Privacy Management Plan

Taronga Conservation Society Australia

February 2024

Table of Contents

1 Introduction

The Taronga Conservation Society Australia ('Taronga') has an obligation to manage personal and health information in line with the *Privacy and Personal Information Protection Act 1998* (PPIP Act) and the *Health Records and Information Privacy Act 2002* (HRIP Act).

This Privacy Management Plan is required under s 33 of the PPIP Act and sets out:

- Taronga's policies and practices to ensure compliance with the PPIP Act and HRIP Act and other relevant privacy legislation
- How these policies and practices are communicated and promoted to Taronga's people (staff, volunteers, contractors etc)
- Procedures for internal review of privacy decisions under Pt 5 of the PPIP Act
- Contact information for privacy enquiries, including how to request access or amendment to personal or health information held by Taronga

2 About Taronga

Taronga operates Taronga Zoo Sydney and Taronga Western Plains Zoo, Dubbo in line with our vision to secure a shared future for wildlife and people.

As set out in the Zoological Parks Board Act 1973 ('ZPB Act'), Taronga's objectives are to:

- conduct programs and research for wildlife conservation and the preservation of endangered species
- conduct public education and awareness programs about species conservation and management
- Offer cultural, recreational and educational visitor experiences to inspire and connect people to wildlife at our two zoos.

In pursuit of these objectives, Taronga carries out a diverse range of activities, including:

- Zoo entry and a range of experiences including animal encounters, high ropes course, pedal boat and venue hire, school holiday programs
- Overnight accommodation at both zoos
- 'Zoo Friends' membership program
- Formal school, tertiary and industry education courses
- Scientific research programs in Australia and overseas
- Major events and concert series
- Retail facilities (car parking, souvenirs and dining)
- Grants programs for conservation projects

- Vet hospitals for injured wildlife
- Customer engagement, competitions and newsletters

Taronga, through the Taronga Foundation, welcomes donations from individuals, trusts, foundations and corporate sponsorships to support the wide range of programs and projects in pursuit of our conservation objectives.

3 Definitions – personal and health information

Personal information and health information are defined in the PIPP Act and HRIP Act.

3.1 What is personal information?

Personal information is defined in section 4 of the PPIP Act as:

'information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion'.

Personal information includes such things as a person's name, address, contact details, photographs, video / audio, fingerprints, body samples or genetic characteristics. Information that does not identify a person on its face may still be personal information if the person's identity can reasonably be ascertained from other sources.

3.1.1 What is not personal information?

There are exceptions to what is considered personal information, set out in s 4 and 4A of the PPIP Act. Information that is not considered personal information under the PPIP Act includes:

- information about an individual that is contained in a publicly available publication (eg a book, newspaper, podcast)
- information about an individual who has been dead for more than 30 years
- information about an individual contained in a public interest disclosure under the *Public Interest Disclosures Act 2022* or that has been collected while dealing with a voluntary public interest disclosure under that Act
- information or an opinion about an individual's suitability for appointment or employment as a public sector official
- information that is 'health information' under the HRIP Act (see below)

3.2 What is health information?

Health information is defined in s 6 of the HRIP Act.

Health information is a specific type of personal information that is information or an opinion about:

- a person's physical or mental health, or disability
- a person's express wishes about the future provision of health services

- a health service provided, or to be provided to a person

Health information includes:

- personal information collected to provide or in providing a health service to an individual
- personal information collected in connection with the donation or intended donation of a person's body substances or organs
- genetic information about a person arising from the provision of a health service, that is predictive of future health of that person or a genetic relative

4 Types of personal and health information held by Taronga

In carrying out our functions and activities, Taronga may hold personal information or health information of individuals.

4.1 Taronga's people

As a statutory body constituted under the ZPB Act, Taronga employs staff in the public service to carry out its functions. In addition, Taronga engages volunteers, contractors and others, including committee members in advisory or consultative roles. Taronga's Board members are appointed by the Minister.

Taronga collects and holds personal and health information of Taronga's people for administrative purposes including payroll, leave management and work, health and safety requirements.

The kinds of personal and health information that may be collected or held include:

Job applicants, employed staff, contractors, volunteers, consultants, advisors, Board members	• Name, contact details (phone, email), address • Qualifications, identity information (eg birth certificate), documents relating to the recruitment process • Date of birth • Images of staff, volunteers, contractors • Next of kin, emergency contact details • Tax file number, bank account and super details, salary • Relevant health information (eg vaccination records, records relating to workers compensation claims, information regarding disability to facilitate workplace adjustments) • Workplace records including performance management and grievance records • Working with Children Check Clearance (if relevant) • Personal information disclosed in line with our Conflict of Interest Policy

4.2 Taronga's guests

Taronga welcomes guests to Taronga Zoo Sydney and TWPZ Dubbo and may hold personal and health information to facilitate guests' visits and ensure the safety and enjoyment of visitors on site.

The kinds of personal and health information that may be collected or held include:

People who interact or engage with Taronga experiences including day guests and zoo program participants, accommodation guests, Zoo Friends members, event ticket holders, Taronga app users, retail customers, users of Taronga guest wi-fi*	• Name, contact details (phone, email), address, postcode • Relevant health information (eg to facilitate dining or accessibility requirements) • For Zoo Friends members - date of birth, interests, preferences and information about use of membership services and benefits, in line with terms of membership • For app users, group memberships, images and app activity (eg interactions and edits) • For users of Taronga guest wi-fi, collection is managed by a third party provider and information collected includes name and postcode

*See Paragraph 4.6.3

4.3 Taronga's supporters

Taronga's core function relates to wildlife conservation in Australia and around the world. Taronga carries out a range of conservation activities including breed and release programs, habitat recovery, scientific research and the rehabilitation and release of injured or orphaned wildlife. Guest experience and community education programs drive public support for our conservation functions, through the Taronga Foundation.

