Privacy Management Plan

Taronga Conservation Society Australia

27 May 2020

Table of Contents

1 Summary

This Privacy Management Plan outlines the measures Taronga Conservation Society Australia (Taronga) takes to comply with the NSW *Privacy and Personal Information Protection Act 1998* (PPIPA) and the NSW *Health Records and Information Privacy Act 2002* (HRIPA) to protect the privacy of its people, students, guests, donors, digital community and others about whom Taronga holds personal and health information.

This Plan has been prepared and implemented as required under section 33 of the PPIPA. Taronga may amend this Plan from time to time, as required, by changes in legislation, processes, procedures or other events.

It describes how a person can request access to and amendment of their personal and health information, held by Taronga and how Taronga conducts an internal review or handles a complaint under the PPIPA or the HRIPA.

2 Introduction

Taronga takes the privacy of its people, students, guests, donors and digital community seriously. This Privacy Management Plan (PMP) has been developed as a reference and guidance tool for the management and protection of personal and health information held by Taronga. It gives effect to the principles detailed in the PPIPA and HRIPA on how `to collect, store, access, amend, use and disclose personal and health information. The PPIPA covers personal information other than health information and requires us to comply with 12 information protection principles (IPPs). Health information includes information about a person's disability and health/disability services provided to them. There are 15 health privacy principles (HPPs) with which we must also comply.

As required, activity specific policies and procedures will be developed to operationalise the PMP. Such policies, guidelines and procedures will be informed by and subsidiary to this PMP.

3 Objectives

The objectives of the plan are to:

- detail Taronga's commitment to protecting the privacy of our staff, students, guests, donors, digital community and others about whom Taronga holds personal and health information
- inform Taronga staff about how to manage and protect personal and health information
- describe how a person can request access to and/or amendment of their personal or health information held by Taronga
- integrate the IPPs and HPPs into existing and future policies, guidelines and procedures that address information issues
- set complaint handling and internal review procedures

- describe how to request an internal review
- explain the right and process of applying to the NSW Civil and Administrative Tribunal, in cases where a person remains dissatisfied with internal review findings.

4 Scope and application

This Plan applies to '**personal information'**, which in all applicable instances includes health information, unless otherwise specified. Personal information and health information are defined in Section 5. Taronga has a range of functions requiring or involving the collection and use of personal information. These are outlined at Appendix 3.

This plan applies to all staff engaged by Taronga, whether by permanent appointment (ongoing), temporary appointment, seconded from another agency, on work experience, volunteer work or as contractors.

This plan applies to:

- For the IPPs, personal information collected since 1 July 2000; and
- For the HPPs, health information collected since 1 September 2004.

5 Definitions

Personal information is defined in section 4 of the PPIPA as:

'information or an opinion about an individual whose identity is apparent or can be reasonably ascertained from the information or opinion'.

Personal information is information that identifies a person and could be:

- a written record which may include a person's name, address and other details about a person
- electronic records, photographs, images, video or audio footage and maps
- biometric information such as fingerprints, blood, and records of genetic material.

The PPIPA excludes certain types of information. The most significant exemptions are:

- information contained in publicly available publications
- information about a person's suitability for public sector employment
- information about people who have been dead for more than 30 years
- a number of exemptions relating to law enforcement investigations
- matters arising out of a Royal Commission or Special Commission of Inquiry
- matters contained in Cabinet documents.

Health information is defined in Section 6 of the HRIPA as:

i) personal information or an opinion about

- *the physical or mental health or a disability (at any time) of an individual*
- *an individual's express wishes about the future provision of health services to him or her*
- *a health service provided, or to be provided, to an individual.*

or

ii) other personal information collected

- *relating to provision of a health service*
- *in connection with the donation of an individual's body parts, organs or body substances*
- *about genetic information pertaining to an individual arising from health service provisions that could potentially predict the health of the individual or his/her relative.*

6 Information protection principles (IPPs)

The 12 Information Protection Principles (IPPs) in the PPIPA establish the legal obligations and standards for collecting and dealing with personal information to minimise the risk of misuse of that information. These IPPs relate to each stage in the personal information management cycle: collection, storage, access, amendment, use, disclosure and destruction when information is no longer required for the purpose for which it was collected.

The degree of sensitivity of the personal information will influence the way in which the IPPs are applied. The more sensitive the nature of the information, the higher level of care that should be used by staff when dealing with such information, particularly where disclosure to a third party is being considered.

6.1 Collecting personal information (IPPs 1-4)

We collect personal information only for a lawful purpose that is directly related to our work, and is reasonably necessary for that work. There are a number of ways that this is collected:

- Provided through direct actions that a person is fully aware of. For example, registering on our website, applying for a licence or informing us of an allegation, complaint or issue. A person may also pay by credit card for a service, take a test or respond to questions or surveys. Information provided to us, is usually with the person's knowledge. It is our preferred way to collect personal information.
- Observed information that may be recorded in our records, as relevant to information provided. This could include details from online cookies or CCTV footage in public places (if combined with facial recognition).

- Derived data which is mechanically collected, such as the number of times a website is visited, how often a service is requested or some other arithmetic process used on current data to predict future required services.
- Inferred data, for example, where statistical information is based on current personal information held by us. For example, it could include response scores, number of services requested, or in some project where big data is being used to generate insights into future needs.

