Kaupapa-here | Privacy Policy

Mō wai me te whānuitanga | Audience and scope

This Policy applies to:

(a) all employees of Te Pūkenga, including contracted staff, consultants and secondees providing services for Te Pūkenga, and those on fixed-term contracts (collectively referred to as Kaimahi in this Policy); and

(b) where appropriate, Ohu Kaitiaki, which extends to all those operating at a governance level, including Council members and members of Council's advisory committees.

Existing privacy policies of Te Pūkenga Business Divisions

An ITP subsidiary that dissolves prior to 31 December 2022 becomes a Te Pūkenga "Business Division". If an ITP subsidiary's privacy procedures and/or data breach response plan were laid out within their Privacy Policy, the successive Business Division may continue to operate under that Policy so long as it is not inconsistent with the principles laid out in this Policy. This is to allow privacy procedures already working well for operational areas to continue uninterrupted, as well as empower each operational area to take accountability and responsibility for privacy matters occurring within their operations.

Application to transitioning ITP subsidiaries

For Te Pūkenga subsidiaries transitioning to Te Pūkenga Business Divisions, this Policy will take effect immediately after an ITP subsidiary has been dissolved.

Contact Details

The name and contact details for the Privacy Officer and Privacy Leads will be notified on Te Pūkenga website. All Business Divisions will also be notified directly of the Privacy Officer's name and contact details.

For present purposes, the Privacy Officer of Te Pūkenga is the Director Legal and Risk.

Mokamoka whakaaetanga | Approval details

Version number	2	**Issue date**	1 June 2022
Version history		*Reason for amendment/s* a) Expanding the Policy to accommodate early movers	
Approval authority	Te Pūkenga Council	**Date of approval**	30 May 2022
Policy sponsor (has authority to make minor amendments)	Director Legal and Risk	**Policy owner**	DCE Operations
Contact person	Sinead Hart	**Date of next review**	1 December 2022

Ngā whakatikatika | Amendment history

Version	Effective date	Created/reviewed by	Reason for review/comment
1	4 August 2021	Sinead Hart	Initial version
2	1 June 2022	Sam Shannon/Sinead Hart	Preparing policy framework to receive early mover ITPs

Ngā Ihirangi | Table of Contents

Kaupapa-here | Privacy Policy

1. Pūtake | Purpose

1.1. The purpose of this Policy is to ensure Te Pūkenga complies fully with its obligations under the Privacy Act 2020 (the **Act**). It is intended to provide high level guidance for both Te Pūkenga head office and Business Divisions when using their respective privacy procedures.

1.2. The purpose of the Act is to promote and protect individual privacy by:

a) providing a framework for protecting an individual's right to privacy of personal information, including the right of an individual to access their personal information, while recognising that other rights and interests may at times also need to be taken in to account; and

b) giving effect to internationally recognised privacy obligations and standards in relation to the privacy of personal information.

1.3. This Policy should be read in conjunction with the relevant Privacy Procedure and data breach response plan.

2. Te Pae Tawhiti | Te Tiriti o Waitangi Excellence Framework

The Council of Te Pūkenga acknowledges that this Policy has been adopted while there is ongoing work being carried out to consider how Te Pae Tawhiti - Te Tiriti o Waitangi Excellence Framework should be fully embedded in the Policy. The Council notes that Te Pūkenga is still on its transition journey and, as it matures, this Policy and others will be reviewed to ensure they align with the new Operating Model and reflect Te Pae Tawhiti best practice.

3. Ngā Mātāpono | Principles

3.1. All Kaimahi and Ohu Kaitiaki must ensure that, when using or dealing with personal information relating to any individual, they comply fully with the Information Privacy Principles within the Act (and as also referred to within the Appendix to this Policy).

3.2. Kaimahi who are responsible for contractors or consultants working for, or on behalf of Te Pūkenga and its Business Divisions, must ensure that the contractors or consultants understand and comply with their obligations under the Act, the requirements of this Policy and the applicable data breach response plan.