The kinds of personal and health information that may be collected or held include:

People who support Taronga including donors, grant applicants, subscribers to Taronga publications, competition / survey entrants, newsletter subscribers	• Name, contact details (phone, email), address, date of birth • Nature of donation or gift (eg one off donation, recurring) • Participation in Zoo offerings • Supporter survey feedback • Entries into competitions

4.4 Taronga's students

Taronga provides education programs to students from preschool to tertiary level. As a Registered Training Organisation, Taronga offers Certificate courses in wildlife and animal care in NSW and interstate. With partner organisations, Taronga also offers bachelor degrees in wildlife conservation.

The kinds of personal and health information that may be collected or held include:

Taronga Tertiary Institute students, bachelor students, school students, professional training students (eg teacher, vets), interns and workshop	• Name, contact details (phone, email), address • Identity information (if relevant for course requirements) • Relevant health information (eg to facilitate dining or accessibility requirements)

participants	• Emergency contact details, next of kin • Qualifications

4.5 Credit card information

Taronga uses a secure payment gateway to receive and process online credit card payments and donations. Credit card details are encrypted through the payment gateway system.

Where credit card details are provided for a donation or payment in physical form, eg paper form, Taronga uses the payment gateway to securely process the payment. The credit card number is redacted from the physical form, before retention of the record in line with retention requirements under the *State Records Act 1998*.

Credit card transactions conducted on the phone are similarly processed using the payment gateway or Eftpos terminal. Taronga does not make audio recording of credit card details provided over the phone.

4.6 Taronga's website and App

4.6.1 Web browsing information

When using Taronga's website or other online sites operated by Taronga and its contractors, we collect the following information:

- the IP (internet protocol) address or host name eg 123.123.123.12 or xxx.yyy.com.au
- the date and time a person visited the website
- the pages or documents that a person attempted to view or download, and whether those pages or documents were displayed
- the web browser and operating system a person is using
- the previous site a person visited, if they reached our website by clicking on a link
- whether they have previously visited our website (only if they accept cookies – see below for more information about cookies).

No attempts are made to identify anyone browsing Taronga's site. The data is captured so that we can accurately evaluate the quality of the content on the website and make continuous improvements.

The only time our website is able to identify a person is if they have signed in as a registered user and agreed to provide their details. In this case, our website maintains a register of their user details in order to make their return visits to the site (and access to information relevant to their association with us) easier for them.

4.6.2 Cookies

Taronga uses 'cookies' to help us understand our website and provide a more customised service to its visitors,(for example by storing user preferences). A 'cookie' is a small file that is sent to your computer, mobile phone or other electronic device when visiting our website. Cookies can be rejected, however, if so, some parts of our website may not have full functionality.

4.6.3 Taronga App

If you have downloaded the Taronga app onto a device, beacons may be used to collect location data about you whilst you are onsite at Taronga Zoo, Sydney and Taronga Western Plains Zoo Dubbo. This data will allow us to send you notifications about how to find your way around our locations (eg to the closest amenities or shows that are scheduled) and keep you informed of promotions running on site at that time.

4.7 CCTV Cameras

Taronga operates Closed Circuit Television (CCTV) cameras in public areas of both zoos. CCTV assists Taronga to provide a safe environment for people, care for wildlife and protect and monitor assets. CCTV cameras are in public areas and are visible and / or signposted. Taronga manages CCTV footage in line with the Information Privacy Principles set out in this Plan, and relevant legislation such as the *Workplace Surveillance Act 2005*.

5 Managing personal and health information – PPIP Act and HRIP Act privacy principles

Taronga manages personal and health information in line with the Information Protection Principles (IPPs) and the Health Privacy Principles (HPPs) set out in the PPIP Act and HRIP Act respectively. The principles govern how we collect, use, store and disclose personal and health information, and how we ensure it is accessible and correct.

In this Plan, the 12 IPPs are numbered in line with the IPC Fact Sheet – Information Protection Principles. The 15 HPPs are set out in the HRIP Act, Schedule 1.

5.1 Collection of personal and health information

5.1.1 Lawful collection (IPP 1, HPP 1)

Taronga will only collect personal or health information if:

- It is for a lawful purpose that is directly related to our functions or activities, and
- It is reasonably necessary for the purpose collected

In line with Taronga's diverse functions and activities set out in the ZBP Act and summarised in Paragraph 2 above, examples of the purposes for which personal and health information may be collected and used include:

- Facilitation of ticketed entry to zoos and or participation in zoo programs and events
- Administration and management of students undertaking educational courses
- Recruitment and safe management of staff and volunteers
- Market research and fundraising activities in pursuit of our conservation objectives
- Customer experience improvement and planning activities (including surveys, competitions)

5.1.2 Direct collection (IPP 2, HPP 3)

Taronga will only collect personal information directly from the person concerned, except where:

