Ngā Hātepe | Privacy Procedure

Mō wai me te whānuitanga | Audience and scope

These procedures are relevant to 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 procedure). Where relevant, these procedures should also be followed by **ohu kaitiaki**, which extends to all those operating at a governance level, including Council members and members of Council's advisory committees.

This procedure applies to Personal Information collected and held by Te Pūkenga and its business divisions in respect of any identifiable individual.

Application to Te Pūkenga Business Divisions

Following dissolution of each of the former ITP and TITO subsidiaries, the successive business division may continue to operate under its existing privacy procedures so long as they are not inconsistent with the principles laid out in Te Pūkenga Privacy Policy. This is to allow privacy procedures already working well for business divisions to continue uninterrupted, as well as empower each business division to take accountability and responsibility for privacy matters occurring within their operations.

Business divisions operating under their own privacy policies and procedures must have regard to points 3.1 to 3.4 in this procedure.

Mokamoka whakaaetanga | Approval details

Version number	3	**Issue date**	26 February 2024
Approval authority	Executive Leadership Team	**Date of approval**	26 February 2024
Procedure sponsor (has authority to make minor amendments)	Director Legal	**Procedure owner**	Chief of Staff
Contact person	Director Legal	**Date of next review**	1 December 2025

Ngā whakatikatika | Amendment history

Version	Effective date	Created/reviewed by	Reason for review/comment
1	4 August 2021		Initial version
2	1 June 2022	Sam Shannon/Sinead Hart	Preparing policy framework to receive early mover ITPs
3	26 February 2024	Kara Hiron	Scheduled review

Ngā Ihirangi | Table of Contents

Ngā Hātepe | Privacy Procedure

1. Pūtake | Purpose

1.1. The purpose of this procedure is to ensure Te Pūkenga complies fully with its obligations under the Privacy Act 2020 (the Act), including any applicable codes of practice issued by the Privacy Commissioner under 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. This procedure should be read in conjunction with the relevant privacy policy and data breach response plan.

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

The Council of Te Pūkenga acknowledges that this procedure 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 Procedure. The Council notes that Te Pūkenga is still on its transition journey and, as it matures, this procedure 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

Business Division procedure for high-risk privacy matters

3.1. Following the dissolution of a former ITP or TITO subsidiary of Te Pūkenga, the successive business division may continue to operate under the privacy procedures that applied immediately prior to dissolution, so long as those procedures are consistent with the principles of Te Pūkenga Privacy Policy.

3.2. The business division's Privacy Lead is responsible for managing privacy matters that arise within the relevant business division.

3.3. All privacy breaches must undergo a risk assessment to categorise the breach as either low, medium or high risk.

3.4. Where any 'high risk' breaches are identified, or any 'notifiable' breaches occur as defined by the Privacy Act 2020, the business division Privacy Lead must notify Te Pūkenga Privacy Officer of the breach .

Head office procedure for high-risk privacy matters

3.5. Te Pūkenga head office Kaimahi are responsible for reporting any 'high risk', or any 'notifiable' breaches that occur as defined by the Privacy Act 2020, to Te Pūkenga Privacy Officer.

3.6. All privacy breaches must undergo a risk assessment to categorise the breach as either low, medium or high risk.

4. Ngā Hātepe | Procedure

Collection of Personal Information

4.1. All kaimahi shall comply with information Privacy Principles 1 to 4 prescribed in section 22 of the Act (refer to the Appendix in Te Pūkenga Privacy Policy).

4.2. Any forms that collect Personal Information about Ohu Kaitiaki, Kaimahi, Ākonga or any other individuals (including employers) (including both physical and electronic forms) must include a privacy statement and specify the purpose(s) for which the information is being collected, together with any other matters that should be disclosed under the Act. The standard Te Pūkenga Privacy Notice should be used in the context of ākonga.

Recruitment of kaimahi

4.3. The Chief People Officer must ensure that:

a) all Personal Information collected from applicants is directly relevant to the position advertised
b) all data collected is treated with due regard to confidentiality and privacy requirements.

4.4. Without limiting the foregoing, **ohu kaitiaki and kaimahi** must:

a) have the applicant's permission to contact referees nominated on any application form or associated correspondence prior to contacting the referees
b) not ask any other person to provide information about the applicant without the applicant's consent. If the applicant is a current or past kaimahi of Te Pūkenga or one of its business divisions, **ohu kaitiaki and kaimahi** may consult the applicant's personnel file.

Access to Personal Information

4.5. All Ohu kaitiaki and kaimahi shall comply with Information Privacy Principle 6 prescribed in section 22 of the Act (refer to the Appendix in Te Pūkenga Privacy Policy).

4.6. Any kaimahi wanting to access their own or another's Personal Information may be required to first produce identification to the person holding the information, such as a current New Zealand driver licence, passport, 18+ card or, a Te Pūkenga or business division kaimahi ID.