3.3. The Privacy Officer is the primary person responsible for engaging with the Privacy Commissioner in relation to privacy matters. This includes responding to compliance notices, cooperating with investigations or complaint proceedings and submitting a notice of any Notifiable Privacy Breach.

3.4. The Chief Executive or delegated Deputy Chief Executive will ensure that at all times Te Pūkenga has a duly appointed Privacy Officer, and each Business Division has a duly appointed Privacy Lead. These roles

will be the first point of contact for any questions and complaints in relation to privacy issues occurring within their respective realms.

4. Ngā Haepapa | Responsibilities

Role	Responsibilities
Te Pūkenga Council	• Adopt this policy
Chief Executive or delegated Deputy Chief Executive	• Ensures Te Pūkenga appoints a Privacy Officer.
Te Pūkenga Executive Leadership Team	• Ensures procedures that support the operation of this Policy within Te Pūkenga head office are reviewed periodically, remain fit for purpose and are compliant with legislation.
Business Division Executive Leadership Teams	• Ensure their Business Division has a Privacy Lead. • If the Business Division's Privacy Policy continues to apply, ensures the Privacy Procedure contained in that Policy are reviewed periodically, remain fit for purpose and compliant with legislation, and are consistent with this Policy.
Privacy Officer	• Ensures that information held by Te Pūkenga is held in accordance with the Act. • Encourages Te Pūkenga Kaimahi to comply with the Information Privacy Principles set out in the Act. • Ensures all within Te Pūkenga comply with this Policy and the Act. • Deals with requests made to Te Pūkenga under the Act with assistance from the teams that hold the relevant information. • Acts as the point of contact for Te Pūkenga as a whole with the Privacy Commissioner, including responding to compliance notices and cooperating with investigations or complaint proceedings. • Upon being notified of a privacy breach, complies with the Central Data Breach Response Plan to determine whether or not the breach is a Notifiable Privacy Breach and, if so, notifies the Privacy Commissioner and any affected parties. • Engages with Privacy Leads when notified of high-risk privacy matters. • Provides guidance to Privacy Leads on whether privacy matters are to be considered 'high-risk' or not. • Ensures details of the Privacy Officer and Privacy Leads remain up to date on Te Pūkenga website.
Business Division Privacy Leads	• Ensures that information held by Te Pūkenga at the Business Division level is held in accordance with the Act. • Encourages Te Pūkenga Kaimahi at the Business Division to comply with the Information Privacy Principles set out in the Act. • Ensures Te Pūkenga Kaimahi at the Business Division comply with the applicable Privacy Policy and the Act.

	• Deals with requests made to the Business Division under the Act with assistance from the teams that hold the relevant information. • Upon being notified of a privacy breach, engages with the Privacy Officer to confirm if the breach is a Notifiable Privacy Breach. • Conducts a risk assessment for all privacy breaches and engages the Privacy Officer when high-risk breaches are identified. • Consults the Privacy Officer if unsure whether a breach falls into the high-risk category.
Te Pūkenga Kaimahi	• Comply with this policy. • Promptly reports any privacy breaches to the relevant Privacy Officer or the Privacy Lead in accordance with this Policy. • Assists with requests made to Te Pūkenga under the Act, where required. • Promptly forwards any compliance notices or other correspondence received from the Privacy Commissioner to the Privacy Officer. • If responsible for engaging contractors or consultants, ensures contractors and consultants understand their obligations under the Act and undertake to comply with this Policy.