- A person has authorised the collection of personal information from a third party (individual or entity)
- Information about a person under the age of 16 is provided by a parent or guardian
- Collection of personal information other than from the person directly, is otherwise permitted by law, for example, under an exemption in the PPIP Act, HRIP Act or as authorised in other legislation, such as the *Workplace Surveillance Act 2005*, *State Records Act 1998* (See Paragraphs 5.9 and 7)

Information may be collected directly through methods such as:

- Online forms (eg guest entry tickets, donations)
- Verbal contact (eg phone accommodation bookings or venue hire)
- Paper applications or forms
- Online self-service platforms (eg community fundraising platforms, human resources platforms)

Collection of personal information may also occur through:

- Use of surveillance cameras on zoo premises (collection of digital images)
- Use of Cookies providing anonymised information about website usage and trends however this is unlikely to identify an individual – see Paragraph 4.6.2.
- Internal processes generating information from our records (for example, audit logs recording electronic access or services requested)

Collection of personal or health information may also occur through contracted service providers or corporate partners, where a person authorises the transfer of personal information to Taronga at the time of collection. Examples include:

- Event ticketing
- Corporate partner promotions
- Research, analysis or philanthropic business partners

Transfer of information with trusted service providers occurs in line with agreed security conditions.

We will only collect health information about a person from someone else where it is unreasonable or impracticable to collect it from the person concerned.

For example, we may collect health information about a child from a parent or guardian of the child.

See further: IPC Statutory guidelines on the collection of health information from a third party

5.1.3 Open collection - Taronga's obligations when collecting information (IPP 3, HPP 4)

When collecting personal or health information from a person, Taronga takes reasonable steps to advise the person:

- That information is being collected
- The name of the agency (Taronga) that is collecting and holding the information
- The purpose for which the information is collected
- The intended recipients of the information
- Whether the supply of the information is required by law or voluntary, and any consequences if the information is not provided
- How a person can access and amend personal information held by Taronga
- The contact details for Taronga's Privacy Officer

Taronga provides this information in the form of a Privacy Statement at the time the information is collected. Taronga's general Privacy Statement is published on the Taronga website and specific privacy statements are included on web pages, application forms, physical forms, online forms, verbal notices (eg phone scripts) when we collect personal and health information.

If health information is collected from a third party, Taronga will take reasonable steps to ensure the person is generally aware of the notification information above.

5.1.4 Relevant collection (IPP 4, HPP 2)

When collecting personal and health information, Taronga takes reasonable steps to ensure the information is:

- relevant to the purpose for which it was collected
- accurate
- up to date
- complete

Taronga takes reasonable steps, taking into account the purposes for collection, to ensure the collection is not excessive, or unreasonably intrusive on the individual's personal affairs.

Information and privacy management requirements are considered at every stage of the data asset lifecycle, including through privacy impact assessments, project planning templates, information management reviews and active monitoring of customer feedback.

5.2 Secure Storage of personal and health information (IPP 5, HPP 5)

5.2.1 Data Security

Taronga stores business records, including personal and health information in secure digital and physical systems to protect against unauthorised access, use, disclosure, loss and theft of data.

Taronga uses the NSW Cyber Security Policy and ISO AS 27001 as benchmarks and is implementing the 'Essential 8' mitigation strategies for digital security, including multi-factor authentication and user access controls.

Where it is necessary and lawful for Taronga to give personal and health information we hold to a third party (eg. a business partner for the provision of a service), Taronga will take all possible steps to ensure that the information continues to be safeguarded, including through contractual terms or digital mechanisms.

Taronga's Cyber Security Policy supports the ongoing implementation of digital security mitigation strategies.

5.2.2 Secure disposal of personal or health information

Taronga will only hold personal and health information for as long as is necessary for the purposes for which the information may lawfully be used. Taronga manages records in line with the *State Records Act 1998* and adheres to the relevant retention and disposal schedules issued by NSW State Records. Taronga's Records Management Policy and related Procedures supports compliance with the Act.

Personal and health information is disposed of in a secure manner, either through digital or physical means, eg paper shredders for the destruction of physical documents.

5.3 Access and Accuracy (IPPs 6, 7 & 8, HPPs 6, 7 and 8)

5.3.1 Transparent (IPP 6, HPP 6)

Taronga is transparent about the personal and health information we hold, generally, and in relation to individuals. We ensure transparency in a variety of ways, including:

- Maintaining our Privacy Management Plan and Privacy Statements at the point of collection
- Using self-service systems where possible

- Maintaining a process for individuals to seek access to personal or health information held by Taronga (see Paragraph 8 of the Plan).

5.3.2 Accessible and correct (IPP 7 & 8, HPP 7 & 8)

Taronga allows people to access their personal and health information upon application, without unreasonable delay or expense (usually within 20 – 30 working days).

Taronga allows people to update, correct or amend their personal or health information to ensure information we hold is relevant, up to date, complete and not misleading, having regard to the purposes for which it was collected. (See Paragraph 8 – How to access and amend personal and health information.)

5.4 Use of personal and health information

5.4.1 Accurate (IPP 9, HPP 9)

Before using personal or health information, Taronga takes reasonable steps to check it is accurate, up to date, relevant, complete and not misleading.

