA Act and GIIC Act. The Information Commissioner also has the right to enter and inspect any premises of a NSW public sector agency and inspect any record.

This Act also allows the Information Commissioner to provide information to the NSW Ombudsman, the Director of Public Prosecutions, the Independent Commission Against Corruption or the Police Integrity Commission.

8.4 *Independent Commission Against Corruption Act 1988* (ICAC Act)

This Act creates an exception to the PPIPA, whereby the Privacy Commissioner or a member of their staff is permitted to disclose personal information where it relates to proceedings for an offence under the ICAC Act.

Further, the ICAC Act provides that Office staff must not participate in corrupt conduct in the course of their employment, including staff must not misuse information obtained while doing their jobs.

8.5 *Public Interest Disclosures Act 1994* (PID Act)

Under the PID Act people working within a NSW public sector agency can make a public interest disclosure (PID) to the Information Commissioner about a failure to properly fulfil functions under the GIPA Act.

We note that the definition of personal information under the PPIPA excludes information contained in a public interest disclosure. This means that "personal information" received or collected under the PID Act is not subject to the IPPs or HPPs.

Please refer to our Public Interest Disclosure Policy and Procedure.

8.6 *State Records Act 1998* and *State Records Regulation 2010*

This law sets out when we can destroy our records. It also authorises the State Records Authority to establish policies, standards and codes to ensure that NSW public sector agencies manage their records appropriately.

8.7 Mandatory Data Breach Notification Scheme

The Mandatory Data Breach Notification Scheme (MNDB) was implemented in November 2023 and has been established to ensure that all relevant authorities and impacted people are advised of data breaches in the public sector.

8.8 Commonwealth Notifiable Data Breach Scheme

The Commonwealth Notifiable Data Breach Scheme requires the NSW public service to notify the Office of the Australian Information Commissioner when a data breach is covered by the Privacy Act 1988 (Cth). A breach that involves tax file numbers is an example of a breach covered by the Commonwealth act.

9 Strategies for Compliance and Continuous Improvement

The Office is committed to ensuring privacy rights of customers, stakeholders, and employees. The Office has adopted several strategies to ensure best practice principles are implemented to ensure compliance with the PPIA.

9.1 Policies and Procedures

The Office has developed policies, procedures, standards and guidelines to advise and assist employees to ensure that privacy is protected. The polices provide advice, guidance and information on privacy matters relating to:

- Acceptable use of technology
- Dealing private personal and health information
- Information security
- Records management
- Privacy breaches
- Use of social media

The Office's policies and procedures broadly correlate with the 6 principles relating to the processing of personal data from EU and UK citizens, as set out by the EU GDPR and UK GDPR:

- Lawfulness, fairness and transparency in processing
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality.

The Office consistently reviews and updates its policies and procedures when and where necessary to ensure compliance with legislation and best practices.

The Office communicates policies and procedures in a variety of ways, such as news items on the intranet, targeted training, and emails.

9.2 Privacy Awareness

The Office undertakes a range of initiatives to ensure employees and our stakeholders are informed about our privacy practices and obligations under the PPIPA and HRIPA. This awareness program also aids with identifying and mitigating privacy concerns and risks.

9.3 Review and Continuous Improvement

The Office is committed to continually taking advantage of opportunities to improve its privacy protection.

The Office consistently evaluates the effectiveness and appropriateness of our privacy practices, procedures and policies through regular reviews to effectively identify, evaluate and mitigate risks of potential non-compliance.

9.4 Privacy Data Registers

The Office maintains the following registers for awareness, review, management and notification:

- Privacy Information Register: an internal register that compiles the data collection points, use, access, system information, storage and security of all private data.
- Internal Eligible Data Register: the Act and the MNDB scheme requires government agencies to maintain an internal register of eligible data breaches. The aim of this register to allow the Office to track, monitor, analyse and review data breaches.
- Public Data Breach Notification Register: the Act and the MNDB scheme requires government agencies to maintain a public register of data breaches. The register is to include details of breach, mitigation action, notification and advice to impacted people and communication information. This register can be found on the Office's website privacy page.

9.5 Data Sharing

The Data Sharing Act authorises NSW government sector agencies to share data with other NSW government sector agencies for specific purposes in accordance with the PPIPA, HRIPA and any applicable Public Interest Direction or Privacy Code of Practice made under the privacy legislation.