5. Ngā Tikanga | Definitions

Term	Definition
Business Division	References an ITP subsidiary that dissolves prior to 31 December 2022.
Information Privacy Principles (IPP)	The information privacy principles prescribed in section 22 of the Act, as also set out in the Appendix to this Policy.
Kaimahi	All employees of Te Pūkenga, including contracted staff, consultants and secondees providing services for Te Pūkenga, and those on fixed-term contracts.
Notifiable Privacy Breach	In accordance with section 112 of the Act, a notifiable privacy breach means a privacy breach that it is reasonable to believe has caused serious harm to an affected individual or individuals or is likely to do so (taking into account the factors set out in section 113 of the Act). The factors set out in section 113 of the Act are: • any action taken by the agency to reduce the risk of harm following the breach • whether the personal information is sensitive in nature • the nature of the harm that may be caused to affected individuals • the person or body that has obtained or may obtain personal information as a result of the breach (if known) whether the personal information is protected by a security measure and • any other relevant matters.

Ohu Kaitiaki	All those operating at a governance level, including Council members and members of Council's advisory committees.
Personal Information	In accordance with the Act, personal information means information about an identifiable individual and includes information relating to a death that is maintained by the Registrar-General under the Births, Deaths, Marriages, and Relationships Registration Act 1995 or any former Act. For the avoidance of doubt, personal information includes (without limitation) the following types of information: name, age, contact details, images, course of study, IRD number and banking details.

6. Reference Documents

- Privacy Act 2020
- Official Information Act 1982
- Office of the Privacy Commissioner website

7. Ngā Hononga ki Tuhinga kē | Links to Other Documents

Ngā Kaupapa-Here e Hāngai ana **| Related Policies**
Ngā Tukanga me ngā Hātepe **| Processes, Procedures** Central Data Breach Response Plan Privacy Procedure

Appendix

Information Privacy Principles (IPP)

Information privacy principle 1

Purpose of collection of personal information

1. Personal information must not be collected unless:
    a. the collection is for a lawful purpose connected with a function or activity of the agency; and
    b. the collection of the information is necessary for that purpose.

2. If the lawful purpose for which personal information about an individual is collected does not require the collection of an individual's identifying information, the agency may not require the individual's identifying information.

Information privacy principle 2

Source of personal information

1. If an agency collects personal information, personal information must be collected from the individual concerned.

2. It is not necessary for an agency to comply with subclause (1) if the agency believes, on reasonable grounds:
    a. that non-compliance would not prejudice the interests of the individual concerned; or
    b. that compliance would prejudice the purposes of the collection; or
    c. that the individual concerned authorises collection of the information from someone else; or
    d. that the information is publicly available information; or
    e. that non-compliance is necessary:
        i. to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences; or
        ii. for the enforcement of a law that imposes a pecuniary penalty; or
        iii. for the protection of public revenue; or
        iv. for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or
        v. to prevent or lessen a serious threat to the life or health of the individual concerned or any other individual;
    f. that compliance is not reasonably practicable in the circumstances of the particular case; or
    g. that the information:
        i. will not be used in a form in which the individual concerned is identified; or
        ii. will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

Information privacy principle 3

Collection of information from subject

1. If an agency collects personal information from the individual concerned, the agency must take any steps that are, in the circumstances, reasonable to ensure that the individual concerned is aware of:
    a. the fact that the information is being collected; and
    b. the purpose for which the information is being collected; and
    c. the intended recipients of the information; and
    d. the name and address of:
        i. the agency that is collecting the information; and
        ii. the agency that will hold the information; and
    e. if the collection of the information is authorised or required by or under law:
        i. the particular law by or under which the collection of the information is authorised or required; and
        ii. whether the supply of the information by that individual is voluntary or mandatory; and
    f. the consequences (if any) for that individual if all or any part of the requested information is not provided; and
    g. the rights of access to, and correction of, information provided by the IPPs (being the Information Privacy Principles).

2. The steps referred to in subclause (1) must be taken before the information is collected or, if that is not practicable, as soon as practicable after the information is collected.

3. An agency is not required to take the steps referred to in subclause (1) in relation to the collection of information from an individual if the agency has taken those steps on a recent previous occasion in relation to the collection, from that individual, of the same information or information of the same kind.