Taronga ensures accuracy of information through a variety of ways, including:

- Active management of databases
- Checking personal information details at the point of collection
- Ensuring staff, volunteers and guests in multi-year programs advise of changes to health information as they arise
- Explicitly checking accuracy of information before use, if warranted

5.4.2 Limited use (IPP 10, HPP 10)

Taronga may use personal and health information about an individual:

- For the purpose for which it was collected, or a directly related purpose
- Another purpose for which the person has consented
- Another purpose where the use of the information is necessary to prevent or lessen serious or imminent threat to someone's life or health
- Another purpose where otherwise permitted by law (including under statutory exemptions (see Paragraph 5.9)

Taronga will use personal and health information for the purpose for which it was collected, or a directly related purpose, as set out in the Privacy Statement provided at the point of collection, (see Paragraph 5.1.3).

In line with Taronga's diverse functions, examples where Taronga may use personal or health information for the purpose it was collected, or a directly related purpose include, but are not limited to:

- Facilitating suitable and safe services, products and experiences for guests and students
- Notifying guests of a change in upcoming event or visit
- Contacting accommodation guests to check accessibility or dietary requirements
- Promoting upcoming events, programs and campaigns
- Conducting surveys to seek feedback on recent experience, visit or stay
- Conducting data research and analytics (either directly or through a contracted service provider) on usage and trends to inform continual improvement, quality assurance and future marketing and planning decisions
- Administering memberships, subscriptions and applications in line with terms of collection eg Zoo Friends, competition entrants, grant applicants

- Administering functions as an employer including remuneration of staff, administering leave entitlements and work health and safety, (either directly or through trusted system support vendors and partners)
- Conducting audits, including through contracted service provider

Taronga ensures that contracted service providers comply with privacy and data security obligations, including through contractual terms of engagement.

Taronga will seek consent to use personal or health information in a manner that is not directly related to the purpose for which it was collected. Consent will always be voluntary, informed, specific and current. Taronga ensures people can easily withdraw consent relating to a use of their personal or health information (ie 'opt out' or unsubscribe) at any time. (see Paragraph 8 - How to access and amend personal or health information).

The HRIP Act sets out exceptional circumstances where Taronga may use health information for a purpose that is not directly related, and without consent of the person concerned. These circumstances include:

- The use of the health information is necessary to assist in an emergency and it is impracticable or unreasonable to seek the consent of the person concerned
- The use of the health information is necessary to lessen or prevent a serious and imminent threat to the life, health or safety of a person, or a serious threat to public health or safety

5.5 Disclosure of personal and health information (IPP 11 & 12, HPP 11 & 14)

5.5.1 Limited and safeguarded disclosure

Taronga may disclose personal information to another person or body if:

- The disclosure is directly related to the purpose for which the information was collected, and we have no reason to believe that the person concerned would object to the disclosure, or
- The person concerned is likely to be aware, including through the Privacy Statement (see Paragraph 5.1.3), that information of the kind is usually disclosed to such person or body, or
- Taronga reasonably believes that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of a person or
- The disclosure is otherwise permitted by law, including under the exemptions in the PPIP Act. For example, disclosure is permitted if the person expressly consents to the disclosure, or if disclosure is required by a subpoena, search warrant or for law enforcement purposes, (See Paragraphs 5.9 and 7).

The disclosure of certain information attracts additional safeguards – this relates to information about a person's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership of sexual activities (called 'sensitive information' in this Plan). Taronga may only disclose sensitive information to another person or body if the disclosure is necessary to prevent a serious and imminent threat to a person's life or health or statutory exemptions apply, for example the person consents to the disclosure (see Paragraph 5.9)

Generally, Taronga may disclose health information to another person or body if:

- The person concerned has consented to the disclosure of the information, or
- The disclosure is for a purpose that is directly related to the purpose for which it was collected and the person would reasonably expect Taronga to disclose the information for that purpose, or
- The disclosure is necessary to assist in an emergency and it is impracticable or unreasonable to seek the consent of the person concerned.

Taronga does not disclose personal or health information to others, except as outlined in this Plan, the Privacy Statement at the time of collection, or as otherwise permitted by law.

Examples of where Taronga may disclose personal or health information include:

- To a corporate partner if the person has consented or is likely to be aware, including through the privacy statement, that personal information is disclosed to the organisation
- To NSW Police for law enforcement or the purposes of locating a missing person
- To NSW Ambulance staff for the purposes of providing lifesaving medical care to a person
- To our insurer for the purposes of workers compensation
- To the Australian Tax Office for the purposes of taxation administration

Privacy considerations around disclosure of information are included in project planning templates to ensure appropriate planning and notification of proposed disclosures in the development of the Privacy Statement. Privacy impact assessments also address proposed disclosures and are encouraged for new initiatives involving personal or health information. Sensitive information is identified at the time of collection and special care is taken to ensure that the additional restrictions around disclosure are applied.

5.5.2 Disclosure outside NSW

Taronga may disclose personal and health information to a person or body outside NSW (another State, Territory or Commonwealth agency) in certain circumstances including:

- The person concerned consents to the disclosure, or
- Taronga reasonably believes that laws similar to PPIP Act and HRIP Act are in place in the receiving jurisdiction, or the information will otherwise be subject to similar protections (eg by contract), or
- Where the disclosure is for a person's benefit, it is impracticable to obtain the person's consent, and the person would likely consent to the disclosure, if asked, or
- The disclosure is necessary for the performance of a contract between Taronga and a person or the implementation of pre-contractual measures taken in response to the person's request.