Of the four methods of collection above, a person may only be aware of the first one, where information has been provided by them. A person may also be aware of observed information and derived data. However, it is unlikely that they would know about the inferred information and it is likely that inferred information would be so de-identified, it would be impossible to specifically identify them.

All of the above methods of collecting data are possible, but may not all be used by Taronga. They are included in this plan to make individuals and Taronga staff aware of the way that information may be collected and as a reminder to us to be careful to manage such information properly.

Taronga takes reasonable steps to ensure that personal information we hold:

- is relevant to the purpose we have collected it for
- is not excessive
- is accurate, up-to-date and complete
- does not unreasonably intrude into the individual's personal affairs.

We only collect personal information directly from a person, unless the person has authorised someone else to give it to us; or, if the person is under 16 years of age, the parent or guardian has provided it.

Some exceptions are in place to authorise public sector agencies to collect information from another public sector agency. These are outlined in Section 8 of this Plan.

When collecting personal information, we explain:

- that personal information is being captured and the manner in which it is being collected
- why we are collecting the information
- the intended user/s and/or recipients of the information
- that personal information will not be disclosed or transferred without consent (unless otherwise lawfully authorised to do so)
- whether there is a legal requirement to give us the information, and what the consequences will be if the information is not provided. If there is no legal requirement, that the information is being collected voluntarily
- that a person has the right to access, modify and suppress their personal information.

In most cases we meet these requirements by including a privacy statement and seeking consent. Refer Section 11 for details.

Staff members (including managing contractors and consultants) responsible for designing forms, surveys or questionnaires, in web-based transactions or other instruments, ensure that they include adequate advice about our privacy management procedures and our contact details.

Where appropriate, a Privacy Impact Assessment is conducted prior to the collection of personal information (refer Section 12 and Appendix 2 for details).

6.2 Storing personal information (IPP 5)

Each of our business units apply appropriate security to protect personal information. The security of information extends to all stages of the information life cycle, from the time of creation, while it is actively used, to archiving and destruction.

We have an ICT policy, use passwords and, where possible, encrypt information to ensure it is protected and kept secure. All staff must comply with the Code of Conduct and are provided with training on privacy.

We do not keep personal information any longer than is necessary. Once personal information is no longer required, our staff ensure it is securely disposed of and protected against misuse.

Taronga's Records Management Policy and the *State Records Act 1998* provide guidance on how to do this. The Retention and Disposal Authority relevant to a particular record will be followed. For example record relating to compensation claims, financial management or industrial relations is kept for a minimum of seven years after action completed.

6.3 Accessing personal information (IPPs 6-7)

If a person wishes to know whether we hold personal information about them, they can contact Taronga's Privacy Officer directly to enquire (contact details below).

Privacy Officer
Taronga Conservation Society Australia, PO Box 20, Mosman, NSW 2088
Phone: +61 (0)2 9969 2777
Email: privacy@zoo.nsw.gov.au

We will be able to tell them whether we hold their personal information, the nature of the personal information we hold and the main purposes for which the personal information is used.

If a person wishes to gain access to their personal information held by us, they can request access to it. Access will be provided without excessive delay or expense, usually within 20-30 working days, of receiving a request. If

there is likely to be a delay in providing the information, Taronga will explain the delay and advise when the information is likely to be available.

If Taronga refuses a request to access personal information under the PPIPA, we will provide detailed reasons. Alternatively, access to personal information can be requested under the *Government Information (Public Access) Act 2009* (GIPA Act).

Section 5 of the PPIPA and section 22 of the HRIPA states that nothing in the PPIPA or HRIPA affects the operation of the GIPA Act. This means that the PPIPA and the HRIPA do not override the GIPA Act or lessen any of our obligations under the GIPA Act.

6.4 Amending personal information (IPP 8)

If a person believes their personal information held by us is inaccurate, irrelevant, not up to date, incomplete and/or misleading, they can request that it be amended. Requests should be submitted to the relevant business unit, if known, or the Privacy Officer (refer Section 8.3 for contact details).

A person needs to demonstrate that the information they want amended is in fact inaccurate, irrelevant, not up to date, incomplete and/or misleading. Some kind of evidence will need to be provided to support this claim.

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.

If the request for amendment is denied, the person has the right to an internal review under the PPIPA. Refer section 13 of this plan for information about Taronga's complaints and internal review processes.

6.5 Using personal information (IPPs 9-10)

Before use, Taronga ensures that personal information is accurate, up-to-date, relevant, complete and not misleading. This means that if some time has passed since the information was collected, or there is any other reason to have concerns about the adequacy of the information, Taronga will take reasonable steps to check that it is still accurate, up-to-date, relevant, complete and not misleading.

Taronga only uses personal information for the purposes for which it was collected. If there is a need to use the information for another purpose, Taronga is required to ask for the person's consent. Consent is only genuine if a person has the capacity to give or withhold consent. For consent to be valid it must be voluntary, informed, specific and current. One exception to this is where the information is used to prevent danger to someone or in other specific situations set out in the PPIPA and outlined in Section 8 of this Plan.