4. It is not necessary for an agency to comply with subclause (1) if the agency believes, on reasonable grounds:
    a. that non-compliance would not prejudice the interests of the individual concerned, or
    b. that non-compliance is necessary:
        i. to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences; or
        ii. for the enforcement of a law that imposes a pecuniary penalty; or
        iii. for the protection of public revenue; or
        iv. for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or
    c. that compliance would prejudice the purposes of the collection; or
    d. that compliance is not reasonably practicable in the circumstances of the particular case; or
    e. that the information:
        i. will not be used in a form in which the individual concerned is identified; or

ii. will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

Information privacy principle 4

Manner of collection of personal information

An agency may collect personal information only:

a. by a lawful means; and
b. by a means that, in the circumstances of the case (particularly in circumstances where personal information is being collected from children or young persons):
    i. is fair; and
    ii. does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Information privacy principle 5

Storage and security of personal information

An agency that holds personal information must ensure:

a. that the information is protected, by such security safeguards as are reasonable in the circumstances to take, against:
    i. loss; and
    ii. access, use, modification, or disclosure that is not authorised by the agency; and
    iii. other misuse; and
b. that, if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

Information privacy principle 6

Access to personal information

1. An individual is entitled to receive from an agency upon request:
    a. confirmation of whether the agency holds any personal information about them; and
    b. access to their personal information.

2. If an individual concerned is given access to personal information, the individual must be advised that, under IPP 7, the individual may request the correction of that information.

3. This IPP is subject to the provisions of Part 4 of the Act which sets out the manner in which requests can be made and the limited circumstances in which a request may be refused (refer Privacy Procedure).

Information privacy principle 7

Correction of personal information

1. An individual whose personal information is held by an agency is entitled to request the agency to correct the information.

2. An agency that holds personal information must, on request or on its own initiative, take such steps (if any) that are reasonable in the circumstances to ensure that, having regard to the purposes for which the information may lawfully be used, the information is accurate, up to date, complete, and not misleading.

3. When requesting the correction of personal information, or at any later time, an individual is entitled to:
    a. provide the agency with a statement of the correction sought to the information (a statement of correction); and
    b. request the agency to attach the statement of correction to the information if the agency does not make the correction sought.

4. If an agency that holds personal information is not willing to correct the information as requested and has been provided with a statement of correction, the agency must take such steps (if any) that are reasonable in the circumstances to ensure that the statement of correction is attached to the information in a manner that ensures that it will always be read with the information.

5. If an agency corrects personal information or attaches a statement of correction to personal information, that agency must, so far as is reasonably practicable, inform every other person to whom the agency has disclosed the information.

6. Subclauses (1) to (4) are subject to the provisions of Part 4 of the Act.

Information privacy principle 8

Accuracy, etc, of personal information to be checked before use or disclosure

An agency that holds personal information must not use or disclose that information without taking any steps that are, in the circumstances, reasonable to ensure that the information is accurate, up to date, complete, relevant, and not misleading.

Information privacy principle 9

Agency not to keep personal information for longer than necessary

An agency that holds personal information must not keep that information for longer than is required for the purposes for which the information may lawfully be used.

Information privacy principle 10

Limits on use of personal information

1. An agency that holds personal information that was obtained in connection with one purpose may not use the information for any other purpose unless the agency believes, on reasonable grounds:
    a. that the purpose for which the information is to be used is directly related to the purpose in connection with which the information was obtained; or

b. that the information:
    i. is to be used in a form in which the individual concerned is not identified; or
    ii. is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
c. that the use of the information for that other purpose is authorised by the individual concerned; or
d. that the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to use the information; or
e. that the use of the information for that other purpose is necessary:
    i. to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences; or
    ii. for the enforcement of a law that imposes a pecuniary penalty; or
    iii. for the protection of public revenue; or
    iv. for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or
f. that the use of the information for that other purpose is necessary to prevent or lessen a serious threat to:
    i. public health or public safety; or
    ii. the life or health of the individual concerned or another individual.