Taronga conducts wildlife conservation activities in interstate and international jurisdictions. On occasion, Taronga may disclose personal or health information of people, for example, staff conducting fieldwork, to a body in a jurisdiction outside NSW, to facilitate the effective and safe conduct of conservation projects. In addition, Taronga partners with interstate zoos to offer certificate courses in wildlife conservation. Personal information such as a cohort list, may be disclosed to an interstate partner zoo to facilitate course activities, safety and site management.

Before personal or health information is disclosed to a body in another jurisdiction, Taronga ensures the person has consented to the disclosure, or another of the above circumstances apply to the disclosure, in line with the privacy principles.

5.6 Health identifiers (HPP 12)

An organisation can assign identifiers to individuals if it is reasonably necessary to enable them to carry out their functions efficiently.

Taronga does not currently use identifiers for the purpose of managing health information however identifiers may be used by external medical practitioners who undertake health assessments for pre-employment or for health assessments when Taronga has cause to use them.

5.7 Anonymity (HPP 13)

Wherever it is lawful and practicable, individuals must be given the opportunity to not identify themselves when entering into health-related transactions with or receiving health services from an organisation.

Taronga does not generally provide health services to people. If health services are provided (for example vaccination services to staff and volunteers), Taronga ensures that, if practicable and lawful, persons have the opportunity to not identify themselves when receiving the service.

Where health services or vaccinations are specified as an essential or recommended requirement of a role (eg vaccinations against zoonotic diseases for people working with animals), Taronga considers it is not practicable for a person to maintain anonymity in receiving the vaccination.

5.8 Linkage of health records (HPP 15)

Taronga does not currently use a health records linkage system.

5.9 Exceptions or modifications to the application of IPPs and HPPs

5.9.1 Statutory exceptions in the PPIP Act and HRIP Act

Some or all IPPs and HPPs may not apply in certain circumstances, or to certain information. Exemptions to the application of the privacy principles are set out in the PPIP Act and HRIP Act, including Part 2, Division 3 (PPIP Act) and Part 2 (HRIP Act). Some of the key areas where exceptions may apply to Taronga include:

- Law enforcement, protection of public revenue, investigative purposes and some complaints handling purposes
- Non-compliance with the principles is lawfully authorised or required eg by a subpoena, warrant or other legislation including the *State Records Act 1998*, *Workers Compensation Act 1987*, *Workplace Injury Management and Workers Compensation Act 1998*
- Non-compliance would benefit the individual concerned or the person has consented to Taronga's non-compliance with certain IPPs
- Exchanges of information between public sector agencies for the purposes of responding to Ministerial correspondence or to enable inquires or the auditing of accounts or performance of the agency
- Research or the compilation of statistics (only as specified in Statutory Guidelines on Research – section 27B)
- Emergency situations (eg fire flood, storm, epidemic) as defined in the *State Emergency and Rescue Management Act 1989*
- In relation to health information, to lessen or prevent a serious threat to public health or public safety, or some compassionate reasons in certain circumstances.

Staff must seek advice from the Privacy Officer (see Paragraph 8) before relying on any of these exemptions.

5.9.2 Privacy Codes of Practice / public interest directions

Privacy Codes of Practice or public interest directions made under the PPIP Act may also modify or exempt the application of the principles.

To the extent that Taronga provides education services, Taronga is a 'human services agency' under the Privacy Code of Practice (General) 2003 ('the Code'). The application of the Information Protection Principles may be modified in line with the provisions of Part 4 of the Code, relating to the collection, use and disclosure of personal information between Taronga and other human service agencies.

5.9.3 Memorandums of Understanding

Taronga does not have any Memorandums of Understanding or referral arrangements with other agencies that would affect the management of personal and health information.

5.9.4 Public Registers

A public register is an official list of names, events or transactions that is required to be made available to the public. The PPIP Act and HRIP Act govern how personal and health information is managed in public registers, including modification of the application of IPPs.

Taronga may publish a public notification register in line with s 59P of the PPIP Act, to publicly notify people of information relating to data breaches. The register is published where Taronga is unable to notify, or it is impracticable to notify people affected by the data breach. The register includes specified information relating to the data breach (eg type of data affected, type of breach, recommended actions in response to breach) but does not contain personal information or information that would prejudice Taronga's functions.

If you have any concern about your personal information being included in a public register managed by Taronga, you can contact the relevant business area, if known, or the Privacy Officer at privacy@zoo.nsw.gov.au (see Paragraph 8). Any requests for suppression of information from a public register must be in writing and set out the reasons for the request. A decision to suppress information will consider your rights and interests and the public interest in maintaining public access to the information, in line with legal requirements.

6 Australian Shark Incident Database (ASID)

Taronga administers the Australian Shark Incident Database (formerly the Australian Shark Attack File) in a joint partnership with Flinders University and the NSW Department of Primary Industries. The purpose of the register is to aid research into patterns and trends in shark incidents with a view to predict and avoid future shark / people interactions and develop effective mitigations.

Taronga or partner organisations collect information relating to shark incidents including shark type, location, time, weather conditions and general information about injury, if applicable. Taronga and partner organisations also use publicly available information, for example from media reports, to collect information.

The de-identified information is entered in the Australian Shark Incident Database, which is publicly available for the purposes of research and statistical analysis.

Taronga administers the ASID in line with the IPPs and HPPs above. The de-identified information contained in the ASID is obtained with the consent of the person concerned, or through publicly available sources. Survey participants consent to the public disclosure of the information at the time of collection.