The Act does not authorise data sharing with Australian Government agencies or the agencies of another State or Territory.

9.5.1 Sharing with entities outside the NSW Government sector

When data is requested to be shared from an entity or organisation outside the NSW Government sector, the following process should be used to determine the relevant risks and mitigations prior to a decision to share any data:

- Identify the type of data i.e. government sector data, confidential or commercially sensitive information, personal information, health information
- Identify whether the Office controls the data
- Identify whether you can legally share the data
- Identify the purpose for sharing the data
- Consideration to whether the data is suitable for use in the manner intended by the requesting party
- Document specific risks and mitigations associated with how this data is intended to be used

- Determine whether consent is required from the individuals who are the subject of the information. If the information has not been de-identified and the individuals did not consent to the information sharing at the time of the collection or is being used for a purpose other than that for which it was collected, consent will generally be required. Sections 17-19 and 26 of the PPIPA outline the consent requirements for the use or disclosure of personal information.
- Determine whether the appropriate storage and access controls be maintained
- Determine whether 'sensitive' personal information be safeguarded
- Determine whether the data contain healthcare identifiers or involve linkage of health records

If data will be transferred to an organisation outside of NSW, the Office will comply with requirements under HPP 14 or section 19(2) of the PPIPA.

If personal or health information is being shared for a secondary purpose, it requires to follow the PIPPA or the HRIPA, unless one of the exceptions or exemptions under the PPIPA or HRIPA applies, or a Public Interest Direction or Privacy Code of Practice operates to provide an exemption.

10 Privacy Requirements of Contractors

While the Act and the MNDB Scheme does not generally apply to the private sector as private information is seen to be 'held' by the private sector and not a public sector agency. However, the Act outlines that private information is taken to be 'held' by an agency if they are in 'possession' or 'control' of the private information and as such retains legal or practical power to deal with the personal information.

To ensure protection and integrity of personal information held by the private sector, the Office includes privacy security requirements in its procurement contracts.

11 Public awareness

This plan is publicly available as open access information under the GIPA Act.

We promote public awareness of this plan by:

- writing the plan in plain English
- publishing the plan on our website
- providing hard copies of the plan free of charge on request
- telling people about the plan when we answer questions about how we manage personal and health information

12 Procedure

12.1 How to access and amend personal and health information

People have the right to access personal information we hold about them. They also have the right to amend their own personal or health information we hold, for example if they need to update their contact details.

The Office must provide access to or amend personal or health information without excessive delay or expense. We do not charge any fees to access or amend personal or health information.

As noted, where the Office provides services to individuals in the EU and UK, the Office can also erase personal information of those individuals in compliance with Article 17 of the EU GDPR and UK GDPR.

12.2 Informal request

The Office encourages people wanting to access or amend their own personal or health information to contact us to request it.

People are encouraged to contact the staff member or team managing their information or alternatively using our general contact details.

In some cases, functionality may be available via our online booking system for persons to update or correct their own information (subject to verification of identity requirements).

A person does not need to put an informal request in writing. If necessary, we will ask them to verify their identity or make a formal application instead.

The Office aims to respond to informal requests within **5 working days**. We will tell the person how long the request is likely to take, particularly if it may take longer than first expected.

The person will be contacted to advise the outcome of the request. In some cases, particularly if it is sensitive information, we may ask them to make a formal application.

If a person is unhappy with the outcome of an informal request, they can make a formal application to us.

12.3 Formal application

People also have the right to make a formal application to access or amend personal or health information.

A person does not need to ask informally before making a formal application, and a person can make a formal application if they have already asked informally.

A person can make a formal application to the Office of Sport Privacy Officer by email or post.

The application should:

- include the person's name and contact details (postal address, telephone number and email address if applicable)
- state whether the person is making the application under the PPIPA (personal information) or HRIPA (health information)
- explain what personal or health information the person wants to access or amend
- explain how the person wants to access or amend it.

We aim to respond in writing to formal applications within **20 working days**. We will contact the person to advise how long the request is likely to take, particularly if it may take longer than expected.

If a person thinks we are taking an unreasonable amount of time to respond to an application, they have the right to seek an internal review. Before seeking an internal review, we encourage people to contact our office to ask for an update or timeframe.