To help protect against the risk of identity theft, personal information used in post, fax or email correspondence is kept to a minimum.

Information made digitally available, to conform with open government principles, or otherwise, to make information available, will be de-identified, anonymised or redacted to remove any personal identifying information of individuals.

6.6 Disclosing personal information (IPPs 11-12)

Taronga can disclose personal information to other parties for another purpose, other than the purpose the information was collected for, only if:

- the owner of the personal information agrees; or
- the owner of the personal information is aware that this sort of information is usually disclosed in the way it is being disclosed; or
- the secondary purpose is directly related to the purpose for which it was first collected; or
- information is supplied by Taronga to prevent danger to someone.

This means that Taronga staff do not provide personal information to a third party without the person's consent, or in other specific situations set out in the PPIPA (refer Section 8 of this Plan).

Taronga does not disclose information relating to a person's ethnic or racial origin, political opinions, religious or philosophical beliefs or trade union membership, except to prevent death or injury.

Taronga does not give personal information to anyone outside NSW unless there are similar privacy laws in that person's state or country or the disclosure is allowed under a privacy code of practice, or under legislation (such as HRIPA and PPIPA). This includes the disclosure of information if the disclosure will benefit the individual, it is impracticable to obtain the individual's consent, and if Taronga could obtain the individual's consent it is likely they would give it. Before any personal information is disclosed outside of NSW, Taronga makes enquiries with the recipient to ensure they have similar privacy laws. Taronga will draw up a contract that meets the requirements of section 19(2) of the PPIPA and may also seek legal advice.

7 Health privacy principles (HPPs)

The HRIPA applies to the protection of health information that is held by Taronga. It enables a person to access their own health information. There are 15 Health Privacy Principles (HPPs) listed in the HRIPA and summarised below.

7.1 Collecting health information (HPPs 1-4)

Taronga collects health information only for a lawful purpose that is directly related to our work, and is reasonably necessary to carry out our functions. The information is collected directly from a person unless it is unreasonable or impracticable to do so. When we collect health information, we refer to the principles for the collection of personal information outlined above for IPPs 1-4.

Where appropriate, a Privacy Impact Assessment is conducted prior to the collection of personal information (refer Section 12 and Appendix 2 for details).

If health information is collected from someone else, we ensure that the person is made aware of this fact and has given their consent. The only time we do not follow these principles, is if making a person aware would:

- pose a serious threat to the life or health of any individual, or
- the collection is made in accordance with guidelines issued by the Privacy Commissioner, or
- the HRIPA or other legislation provides an exemption.

7.2 Storing health information (HPP 5)

Taronga divisions and business units apply appropriate security to protect health information that they hold. The security of information extends to all stages of the information life cycle, from the time of creation, while it is actively used, to archiving and destruction.

The storing of personal information is informed by the following key principles:

- records are managed in accordance with best practice in electronic and paper records management and the *State Records Act 1998* (NSW)
- information is kept for only as long as it is necessary, and
- information is destroyed in a secure manner when no longer required (for example, using a secure document destruction service).

7.3 Accessing health information (HPPs 6-7)

If a person wishes to know whether we hold health information about them, they can contact the Privacy Officer directly to enquire (refer Section 6.3 for contact information)Taronga will be able to tell them whether we hold their health information, the nature of the health information we hold and the main purposes for which the health information is used.

A person can also request access to their own health information held by us by contacting the Privacy Officer. Access will be provided without excessive delay, usually within 20 days and never longer than 45 days. If there

is likely to be a delay in providing the information, Taronga will explain the delay and advise when the information is likely to be available. A fee may be charged for providing a copy of health information.

If Taronga's refuses a request from a person to access their health information, detailed reasons will be provided. Alternatively, access to health information can be requested under the GIPA Act.

7.4 Amending health information (HPP 8)

If a person believes that the health information held by us is inaccurate, irrelevant, not up to date, incomplete and/or misleading, they can make a request to the Privacy Officer that it be amended (refer Section 6.3 for contact details). The person will need to provide evidence of their identity with their request for amendment, as well as details supporting that the information they want amended is in fact inaccurate, irrelevant, not up to date, incomplete an d/or misleading.

Taronga is required to determine whether it is appropriate to amend the health information we hold within 45 days of receiving a request. If Taronga is not prepared to amend the health information, the reasons will be provided and we may instead attach a notation to the information indicating the amendment that has been sought.

If a request for amendment is denied, the person has the right of internal review under the HRIPA. See section 15 of this plan about complaints and internal reviews.

7.5 Using health information (HPPs 9-10)

Before use, we ensure that health information is accurate, up-to-date, relevant, complete and not misleading. This means that if some time has passed since the information was collected, or there is any other reason to have concerns about the adequacy of the information, we will take reasonable steps to check that it is still accurate, up-to-date, relevant, complete and not misleading.

We only use health information for the purposes for which it was collected. If there is a need to use the information for another purpose, the person's consent is obtained. One exception to this, is where the information is used to prevent danger to someone or in other specific situations set out in the HRIPA (refer Section 8 of this Plan).