7 Other privacy related laws and Taronga policies

Taronga's management of personal or health information may also be affected or regulated by State or Commonwealth legislation, and implemented through Taronga policies.

7.1 State Records Act 1998

The *State Records Act 1998* sets out the framework for the management of Taronga's records. Retention and destruction schedules issued under the Act specify the mandated minimum retention periods for each particular record class held by Taronga. Taronga's Records Management Policy supports compliance with the Act.

7.2 Government Information (Public Access) Act 2009 ('GIPA Act')

Under the GIPA Act, people to have a right to access government information. Where this includes the personal or health information of others, restrictions may apply to the release of the information. Taronga's Agency Information Guide sets out processes for access to government information.

7.3 Data Sharing (Government Sector) Act 2015

This Act allows the sharing of government data between government agencies and between agencies and the Data Analytics Centre, with safeguarded measures to ensure protection of personal and health information in line with the PIPP Act and HRIP Act.

7.4 Privacy Act 1988 (Commonwealth) and the Privacy (Tax File Number) Rule 2015

The *Privacy Act 1988* has relevance for Taronga in relation to the management of Tax File Numbers. The Privacy (Tax File Number) Rule 2015, issued under the *Privacy Act 1988* regulates how we collect, store, use, dispose of Tax File Numbers and notification requirements in event of a data breach.

Complaints regarding the mishandling of Tax File Numbers may be made to the Office of the Australian Information Commissioner (OAIC).

7.5 Public Interest Disclosures Act 2022 ('PID Act')

The PID Act provides a mechanism for the reporting of suspected serious wrongdoing within Taronga. Reports made in line with the Act are assessed and investigated and the reporter is protected against any detrimental action. Reports under the PID Act can be made about serious wrongdoing including in relation to corrupt conduct, serious maladministration and privacy contraventions. A privacy contravention is a failure, other than a trivial failure, to exercise functions in accordance with the PPIP Act or HRIP Act.

The PID Act also places obligations on Taronga to not disclose the identity of the person who makes a report, except in certain specified circumstances under the PID Act.

Taronga's Public Interest Disclosure Policy supports reporting processes under the PID Act.

7.6 Workplace Surveillance Act 2005

Taronga employs continuous CCTV cameras, physical access controls, computer and application activity logging and monitoring to ensure the safety and security of Taronga's people and assets. Taronga's people are notified of this overt surveillance, including through Taronga's ICT Acceptable Use Policy, induction program, signage and internal messages. Taronga complies with the *Workplace Surveillance Act 2005* in relation to the management of any personal information obtained through workplace surveillance.

7.7 Surveillance Devices Act 2007

The *Surveillance Devices Act 2007* governs the installation and use of surveillance devices, including CCTV cameras as installed at both zoos. Additional provisions may apply to the management of information contained in CCTV footage held by Taronga and Taronga complies with this legislation in addition to the PPIP Act.

7.8 General Data Protection Regulation (EU) ('GDPR')

The GDPR is a law of the European Union relating to the protection and management of personal data of people in the European Union (EU). In some circumstances, the GDPR also applies to the management of the personal data by organisations outside the EU.

Taronga considers the application of the GDPR, which may apply in some circumstances, including where Taronga:

- Offers goods and services specifically to people in the EU, or
- Monitors the behaviour of people in the EU

While Taronga's products are accessible globally through our website, generally, our offers do not directly target a particular group, including people in the EU. The collection and use of personal information through access to our website is set out in Paragraph 4.6.

See Fact sheet - NSW public sector agencies and the GDPR for further information.

7.9 Spam Act 2003 (Cth) and Spam Regulations

Taronga operates in line with the *Spam Act 2003* and will only send commercial electronic messages as permitted under that Act.

8 How to access and amend personal or health information

In most cases, you have the right to access and amend the personal or health information we hold about you.

To request access or seek to update, correct or amend personal or health information held by Taronga, contact the relevant business unit (if known), or the Privacy Officer:

Privacy Officer

Taronga Conservation Society Australia

PO Box 20, Mosman, NSW 2088

Phone: +61 (0)2 9969 2777

Email: privacy@zoo.nsw.gov.au

For some products and services, you may be able to update your personal or health information yourself via a self- service portal.

Personal and health information may be amended if it is inaccurate, irrelevant, not up to date, incomplete and/or misleading. In many cases, Taronga will be able to amend information informally, for example by updating

contact information or preferences. In some cases, a formal request, by email to the Privacy Officer will be necessary, and evidence to support the request will be required.

Taronga will determine whether it is appropriate to amend the personal information we hold, usually within 20-30 working days of receiving a request. If Taronga is not prepared to amend personal information, the reasons will be provided and Taronga may instead attach a statement to the information indicating the requested amendment.

Requests to access personal information can also be requested under the *Government Information (Public Access) Act 2009* (GIPA Act).

9 Review and complaint rights

9.1 Overview

If a person believes that Taronga may have breached their privacy, or have not complied with a request for access or amendment, they can:

- raise an informal complaint
- raise a formal complaint or
- submit an application for internal review of conduct with us.

In each case, the person should contact the relevant business unit, if known, or the Privacy Officer, to discuss their issue in the first instance.

Complaints that involve the unauthorised disclosure or personal or health information will be managed in line with Taronga's Data Breach Policy (see Paragraph 10).