2. In addition to the uses authorised by subclause (1), an intelligence and security agency that holds personal information that was obtained in connection with one purpose may use the information for any other purpose (a secondary purpose) if the agency believes on reasonable grounds that the use of the information for the secondary purpose is necessary to enable the agency to perform any of its functions.

Information privacy principle 11

Limits on disclosure of personal information

1. An agency that holds personal information must not disclose the information to any other agency or to any person unless the agency believes, on reasonable grounds:
    a. that the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained; or
    b. that the disclosure is to the individual concerned; or
    c. that the disclosure is authorised by the individual concerned; or
    d. that the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to disclose the information; or
    e. that the disclosure of the information is necessary:
        i. to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences; or
        ii. for the enforcement of a law that imposes a pecuniary penalty; or

iii. for the protection of public revenue; or iv. for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

f. that the disclosure of the information is necessary to prevent or lessen a serious threat to:
    i. public health or public safety; or
    ii. the life or health of the individual concerned or another individual; or
g. that the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions; or
h. that the information:
    i. is to be used in a form in which the individual concerned is not identified; or
    ii. is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
    iii. that the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern.

2. This IPP is subject to IPP 12.

Information privacy principle 12

Disclosure of personal information outside New Zealand

1. An agency (**A**) may disclose personal information to a foreign person or entity (**B**) in reliance on IPP 11(1)(a), (c), (e), (f), (h), or (i) only if:
    a. the individual concerned authorises the disclosure to B after being expressly informed by A that B may not be required to protect the information in a way that, overall, provides comparable safeguards to those in this Act; or
    b. B is carrying on business in New Zealand and, in relation to the information, A believes on reasonable grounds that B is subject to this Act; or
    c. A believes on reasonable grounds that B is subject to privacy laws that, overall, provide comparable safeguards to those in this Act; or
    d. A believes on reasonable grounds that B is a participant in a prescribed binding scheme; or
    e. A believes on reasonable grounds that B is subject to privacy laws of a prescribed country; or
    f. A otherwise believes on reasonable grounds that B is required to protect the information in a way that, overall, provides comparable safeguards to those in this Act (for example, pursuant to an agreement entered into between A and B).

2. However, subclause (1) does not apply if the personal information is to be disclosed to B in reliance on IPP 11(1)(e) or (f) and it is not reasonably practicable in the circumstances for A to comply with the requirements of subclause (1).

3. In this IPP:

    prescribed binding scheme means a binding scheme specified in regulations made under section 213 of the Act,

    prescribed country means a country specified in regulations made under section 214 of the Act.

Information privacy principle 13

Unique identifiers

1. An agency (**A**) may assign a unique identifier to an individual for use in its operations only if that identifier is necessary to enable A to carry out 1 or more of its functions efficiently.

2. A may not assign to an individual a unique identifier that, to A's knowledge, is the same unique identifier as has been assigned to that individual by another agency (B), unless:
    a. A and B are associated persons within the meaning of subpart YB of the Income Tax Act 2007; or
    b. the unique identifier is to be used by A for statistical or research purposes and no other purpose.

3. To avoid doubt, A does not assign a unique identifier to an individual under subclause (1) by simply recording a unique identifier assigned to the individual by B for the sole purpose of communicating with B about the individual.

4. A must take any steps that are, in the circumstances, reasonable to ensure that:
    a. a unique identifier is assigned only to an individual whose identity is clearly established; and
    b. the risk of misuse of a unique identifier by any person is minimised (for example, by showing truncated account numbers on receipts or in correspondence).

5. An agency may not require an individual to disclose any unique identifier assigned to that individual unless the disclosure is for one of the purposes in connection with which that unique identifier was assigned or is for a purpose that is directly related to one of those purposes.