12.4 Decision not to give access to or amend personal or health information

If a decision is made not to give access to or amend personal or health information, we will clearly explain our reasons.

If a person disagrees with the outcome of an application, they have the right to seek an internal review.

If the Office and the individual disagree about whether personal information held by the Office is accurate, complete, and up to date, the Office will, at the request of the individual, attach a statement provided by the individual of the amendments requested.

12.5 Limits on accessing or amending other people's information

The Office is restricted from giving people access to someone else's personal and health information. The PPIPA and the HRIPA give people the right to access their own information; they generally do not give people the right to access someone else's information.

Under the PPIPA, a person can give consent to disclose their personal information to someone that would not normally have access to it.

Under the HRIPA, an "authorised representative" can act on behalf of someone else. The HPPs also contain information about other reasons we may be authorised to disclose health information, such as in the event of a serious and imminent threat to the

life, health and safety of the individual, to find a missing person or for compassionate reasons.

If none of the above scenarios are relevant, a third party could also consider making an application for access to government information under the GIPA Act.

12.6 Internal Reviews

People have the right to seek an internal review under PPIPA if they think that the Office has breached the PPIPA or HRIPA relating to their own personal or health information.

The Office encourages people to try to resolve privacy issues informally first before going through the review process or making a complaint, under section 45 of the PPIPA, to the Privacy Commissioner. We recommend individuals contact the Privacy Officer before lodging an internal review to discuss the issue.

It is not possible for someone to seek an internal review for a breach of someone else's privacy unless they are authorised representatives of the other person.

Internal review applications need to be received within **six months** of individuals becoming aware of the breach. In exceptional cases late applications may be considered for internal review.

12.7 Internal Review Process

A person can seek an internal review by filling out the internal review application available on our website (copy at **Appendix F**) and sending it to our Privacy Officer by email, post or in person along with any relevant information.

The Privacy Officer will conduct the internal review unless the internal review is about the conduct of the Privacy Officer. In this case another suitably qualified employee within our office will be appointed to conduct the internal review.

The Privacy Officer aims to:

- acknowledge receipt of an application for internal review within 7 calendar days
- complete an internal review within 60 calendar days.

The Privacy Officer will inform the person of the progress of the internal review, particularly if it is likely to take longer than first expected.

The Privacy Officer will respond to the person in writing within **14 calendar days** of deciding the internal review. This is a requirement under the PPIPA.

If a person disagrees with the outcome of an internal review or is not notified of an outcome within 60 days, they have the right to seek an external review.

12.8 The Privacy Commissioner's role in internal reviews

When an internal review application is received the Office must notify the Privacy Commissioner of the internal review and of the proposed outcome.

The Privacy Commissioner is entitled to make submissions to the Office of their view on the matter.

12.9 External Review Process

A person can seek an external review if they are unhappy with the outcome of an internal review we have conducted or do not receive an outcome within **60 calendar days**.

To seek an external review, a person must apply to the NSW Civil and Administrative Tribunal (NCAT). Generally, a person has **28 calendar days** from the date of the internal review decision to seek an external review. A person must seek an internal review before they have the right to seek an external review.

NCAT has the power to make binding decisions on an external review.

For more information about seeking an external review including current forms and fees, please contact NCAT:

Website: www.ncat.nsw.gov.au
Phone: 1300 006 228
Address: Level 9, John Maddison Tower
86-90 Goulburn St
SYDNEY NSW 2000
PO Box K1026
HAYMARKET NSW 1240

NCAT cannot give legal advice, however the NCAT website has general information about the process it follows and legal representation.

12.10 Other ways to resolve privacy concerns

The Office welcomes the opportunity to discuss any privacy issues you may have. You are encouraged to try to resolve privacy issues with the Office of Sport informally before lodging an internal review.

You can raise your concerns by contacting the Privacy Officer or making a complaint through the Office of Sport's website via the Contact the Office of Sport link.

You may also make a complaint directly to the Privacy Commissioner.

Please keep in mind that you have six months from when you first become aware of the potential breach to seek an internal review. This six-month time frame continues to

apply even if attempts are being made to resolve privacy concerns informally. Please consider this time frame when deciding whether to make a formal request for internal review or continue with informal resolution.

13 Contacting Us

For further information about this plan or the personal and health information we hold, or to raise any concerns please feel free to contact us.