7.6 Disclosing health information (HPP 11, 14, 15)

Taronga can only disclose health information to other parties for another purpose, other than the purpose the information was collected, if:

- the owner of the health information agrees; or
- the secondary purpose is directly related to the purpose for which it was first collected; or

- information is supplied by us to prevent danger to someone; or
- the secondary purpose is reasonably necessary for the funding, management, planning or evaluation of health services or for training, research or for other reasons set out in the HRIPA; or
- the exceptions set out in the HRIPA are established (refer Section 8 for details).

Further restrictions apply to the provision of health information to another person or body who is in a jurisdiction outside New South Wales or to a Commonwealth agency. Taronga adheres to these requirements as detailed in HPP14.

Restrictions also apply to the inclusion of health information or health identifiers in a health linkage system unless express consent has been given for the information to be included. However there may be times when we are lawfully authorised not to comply with HPP15, or where non-compliance is otherwise permitted under an Act or any other law, or the use complies with HPP 10(1)(f) and the disclosure complies with HPP 11(1)(f).

7.7 Identifiers (HPP 12)

Taronga can assign identifiers to individuals if it is reasonably necessary to enable us to carry out our functions efficiently. This identifier can in certain circumstances be adopted by a private sector person to carry out certain functions. The use and disclosure of an identifier can also be done if the owner of the health information has consented to it.

7.8 Anonymity (HPP 13)

Where it is lawful and practicable, an individual will be given an opportunity to retain their anonymity when entering into transactions with us.

8 Exceptions to the application of PPIPA and HRIPA

8.1 Public registers

Under the PPIPA, a public register is a register of personal information that is required by law to be, or is made, publicly available or open to public inspection. Information on public registers is only made available for legitimate purposes: that is a purpose relating to the reason the register exists, or of the Act or legislation under which the register is kept.

Taronga does not currently maintain any public registers.

Any person whose personal information is recorded in a register has the right to request that their personal details be suppressed. This is to protect people whose position or occupation requires a high level of personal security or people who have well-founded fears of violence or harm e.g. victims of domestic violence, police informants, judges, and/or senior police officers. If a person wants their personal information that is contained in

a public register suppressed they should contact the Privacy Officer to make an application (refer Section 6.3 for contact details).

8.2 Directions of the Privacy Commissioner

Under section 41 of the PPIPA and section 62 of the HRIPA, the Privacy Commissioner may make a direction to waive or modify the requirement for a public sector agency to comply with an IPP, a HPP or a privacy code of practice.

Agencies can approach the Privacy Commissioner to request a Direction. The general intent is for the Directions to apply temporarily. If a longer term waiver or in the application of an IPP or HPP, then a Code of Practice may be more appropriate.

As of 1 January 2016, some previous Directions have been incorporated into legislation, including the PPIPA. Directions currently in operation are listed on the website of the Privacy Commissioner (www.ipc.nsw.gov.au/public-interest-directions).

8.3 Some exemptions covered by the PPIPA or the HRIPA

Both the PPIPA and the HRIPA provide some specific exemptions from the IPPs and the HPPs.

Some of the exemptions in the PPIPA are listed in sections 22-28 and include:

- law enforcement and related matters (section 23)
- investigative agencies (section 24)
- where lawfully authorised or required (section 25)
- when it would benefit the individual concerned (section 26)
- specific exemptions in relation to ICAC, NSW Police Force, PIC and the NSW Crime Commission (section 27)
- exchanges between public sector agencies (section 27A)
- research (section 27B)
- credit information (section 27C)
- other exemptions (section 28).

The HRIPA also lists certain circumstances in which Taronga is not required to comply with the HPP principles. Some of these include:

- where lawfully authorised or required
- where non-compliance is otherwise permitted under an Act or any other law
- there is a serious threat to health or welfare

- the use for a secondary purpose, such as management of health services, training and/or research will only be done where it is not possible to carry out that purpose using de-identified information and it is not reasonably practicable to seek your consent.
- finding a missing person
- suspected unlawful activity or conduct grounds for disciplinary action.

An individual may also give Taronga consent to not comply with any or some of the IPPs or the HPPs in particular circumstances.

Staff must seek advice from the Privacy Officer (refer Section 6.3 for contact information) before taking any action with respect to the possible application of any of these exemptions.

9 Information Sharing

9.1 Data Analytics Centre

The *Data Sharing (Government Sector) Act 2015* (DSGS Act) was created to promote sharing of information for certain purposes which include allowing the government to carry out data analytics for the purposes of identifying issues and solutions to better develop government policy, program management, and service planning and delivery.

The DSGS Act provides for the expeditious sharing of information with the Data Analytics Centre (DAC), which operates within the Department of Customer Service, or between other government sector agencies. It also provides protections in connection with data sharing and ensures compliance with the requirements of PPIPA and HRIPA for privacy protection.

Taronga is required to ensure that health and/or personal information contained in the data that is shared complies with privacy legislation. We are also obliged to ensure that any confidential and commercial-in-confidence information contained in the data to be shared complies with any contractual or equitable obligations of the data provider concerning how it is dealt with.

Before responding to a request from DAC to provide information, Taronga consults internally with the Privacy Officer (refer Section 6.3 for contact information) to obtain relevant advice. We may also ask the Privacy Commissioner to guide us on the best way to comply with the request for information whilst upholding the IPPs and HPPs.