A complaint can also be lodged with the Information and Privacy Commission. The Privacy Commissioner may only make recommendations and does not investigate complaints regarding alleged conduct of public sector agencies where the internal review mechanism is available. The investigative functions may result in an investigation report or conciliation of a complaint. The Privacy Commissioner's functions do not result in binding outcomes.

The contact details for the Information and Privacy Commission are:

Email: ipcinfo@ipc.nsw.gov.au

Phone: 1800 472 679

Address: Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000

Postal: GPO Box 7011, Sydney NSW 2001

9.2 Informal complaint

Informal complaints will be handled in accordance with divisional or business unit guidelines for managing external complaints and allegations, if appropriate. Informal complaints are dealt with by Taronga's officers and there are no formal review rights.

The complaint may also be referred to internal review, if it is considered that it is more appropriate to deal with the complaint through this process.

9.3 Formal complaint

A formal complaint is dealt with by Taronga's officers in the first instance. Under the formal complaints process, a person can have a decision reviewed by the Administrative and Equal Opportunity Division of the NSW Civil and Administrative Tribunal (NCAT). The NCAT can be contacted on 1300 006 228, (see NCAT website for further contact details).

9.4 Internal Review

Under the HRIP Act and PPIP Act, applications for internal review to Taronga:

- Should be lodged within six months of becoming aware of the legal implications/ significance of the alleged conduct (Taronga may also, at its discretion, accept a late application for internal review)
- Should be in writing
- Must have a return address in Australia.

An internal review is conducted by a senior officer who was not substantially involved in the matter being complained about. This officer is responsible for reviewing the action or decision and deciding if it is correct. The NSW Privacy Commissioner has an oversight role in the internal review process, and may make submissions in relation to Taronga's draft findings and recommendations, for consideration in finalising the review. The NSW Privacy Commissioner is also provided with a final report of the review.

If a person is unhappy with the result of an internal review, they can appeal to the NCAT. Appeals may be lodged with the NCAT within 28 days after receiving the report. If Taronga does not complete the internal review within 60 days, then an appeal may be lodged with NCAT within 28 days after the individual was due to receive the report.

Taronga's internal review process is set out in **Appendix 1**. Please contact our Privacy Officer (see Paragraph 8 for contact information) for a copy of the application form for a privacy complaint and internal review. There is no cost to lodge a complaint or request an internal review.

10 Data Breach

Data breaches occur if there is unauthorised access to, or disclosure of, personal or health information held by Taronga, or where personal or health information is lost in circumstances where it is likely that unauthorised access or disclosure of the information may occur.

A data breach may be inadvertent or malicious. A breach may occur internally within Taronga, between Taronga and other organisations, or by an external person or entity accessing Taronga's data without authorisation.

Taronga has a separate Data Breach Policy, which guides Taronga's assessment and management of data breaches. In line with the Data Breach Policy, Taronga notifies eligible data breaches – those which are likely to cause serious harm to the person/s affected – to the IPC and / or affected persons.

Taronga's Data Breach Policy is accessible on the Taronga Website.

11 Offences – corrupt use or disclosure

Taronga's people must manage personal and health information in line with the PPIP Act and the HRIP Act and other relevant laws.

It is a criminal offence, punishable by up to two years' imprisonment, an $11,000 fine (or both), for any person employed or engaged by Taronga (including former employees and contractors) to intentionally use or disclose any personal or health information about another person, to which the employee or contractor has or had access in the exercise of official functions, except in connection with the lawful exercise of official functions.

12 Promoting the Plan

Taronga's Privacy Management Plan guides Taronga's people in managing personal and health information in line with privacy legislation. Taronga's people are encouraged to contact the Privacy Officer with any questions related to privacy and the management of personal and health information.

Taronga ensures transparency, awareness and compliance with the PPIP Act and HRIP Act by:

- Publishing the Privacy Management Plan on Taronga's website
- Containing links to the Plan on public privacy statements and forms
- Maintaining a comprehensive policy framework in support of privacy, including Code of Conduct, Cyber Security, Records Management, Data Breach policies and ensuring they are accessible to Taronga's people by publication on Taronga's intranet / website
- Reporting on privacy issues in the Annual Report
- Providing regular training to Taronga's people about privacy matters, including at induction, management forums and individual training and advice for specific privacy issues
- Promoting a 'privacy by design' approach by encouraging consideration of privacy in all stages of projects or programs (eg inclusion on project templates, checklists, procurement planning)
- Promoting Taronga's privacy management to staff including at Privacy Awareness Week / Month, internal notices
- Facilitating Privacy Impact Assessments for projects or programs that affect privacy
- Regularly reviewing privacy practices and processes for compliance or best practice improvements, including through internal audit
- Providing educational awareness material and fact sheets regarding privacy legislation

13 Accountabilities

Position	**Responsibility**
Chief Executive and Executive	• Oversee development of policies, systems and procedures for all aspects of privacy management • Ensure information and privacy risks are identified and managed in line with Taronga's risk management process • Make the Privacy Management Plan publicly available on the Taronga website. • Ensure privacy obligations are included in Taronga's induction program