Website: www.sport.nsw.gov.au
Email: privacy@sport.nsw.gov.au
Phone: 131302 or 02 8754 8796
Mail: Locked Bag 1422
SILVERWATER NSW 2128
Address: Level 3, 6B Figtree Drive
SYDNEY OLYMPIC PARK NSW 2127

Information and Privacy Commission Contact

Website: www.ipc.nsw.gov.au
Email: ipcinfo@ipc.nsw.gov.au
Phone: 1800 472 679
Mail: Information & Privacy Commission
GPO Box 7011
SYDNEY NSW 2000
Address: Level 15
McKell Building
2 – 24 Rowson Place
HAYMARKET NSW 2000

Appendix A: Office of Sport Privacy Statement

The personal information you provide is subject to the *Privacy & Personal Information Protection Act 1998* (NSW) (PPIPA). It is being collected by the Office of Sport and will be used and disclosed for the Office of Sport's purposes, or a directly related purpose, unless you consent to another use or disclosure, in emergencies or as otherwise required or authorised by law.

On most occasions, the provision of information to the Office of Sport is voluntary, however in some circumstances it is required by law. If you choose not to provide the requested information, we may not be able to provide certain products or services to you.

Under the PPIPA, you have the right to access your personal information held by the Office of Sport, without excessive delay or expense. You also have the right to have your personal information corrected in certain circumstances (e.g. if it is inaccurate).

The European Union General Data Protection Regulation (GDPR) and United Kingdom (UK) GDPR apply to the personal data of individuals residing in the EU and UK that the Office intends to provide goods and services to.

Should you wish to access or correct your personal information, please specify if you reside in the EU or UK and contact us on:
Email: privacy@sport.nsw.gov.au
Phone: 13 13 02
Post: Locked Bag 1422, SILVERWATER NSW 2128
Address: Level 3, 6B Figtree Drive, SYDNEY OLYMPIC PARK NSW 2127

For more information please read our Privacy Management Plan.

Appendix B: Internet Privacy Statement

This website is maintained by the Office of Sport and this Privacy Statement applies to all the publicly accessible pages located at sport.nsw.gov.au.

The privacy of our website visitors is of utmost importance to us. The purpose of this statement is to let you know what information is collected when you visit the Office of Sport's website and how this information is used.

The Office of Sport does not have any responsibility for the privacy policies or practices of third party sites linked to our site.

If you have any questions about our site, or the application of this privacy statement or a request for access to information held, please contact us.

What information do we collect?

When you look at the pages on our site, our computers automatically record information that identifies, for each page accessed, our computers collect:

- the IP (internet protocol) address of the machine which has accessed it;
- the date and time of your visit to the site;
- the pages accessed and documents downloaded; and
- the type of browser and operating system you have used.

Cookies used by the Office of Sport's website do not collect personal information.

How do we use the information collected?

The Office of Sport may use and publish aggregated information collected from our systems to improve our services, including monitoring to prevent security breaches and for research and development to the extent that the information does not identify individual users.

Personal information you provide to the Office of Sport will only be used for the purpose for which it was provided or as otherwise permitted by privacy legislation. For example, if you choose to provide your name and email address when recording feedback on a webpage for the purpose of receiving a response from the Office of Sport, the information will only be used for that purpose.

The European Union General Data Protection Regulation (GDPR) and United Kingdom (UK) GDPR also apply to our data processing activities in relation to the personal data of individuals located in the EU and UK that the Office intend to provide goods or services to.

Unauthorised and unlawful use of the website

The Office of Sport will collect more extensive information if it identifies unauthorised attempts to interfere with or compromise the security of its website or where it suspects there has been a breach of the laws of New South Wales or the Commonwealth of Australia.

The Office of Sport reserves the right to make disclosures to relevant authorities where the use of its website raises a suspicion that an offence is being or has been committed.

Appendix C Email Marketing Privacy Statement

The Office of Sport uses Swift Digital, an online marketing platform service provider to send and manage emails. In using this service, the company Swift Digital may collect personal information which may contain email addresses and other information to be used for the distribution of email campaigns and other important information.

All information collected using the Swift Digital service is the property of the Office of Sport and is never shared or used by third parties.