9.2 Requests for information from other agencies

Taronga may receive a request from another agency, such as NSW Police, the Ombudsman's Office, the Independent Commission Against Corruption or others. When such a request is received Taronga asks for it in writing, on letter-head (or email with adequate details to identify the agency) and for the request to nominate a contact person.

Before releasing information to the other agency, Taronga checks the named legislation relied upon for the provision of information and ensures the request is legitimate. This is often done by contacting the nominated officer by telephone.

If in any doubt as to the legitimacy of the request, Taronga checks internally with the Privacy Officer (refer Section 6.3 for contact information) or contacts the agency that asked for the information.

10 Other privacy related legislation and policies

In addition to the PPIPA and HRIPA, there are other NSW and Australian laws that may affect a person's right to privacy. Key legislation is identified by the Information and Privacy Commission New South Wales and available on its website https://www.ipc.nsw.gov.au/,

Taronga also has a number of policies and procedures that are relevant to privacy and may affect an individual's personal and health information. These documents are listed in Appendix 6 and make reference to this plan to ensure compliance with the PPIPA and the HRIPA.

11 Privacy Impact Assessment

A Privacy Impact Assessment (PIA) may be required to assess any actual or potential effects that an activity, project or proposal may have on personal information held by us. A PIA can also outline ways in which any identified risks can be mitigated and any positive impacts enhanced.

Public consultation and measuring community expectations is an important part of any thorough PIA. A PIA should examine both the positive (privacy-enhancing) and negative (privacy-invasive) impacts, but primarily focus will be on the negative impacts and how to address such risks.

Privacy risks can be avoided or mitigated by carrying out a PIA to:

- ensure a project complies with privacy legislation,
- ensure a project meets community expectations by anticipating and responding to possible privacy concerns,
- make a project less privacy-invasive, and
- make a project more privacy-enhancing.

It may not be possible to eliminate or mitigate every risk, but ultimately a judgement will be made as to whether the public benefit to be derived from the project will outweigh the risk posed to privacy.

To know if a PIA is required, staff should refer to Appendix 2, which sets out a checklist with some simple yes/no questions. If the answer to one of more of those questions is "yes", then a PIA should be seriously considered and advice sought from the Privacy Officer (refer Section 6.3 for contact details).

12 Seeking consent/privacy statement

Taronga is obliged to provide a notification or privacy statement when personal information is collected. If information is to be used for another purpose than what it was collected for, consent is required to be specifically sought.

Consent means 'express consent or implied consent' and should:

- adequately inform a person prior to their giving consent,
- be provided voluntarily,
- be current and specific, and
- take into account their capacity to understand and communicate their consent.

A person can provide express consent either orally or in writing. It may include a handwritten signature, an oral statement, an electronic medium or voice signature.

Implied consent arises where it may be reasonably inferred in the circumstances from a person's conduct. Silence is not consent. If a person does not object to giving consent, it does not mean that they have given consent.

Voluntarily should be understood to mean that there was a genuine opportunity for a person to provide or withhold their consent. Consent is not voluntary where there is duress, coercion or pressure that could overpower a person's will.

Opting out is not an advisable way to seek consent. However, there are times when this is Taronga's most appropriate option. If an opt-out is used, the following factors, where relevant, must be met:

- The opt out option is clearly and prominently presented
- It is likely the information about collection, use or disclosure and opt-out was read (it formed part of a form filled out by the person, for example)
- Information about the implications of not opting out was given
- The opt-out option is freely available and not bundled with other purposes
- It is easy to choose the opt-out, e.g. little or no cost or effort required to do so
- Consequences of failing to opt-out are not serious
- If opting out later, it will appear as if opted out earlier (as far as practicable).

Bundled consent refers to the practice of putting together multiple requests for consent to a wide range of collections, uses and disclosure of personal information, without giving a person the opportunity to choose which collections, uses and disclosures to agree to and which not to. It undermines the voluntary nature of the consent and should not be used in a privacy statement or consent request.

13 Complaints and internal reviews

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, to discuss their issue in the first instance.

A complaint can also be lodged with the Information and Privacy Commission (contact details below). 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.

Information and Privacy Commission

Email | ipcinfo@ipc.nsw.gov.au
Phone | 1800 472 679
Fax | 02 6446 9518
Address | Level 17, 201 Elizabeth Street Sydney 2000
Postal | GPO Box 7011, Sydney NSW 2001

13.1 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 for an internal review to be carried out, if it is considered that a serious breach of privacy has occurred, or that it is more appropriate to deal with the complaint on a formal basis.

13.2 Formal complaint

A formal complaint is dealt with by Taronga's Officers in the first instance however 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.

13.3 Internal review

Under the HRIPA and PPIPA, complaints or applications for internal review to Taronga:

- should be lodged within six months of becoming aware of the legal implications/ significance of the alleged conduct
- should be in writing (a form is available from our website, but is not necessary)
- 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. There is no cost to lodge a complaint or request an internal review. Reviews must be completed within 60 days. Please contact our Privacy Officer (refer Section 6 for contact information) for a copy of the application form for a privacy complaint and internal review.

Taronga's internal review process is set out in Appendix 1. Please note that the Privacy Commissioner may make recommendations in respect of the process.

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.