	• Identify, assess and respond to data breaches in line with Taronga's Data Breach Policy
Director, Information Technology	• Implement and monitor data security in Taronga's systems and processes, including the Essential 8 processes
Manager, Governance and Risk / Privacy Officer	• Prepare, maintain and review the Privacy Management Plan every three years, or in the event of changes to Taronga's internal or external context • Support and monitor compliance with privacy legislation and this Plan • Report on privacy issues in the annual report • Advise and assist Taronga's people in relation to privacy matters including privacy statements and privacy impact assessments • Advise and assist Taronga's people and the public in responding to requests for information or privacy complaints • Support the Plan through awareness-building, skills development, procedures and user training • Coordinate internal review process if required
All Taronga's people (including staff, volunteers, contractors)	• Apply the Information Protection Principles and Health Privacy Principles in all business activities and projects • Identify and manage data and privacy risks in line with Taronga's risk management process • Complete privacy training at induction and regular formal and informal awareness programs • Consider privacy issues for new projects or reviews at every stage of the data lifecycle • Ensure privacy obligations are addressed in third party contracts • Carry out a Privacy Impact Assessment for new projects or changes where a project or program may have privacy impacts • Identify and report data breaches or suspected data breaches to a Manager or more senior person immediately in line with Data Breach Policy

14 Version Control

Version Control	Date Effective	Approved By	Amendment
1.1	20 November 2020	CEO / Executive (following feedback by NSW Privacy Commissioner)	

1.2	February 2024	CE / Executive (following feedback from NSW Privacy Commissioner)	Review of Privacy Management Plan, incorporating updates relating to legislative changes including Part 6A PPIP Act (mandatory data breach provisions)

15 Review Date

This Privacy Management Plan will be reviewed in February 2027, or sooner if required due to changes in practice or legal requirements.

16 Approval

Policy Owner	Manager Governance and Risk	**Divisional Director**	Corporate Services and Governance
Approval Authority	CE / Executive	**Approval Date**	February 2024

17 Appendices

Appendix 1: Internal Review Procedures

Appendix 1 – Internal Review Procedures

Any complaint or request for an internal review in relation to a privacy matter is to be forwarded to the Privacy Officer (refer paragraph 8 for contact details).

A senior reviewing officer will be allocated and will:

Step 1: Assess the application to confirm that:

- it is about personal information in relation to conduct that occurred after 1 July 2000, or
- it is about health information in relation to conduct which occurred after 1 September 2004, and
- it has been lodged within 6 months of the applicant becoming aware of the legal implications or significance of the alleged conduct.

If the application does not meet these criteria it may be referred to relevant managers for handling under relevant complaint handling procedures instead.

Taronga may, its discretion, accept a late application for internal review. Reasons for not accepting a late application must be communicated to the applicant and the applicant advised how their complaint will be handled instead, as well as their right to complain to the Privacy Commissioner.

If the criteria are met, the reviewing officer will proceed with the following steps.

Step 2: Write to the applicant within 14 days of receiving the application stating:

- the officer's understanding of the conduct complained about
- the officers understanding of the privacy principle/s at issue
- that an internal review under the NSW *Privacy and Personal Information Protection Act 1998* and/or the *NSW Health Records and Information Privacy Act 2002*, as appropriate, is being conducted
- the reviewing officer's name, title and contact details
- how, or just that, the reviewing officer is independent of the person/s responsible for the alleged conduct (more detail can be provided in the review report)
- the estimated completion date for the review process
- that if the review is not completed within 60 days of the date the application for review was received, the applicant can go to the Administrative and Equal Opportunity Division of the NSW Civil and Administrative Tribunal (NCAT) for an external review of the alleged conduct
- that a copy of the letter will be provided to the Privacy Commissioner who has an oversight role.

Step 3: Send a copy of the above letter to the Privacy Commissioner.

Step 4: Review the situation to determine whether the conduct occurred, and if so whether it constituted an unauthorised breach of the relevant privacy legislation.

Step 5: Should the review not be finalised within four weeks of the issuing of the letters at steps 2 and 3 above,

send a progress report to the applicant, copied to the Privacy Commissioner:

- detailing progress to date
- advising of any anticipated delays, the reasons for these, and a revised estimated completion date for the review process
- a reminder that if the review is not completed by this new date (which is likely later than 60 days of the date the application for review was received), the applicant can go to NCAT for an external review of the alleged conduct.

Step 6: On completion of the review, write a draft report:

- detailing the review findings about the facts of the matter, the law and the reviewer's interpretation of the law
- setting out a determination as to whether a breach has occurred, with one of the following findings:
- insufficient evidence to suggest alleged conduct occurred
- alleged conduct occurred but complied with the privacy/health privacy principles and/or public register provisions
- alleged conduct occurred, but the non-compliance was authorised by an exemption, Code or Direction (s.41 of PPIP Act / s.62 of HRIP Act)
- alleged conducted occurred: conduct did not comply with principles or public register provisions and was not authorised, so constitutes a "breach" of the legislation
- making recommendations on appropriate action by way of response or remedy (this may include an apology, changing agency processes, providing training to relevant staff, etc.).

Step 7: Provide a copy of the draft report to the Privacy Commissioner for comment, and check whether the Commissioner wishes to make a submission

Step 8: Finalise the report, taking into consideration any comments or recommendations provided by the Privacy Commissioner, and submit for endorsement by the relevant senior officer (Chief Executive Officer or the Divisional Director, Corporate Services and Governance as their delegate).

Step 9: Notify the complainant and the Privacy Commissioner in writing: that the review is finished; of the review findings (and the reasons and legislative basis for those findings), and any action proposed to be taken; and of the right to apply within 28 days to the Administrative and Equal Opportunity Division of the NSW Civil and Administrative Tribunal (NCAT) for a further review, providing contact details for the NCAT.