Swift Digital maintains your data in compliance with Australia's *Spam Act 2003* (Cth) and Australian Privacy Principles.

All data is maintained within Australia and never leaves Australian jurisdiction. Where stipulated data is encrypted in transit using Secure Sockets Layer (SSL) connections. All data stored via Swift Digital is encrypted at rest.

Should you wish to contact Swift Digital, you can find contact details on the website.

Appendix D: Centres, Venues & Regions Privacy Statement

We may collect personal information from you and/or your child about you and/or your child, including CCTV footage and photographs of you and/or your child while attending a program run at one of our facilities. This may be collected over the internet, over the phone, in person and/or in writing.

The types of personal information that we collect about you and/or your child will depend on our relationship with you and the circumstances of the collection. This may include:

- You, your child's, emergency contact or carer's contact details;
- You and/or your child's date of birth, gender and Medicare card or Companion Card information;
- Personal and health details of you and/or your child including medical conditions and medications, behavioural issues, dietary and allergy information, disability status, indigenous status and language spoken at home; and
- Banking and/or credit card details.

We collect and uses personal and health information about you and/or your child/children in order to:

- Operate our facilities and facilitate delivery of programs at our facilities;

- Process payment for you and/or your child's participation at a program;
- Carry out market data analysis, prevent or detect fraud or abuses, or enable third parties to carry out functions on our behalf;
- Assess your child's readiness for physical activity/exercise, ability to participate in programs, general welfare and to provide your child the medical treatments as required; and
- Conduct other purposes that are reasonably necessary for the operation, delivery and evaluation of a program.

We may disclose personal information about you and/or your child to:

- Our related entities and affiliates;
- Medical and health care providers who provide services to us;
- Organisations delivering a program at our facilities that you and/or your child have registered for;
- Contracted third party service providers, financial service providers, credit reference agencies or debt collection agencies if you default on payments due or to obtain payment from you; or
- Any specified recipient as required by law.

We are not likely to disclose any personal and health information about your and/or your child to overseas recipients.

With your express approval as part of the registration process, we may also use photographs, sound and film recording of your child for publicity and advertising purposes. If you do not wish for photographs of your child/children to be taken and/or used for the promotion of NSW Government services and initiatives to the media and general public, this must be notified to us in writing.

You are able to request access to personal and health information held by us about you and/or your child and seek correction of such information. Please refer to our Privacy Statement located on our website. You can also refer to the Privacy Statement for information on how to complain about a breach of our obligations under the *Privacy and Personal Information Protection Act 1998* (NSW) and the *Health Records and Information Privacy Act 2002* (NSW) and how we will deal with such a complaint.

The European Union General Data Protection Regulation (GDPR) and United Kingdom (UK) GDPR also apply to our data processing activities in relation to the personal data of individuals located in the EU and UK that the Office intend to provide goods or services to.

If you do not provide the personal and health information requested in the registration form then we may not be able to process your enrolment form, allow you or your child/children to participate in any programs at our facilities or handle your enquiries.

Appendix E: Combat Sports Privacy Statements

COMBAT SPORTS REGISTRATION SYSTEM:

The Office of Sport of Level 3 6B Figtree Drive, Sydney Olympic Park, NSW 2127 will collect and store the information you provide to enable administration of the *Combat Sports Act 2013* (NSW) on behalf of the Combat Sports Authority of NSW (the Authority).

Any information provided by you will be stored on the database and in hard and soft copy files that can only be accessed by you, staff of the Office of Sport, the Authority and other relevant personnel authorised by the Authority, and the NSW Police Force. The information will only be used for the purpose for which it was collected. The information may also be released when required by law including when subject to an order of the court.

COMBATANT REGISTRATION:

The Office of Sport of Level 3 6B Figtree Drive, Sydney Olympic Park, NSW 2127 will collect and store the information you provide to enable administration of the *Combat Sports Act 2013* (NSW), including processing of registration applications, on behalf of the Combat Sports Authority of NSW (the Authority).

Any information provided by you will be stored on the database and in hard and soft copy files that can only be accessed by you, staff of the Office of Sport, the Authority and other relevant personnel authorised by the Authority, and the NSW Police Force. The information will only be used for the purpose for which it was collected. Any information concerning my health will be collected, used and stored in accordance with Health Privacy Principles, the *Health Records and Information Privacy Act 2002* (NSW) and the *Privacy and Personal Information Protection Act 1998* (NSW).