14 Workplace surveillance

On our sites, cameras, computers or tracking devices may be used to carry out surveillance for a number of purposes which may include surveillance of our employees. When this occurs, the Workplace Surveillance Act 2005 must be complied with.

A member of the public is not affected by this, other than perhaps being captured by the video recordings, tracking or other surveillance in place.

In general, an employer may carry out a wide range of surveillance, as long as employees are properly notified. This is called 'overt surveillance', or surveillance of which everyone is aware.

Surveillance that employees are not properly notified about is automatically regarded as 'covert surveillance' and is generally prohibited by legislation, except for the purpose of establishing whether employees are involved in unlawful activity whilst at work. Covert surveillance can only be done with the authority of a Magistrate.

Recording of private conversations is covered by the Surveillance Devices Act 2007. Legal advice can be sought, internally or externally, by staff, in respect of both workplace surveillance and the recording of private conversations.

If overt surveillance is in place, employees must be given written notice that includes the following items:

1. The kind of surveillance used (e.g. camera, computer, or tracking)

2. How the surveillance will be carried out

3. When it will start

4. Whether it will be continuous or intermittent, and

5. Whether the surveillance will be ongoing or for a specified limited period.

Information or the results collected through overt surveillance, cannot be used or disclosed unless the use or disclosure is:

- Related to the employment of our employees,
- Related to our business activities or functions,
- To a law enforcement agency in relation to an offence,
- Related to civil or criminal proceedings, or
- Reasonably believed necessary to avert an imminent threat of serious violence to persons or substantial damage to property.

A breach of the above restrictions carries a fine. Note that access to the information can be requested by an employee or a person that was captured by the surveillance. Such requests can be made under the PPIPA or the Government Information (Public Access) Act 2009.

15 Breach of privacy/data breach notification

If a data breach is identified, whether serious or not, individuals to whom the information relates will be notified, unless the breach is in relation to information that is not sensitive, poses little to no risk of harm to them, or if it is decided that notification is not required.

A serious data breach is defined as unauthorised access to, unauthorised disclosure of, or loss of, personal information held by us, and as a result, there is a real risk of serious harm to any of the individuals to whom the information relates.

A less serious breach may occur when there is a failure that has caused, or has the potential to cause, unauthorised access to data, such as:

- Accidental loss or theft of classified material data or equipment on which such data is stored (e.g. loss of paper record, laptop, iPad or USB stick)
- Unauthorised use, access to or modification of data or information systems (e.g. sharing of user login details – deliberately or accidentally)
- Compromised user account (e.g. disclosed through phishing)
- Unauthorised disclosure of classified material information (e.g. email sent to incorrect recipient, or posted to incorrect address or addressee, or published on website
- Failed or successful attempts to gain unauthorised access to information
- Equipment failure
- Malware infection

- Disruption to or denial of IT services (where system flooded to break functions).

Data breaches may result in unauthorised collection, use, disclosure or access to personal information. If this happens, we will act quickly to contain the breach, evaluate the risks, consider notifying affected individuals and prevent a repeat.

Notifying individuals can assist in mitigating any damage for those people and reflects positively on Taronga. If the data breach creates a real risk of serious harm to the individual, then they must be notified immediately, or as soon as possible. The Privacy Commissioner should also be notified, if the breach is serious.

16 Promoting the plan

Taronga's employ the following broad strategies to ensure ongoing compliance with the privacy legislation:

- As part of our induction program, new staff are provided with information to raise their awareness and appreciation of the privacy legislation requirements
- Taronga provides refresher and on-the-job training for specialist staff
- Taronga highlights and promotes the Privacy Management Plan during the annual Privacy Awareness Week/ Month
- Where we propose to collect personal information on forms, questionnaires, survey templates, interview sheets, etc., these are reviewed by the responsible managers to ensure compliance with privacy principles
- When existing tools for collecting personal information are updated, managers review them to ensure compliance with privacy principles
- We provide specialist advice internally to staff, relating to the interpretation and practical implementation of the privacy legislation
- The Privacy Management Plan is published and made available to staff and members of the public on Taronga's website
- The Privacy Management Plan is reviewed and updated every three years
- A formal review/ audit of Taronga's compliance with the privacy legislation is also conducted within 3 years of the date of adoption.

17 Accountabilities

All staff have a duty to act in accordance with this plan. Staff are also required to comply with Taronga's Code of Conduct.

If staff feel uncertain as to whether certain conduct may breach their privacy obligations, they should seek advice from the Privacy Officer (refer Section 6.3 for contact information).

17.1 Offences

It is a criminal offence, punishable by up to two years' imprisonment, for any employee (or former employee) of our organisation 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.

Part 8 of the PPIPA and part 8 of the HRIPA provide further details about offences in respect of personal and health information.

Section 308H of the Crimes Act 1900 provides that it is an offence to access or modify computer records for purposes that are not connected with the duties of the person.

17.2 Protection from liability

Part 8 of the PPIPA and part 8 of the HRIPA also provide certain protections from liability where a person has acted in good faith.

17.3 Responsibilities

Positions with significant responsibilities are:

Position	Responsibility
Chief Executive and Executive	• Establish and maintain policies, systems and procedures for all aspects of privacy management relevant to their areas of responsibility. • Ensure mechanisms for responding to critical issues or risks arising are appropriate and effective (e.g. identification of circumstances in which a Privacy Impact Assessment is required; sufficiency of internal review process) • Ensure areas of work that are of inherently higher risk are identified and that preventive strategies are in place. • Make the Privacy Management Plan publicly available on the Taronga website. • Confirm support of privacy compliance requirements in the Code of Conduct.
Managers and supervisors	• Make staff aware of this plan and help them to use it. • Ensure staff are provided with access to privacy training that meets the requirements of their role in collecting and managing personal and health information. • Identify privacy issues when implementing new systems. • Provide feedback regarding the effectiveness of the plan and suitable refinements to the Governance Manager as necessary.

Manager, Governance and Privacy Officer	• Reinforce compliance with privacy legislation. • Report on privacy issues in the annual report. • Advise and assist staff and the public in responding to requests for information. • Support the plan through awareness-building, skills development and user training. • Help staff by providing advice and assistance if clarification regarding the plan is required. • Monitor the effectiveness of the plan and propose suitable refinements where appropriate.

18 Approval

This document (Privacy Management Plan v.1.0) was adopted and approved for submission to the Privacy Commissioner on 27 May 2020 by Taronga's Executive Team. Publication to Taronga's website was also approved.

Appendices

Appendix 1 Internal review procedures
Appendix 2 Privacy Impact Assessment checklist
Appendix 3 Key functions and information collected

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 section 6 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.

A late application may be accepted and the reviewing officer should make a decision about whether to accept it or not. 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 PPIPA / s.62 of HRIPA)
    - 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 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

Appendix 2 Privacy Impact Assessment checklist

A PIA is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals and sets out recommendations for managing, minimising or eliminating that impact. If the answer to one or more of the questions below is yes, then a Privacy Impact Assessment (PIA) should be considered.

Will the project involve?		Yes	No
1	The collection of personal information, compulsorily or otherwise, for a new project or business initiative?		
2	A new use of personal information that is already held?		
7	A new requirement to sight, collect or use existing ID, such as an individual's driver's licence?		
8	The creation of a new identification system, e.g. using a number, or a biometric?		
4	Restricting access by individuals to their own personal information?		
3	A new or changed system of regular disclosure of personal information, whether to another agency, another State, the private sector, or to the public at large?		
9	Linking or matching personal information across or within agencies?		
10	Exchanging or transferring personal information outside NSW?		
5	Amendment to the PPIPA or HRIPA that impacts the collection and management of personal or health information.		
11	Handling personal information for research or statistics, de-identified or otherwise?		
12	Powers of entry, search or seize, or other reasons to touch another individual (e.g. taking a blood or saliva sample)?		
13	Surveillance, tracking or monitoring of individuals' movements, behaviour or communications?		
15	Any other measures that may affect privacy?		

If the above shows a need to carry out a PIA, consider whether a PIA previously conducted is applicable to the circumstances. This may be the case for repeat activities where the collection and management of information is consistent. If a new PIA is needed, contact the Privacy Officer (refer Section 6.3 for contact information).

If a PIA is not needed, it is recommended that a copy of the above questions and any supporting information is saved to file. This helps if privacy issues arise later in the project.

Note: Even if the list above does not indicate the need for a PIA, it may still be advisable to create a short PIA, particularly if the project will change hands several times. A consistent approach to the management of privacy in the project is crucial.

A PIA should include an assessment of the matters outlined below.

Need for a PIA	• Using the above checklist • By addressing the threshold question of whether the collection of personal data is necessary to achieve the project objectives
Scope of the PIA	• Will it cover one product and service or a group of products and services? • Does it relate to a one-off (e.g. research question) or recurring (e.g. membership) collection of personal information
Key stakeholders & consultation requirements	• Who are the stakeholders? • Are consultations required to discuss potential risks and concerns?
Information flows	• Map the data life cycle. • What is collected, how, by whom and here is it going? • What are the security and quality processes around the data? • Map the data against compliance with the IPPs and HPPs and identify gaps.
Privacy impact analysis and compliance check	• After step 5, analyse the gaps. • Identify the risks and where they are coming from. • Identify the data or compliance leakage
Privacy management – addressing risks	• What options will allow you to remove, minimise or mitigate any identified risks? • Are there any changes that would achieve a more appropriate balance between the project's goals, the interests of affected individuals, and the agency's interests? • Are you being transparent enough (privacy notice issued)? • Are any of the identified privacy impacts so significant that the project should not proceed?

On completion of the PIA, a report should be prepared to inform decision-making at Executive or Management level as appropriate.

Appendix 3 Key Functions and Information collected

The type of personal information that Taronga collects will depend on the circumstances of collection and on the type of service requested from Taronga.

Information collected from web browsing

When viewing Taronga's website or, tarongafoundation.com.au, roarandsnore.com.au, zoofari.com.au 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.