Appendix F: Privacy Internal Review Request Form

SENSITIVE: NSW GOVERNMENT

NSW GOVERNMENT Office of Sport

Privacy Internal Review Request Form	
This is an application for review of conduct under (please tick one) ☐ s53 of the *Privacy and Personal Information Protection Act 1998* (PPIP Act) ☐ s21 of the *Health Records and Information Privacy Act 2002* (HRIP Act)	
YOUR DETAILS	
Name:	
Postal Address:	
Telephone:	
Email:	
COMPLAINT	
What is the specific conduct you are complaining about? *("Conduct" can include an action, decision or inaction by an agency)*	

Please tick which of the following describes your complaint: *(you may tick more than one option).*	☐ collection of my personal or health information ☐ security or storage of my personal or health information ☐ refusal to let me access or find out about my own personal or health information ☐ accuracy or my personal or health information ☐ use of my personal or health information ☐ disclosure of my personal or health information ☐ other ☐ unsure
What date did the conduct occur? *(please be as specific as you can)*	
What date did you first become aware of this conduct?	
What effect did the contact have on you?	

What effect might the conduct have on you in the future?	
What would you like to see the agency do about the conduct? *(eg: an apology, a change in policies or practices, your expenses paid, damages paid to you, training for staff, etc)*	

You need to lodge this application within six months of the date you became aware of the conduct. If you have taken more than six months, please explain why.	
	I understand that this form will be used by the agency to process my request for an internal review. I understand that details of my application will be referred to the Privacy Commissioner in accordance with: section 54(1) of the *Privacy and Personal Information Protection Act*, or section 21 of the *Health Records and Information Privacy Act*, and that the Privacy Commissioner will be kept advised of the progress of the internal review.
Signature:	
Date:	
LODGEMENT OF FORM	
Please e-mail completed forms to: privacy@sport.nsw.gov.au or Post to: Office of Sport Privacy Officer Office of Sport Locked Bag 1422, SILVERWATER NSW 2128	
PLEASE KEEP A COPY OF THIS FORM FOR YOUR RECORDS	NOTE: It is not a requirement under the PPIP Act or the HRIP Act that you complete an application form. This form is designed for your convenience only. However, you must make a written request in some form to the agency for the matter to be a valid internal review.

Appendix G: Information Protection Principles (IPPs)

Collection

Lawful

Only collect personal information for a lawful purpose, which is directly related to the agency's function or activities and necessary for that purpose.

Direct

Only collect personal information directly from the person concerned, unless they have authorised collection from someone else, or if the person is under the age of 16 and the information has been provided by a parent or guardian.

Open

Inform the person you are collecting the information from why you are collecting it, what you will do with it and who else might see it. Tell the person how they can view and correct their personal information, if the information is required by law or voluntary, and any consequences that may apply if they decide not to provide their information.

Relevant

Ensure that the personal information is relevant, accurate, complete, up-to-date and not excessive and that the collection does not unreasonably intrude into the personal affairs of the individual.

Storage

Secure

Store personal information securely, keep it no longer than necessary and dispose of it appropriately. It should also be protected from unauthorised access, use, modification or disclosure.

Access and Accuracy

Transparent

Explain to the person what personal information about them is being stored, why it is being used and any rights they have to access it.

Accessible

Allow people to access their personal information without excessive delay or expense.

Correct

Allow people to update, correct or amend their personal information where necessary.

Use

Accurate

Make sure that the personal information is relevant, accurate, up to date and complete before using it.

Limited

Only use personal information for the purpose it was collected unless the person has given their consent, or the purpose of use is directly related to the purpose for which it was collected, or to prevent or lessen a serious or imminent threat to any person's health or safety.

Disclosure

Restricted

Only disclose personal information with a person's consent or if the person was told at the time that it would be disclosed, if disclosure is directly related to the purpose for which the information was collected and there is no reason to believe the person would object, or the person has been made aware that information of that kind is usually disclosed, or if disclosure is necessary to prevent a serious and imminent threat to any person's health or safety.

Safeguarded

An agency cannot disclose sensitive personal information without a person's consent, for example, information about ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership. It can only disclose sensitive information without consent in order to deal with a serious and imminent threat to any person's health or safety.