Information collected from online forms and services

When a person submits a form on our website, or provides information as part of using an online service, we collect information from the activity. This information may include personal and organisational details such as a person's full name, date of birth, phone number, business name and ACN or ABN details, email address and street address. Examples of online forms and services include:

- purchasing a ticket or Zoo Friends membership (refer below for additional information on the collection and use of personal information about Zoo Friends)
- making an accommodation or program booking (refer below for additional information on accommodation bookings)

- making a donation to the Taronga Foundation or sponsoring an animal
- registering details for a survey, competition, petition, research or any other purpose
- accepting or declining an event invitation

Clicking on the 'submit' button on the form acts as consent for Taronga to collect the information that has been provided.

Information collected from online transactions using credit cards

Online

Transmission of credit card information is via secure, encrypted services. This means that all personal information, including name, address and credit card number, cannot be read and is not held in our systems.

Paper-based

A small number of programs and events require individuals to provide their credit card details on a paper-based form. In these circumstances the information is entered into secure online or EFT systems and the form, or sections of it containing Credit Card information is immediately destroyed. Some other personal information may be retained, if required (e.g. to issue a tax invoice for a donation to the Taronga Foundation; to facilitate participation in an education program).

Information collected from subscription services

Taronga offers subscription services on its website. These services are offered on an 'opt in' basis. A person can opt out at any time by using the unsubscribe button at the foot of each email received or contacting us via unsubscribe@zoo.nsw.gov.au and we will promptly process the request.

When a person subscribes to a newsletter or news alert service from Taronga we will use their personal information in order to provide the content to them. We may also use their personal information to tell them about associated services, public information campaigns or web content we think they might be interested in, but only if they have indicated that they are happy to receive this information.

Information collected from direct correspondence

Taronga handles a high volume of inquiries from the general public. Taronga may collect personal information from a person when they communicate with us directly via email, telephone, written correspondence (letter, fax) or in person. As required, we will record contact information for the purpose of responding to inquiries. Details may also be kept for statistical purposes including the nature of the inquiry to improve service delivery.

As well as collecting personal information directly from a person, there may be occasions when we collect information about a person from a third party. For example, from a person or organisation who are making a donation, purchase or booking on behalf of a person.

Information collected as part of the Zoo Friends Membership program

Additional information is collected by us when a person joins the Zoo Friends membership program. This includes information such as their name and date of birth and the name and date of birth of any additional members, home address, other addresses, email address, telephone numbers, fax number, credit card details as well as any special interests and preferences.

Taronga also keeps a record of Zoo Friends' use of membership services and benefits. This information includes date and time of visit, purchases, events attended and benefits redeemed. The collection of this information assists Taronga to monitor the use of, and improve, the Zoo Friends membership program and benefits.

Information on our Zoo Friends databases is used for additional purposes which members consent to as part of the terms and conditions of membership. This includes Taronga marketing its products and services or the products and services of its partners. Other purposes include improving its customer service by means of research, product development and planning.

Some of the information is deemed mandatory for participation in the Zoo Friends membership program. Members are advised that if all or any of the non-mandatory information is not provided, the services provided by Taronga may be affected.

Zoo Friends members can update their profile information at any time by contacting the Zoo Friends membership office on (02) 9968 2822.

Information collected from Taronga Foundation donors

The Taronga Foundation receives donations from members of the public in support of Taronga's conservation, research and education functions. Information collected from donors may include their name and date of birth, home address, other addresses, email address, telephone numbers, fax number, credit card details (managed as per item 2 above) as well as any special interests that relate to Taronga's activities.

Information collected from grant applicants

The Taronga Foundation administers a number of grant programs including the Taronga Green Grants, Taronga Field Conservation Grants and Taronga HATCH accelerator program. As part of grant applications, personal information is collected including name and date of birth, address, email address and telephone numbers. Study and employment history is also supplied in resumes and referee reports. This is information is mandatory for participation in grant programs and applicants are advised that if all or any of the mandatory information is not provided, their application will not be considered.

Information collected from accommodation guests and program participants

Taronga provides accommodation and runs public programs, including education programs and tours, with the objective of engaging the community in wildlife conservation and raising funds to support its activities. Personal information is collected from accommodation guests and program participants to facilitate their visit and ensure their safety on site at Taronga and Taronga Western Plains Zoos. This includes information such as their name and date of birth and the name and date of birth of any additional participants / guests, home address, other addresses, email address, telephone numbers, credit card details as well as any special requirements or preferences.

Information collected from guests

Except as described above (e.g. information collected from online forms and services) Taronga does not ordinarily collect personal information from guests. However in certain circumstances, for example, a first aid incident involving a guest, Taronga may collect personal information in an incident report. Personal information collected will only be used to communicate directly with the person about the incident. With the person's consent, information may also be provided to legal representatives and/or Taronga's insurer.

Information collected from Taronga personnel

Personnel records are kept on all staff members by the People, Culture and Safety Division in accordance with Taronga policies and procedures and Public Sector Management Act. Staff are aware of the purposes of personnel files. Personnel information is also kept on Board members, volunteers, students completing work placements, internships or work experience with Taronga, consultants and contractors, and students enrolled with the Taronga Training Institute. People seeking employment with Taronga also provide personal information to Taronga which is kept on file for a short period of time, as do potential Board members when vacancies occur.

Information held in personnel records include payroll and recruitment records, sick leave and other leave forms, performance management, grievance, WHS and EEO related matters. Taronga also holds personal information relating to worker's compensation claims.