Access to Te Pūkenga ākonga files

4.7. Kaimahi may access Personal Information relating to Te Pūkenga ākonga only if that is necessary for the kaimahi to carry out their employment responsibilities.

4.8. No person may remove any Te Pūkenga ākonga file from a physical location where it is held unless they are required to by law or have approval from the relevant Head of School or such other person of equivalent authority at the relevant location. Any Te Pūkenga Ākonga files removed from a campus must be kept safely and securely at all times in accordance with section 4 of these Privacy Procedures.

4.9. Te Pūkenga ākonga wishing to view a physical copy of their own files must first request access from the relevant Head of School (or equivalent) who, if approved, will arrange for Kaimahi to be present during the viewing.

4.10. A Te Pūkenga ākonga must not remove any information from, or alter any part of, their physical Te Pūkenga ākonga file.

4.11. Any "evaluative material" (as referred to in section 50 of the Privacy Act 2020) supplied in confidence by the writer (e.g., expressions of opinion contained in reports, references, assessments) may be disclosed to the ākonga only at the discretion of the relevant Head of School (or equivalent) and with the written consent of the person who supplied the evaluative material, unless otherwise required by law.

Access to ohu kaitiaki or kaimahi files by ohu kaitiaki or kaimahi

4.12. Subject to the provisions of this procedure and any limitations specified in the Act, all ohu kaitiaki and kaimahi have the right to access their own ohu kaitiaki or kaimahi file.

4.13. Ohu kaitiaki or kaimahi should request permission from the People, Culture and Wellbeing team, or the relevant business division equivalent, if they wish to access their file.

4.14. Ohu kaitiaki and kaimahi must not remove any information from, or alter any part of, their file. The original file must stay in a secure location at Te Pūkenga.

4.15. Ohu kaitiaki and kaimahi may request a copy of any document or extract from their file.

4.16. Any 'evaluative material' about ohu kaitiaki or kaimahi (as referred to in section 50 of the Privacy Act 2020) supplied in confidence by the writer (e.g. expressions of opinion contained in reports, references, assessments, reviews) may be disclosed to ohu kaitiaki or kaimahi only at the discretion of the relevant manager and with the written consent of the person who supplied the evaluative material, unless otherwise required by law.

Access to ohu kaitiaki and kaimahi files by other Te Pūkenga kaimahi or ohu kaitiaki

4.17. Authorised personnel may access kaimahi and ohu kaitiaki files but only if that access is necessary for the purpose of carrying out their employment duties / role. In accessing the files, the authorised person may only access the parts of the files that are relevant to the employment duty / role they are carrying out. For the purposes of this section, authorised personnel comprise:

a) Chair and Deputy Chair of Council in relation to ohu kaitiaki and the Chief Executive
b) members of the Executive Leadership Team
c) line managers (permitted access to the kaimahi files of those they manage)
d) Kaimahi employed in People, Culture and Wellbeing team; and
e) Executive Assistants and administrators acting on the direction of those ohu kaitiaki and kaimahi referred in paragraphs 3.17a) – d) (inclusive)
f) any other Kaimahi expressly authorised by the Chief People Officer or the Chief Executive.

Maintaining Personal Information

4.18. All ohu kaitiaki and kaimahi shall comply with Information Privacy Principles 7 and 8 prescribed in section 22 of the Act (refer to the Appendix in Te Pūkenga Privacy Policy).

4.19. Kaimahi responsible for maintaining files containing Personal Information must ensure they contain accurate, up to date, complete and relevant information that is not misleading.

4.20. All ohu kaitiaki and kaimahi must ensure that their current name and contact details provided to Te Pūkenga are correct and must notify People, Culture and Wellbeing kaimahi when any changes occur.

Corrections to files

4.21. Kaimahi and ohu kaitiaki may at any time request corrections to their Personal Information. A request for correction must be noted in the individual's record.

4.22. If a correction is requested, the person who maintains the file must take reasonable steps to correct that information, having regard to:

a) the purposes for which the information may lawfully be used, and
b) the obligation of Te Pūkenga (including its business divisions) to take reasonable steps to ensure that the information is accurate, up to date, complete, and not misleading.

4.23. If the person who maintains the file does not agree to the correction, they must ensure that any statement provided by ohu kaitiaki, Te Pūkenga ākonga or kaimahi is able to be viewed alongside the original information.

Maintaining kaimahi files

4.24. Kaimahi who require access to kaimahi information to carry out their employment duties / role responsibilities may maintain Personal Information relating to kaimahi and ohu kaitiaki to the extent that the information is required to carry out their employment duties / role responsibilities.

Storage and security of Personal Information

4.25. All ohu kaitiaki and kaimahi must comply with Information Privacy Principles 5 and 9 prescribed in section 22 of the Act, the Public Records Act 2005 and the applicable Information and Records Management Policy.

4.26. Hard copy files containing Personal Information must be stored in a secured and locked storage space. Individuals holding these files are responsible for their security.

4.27. Hard copy files containing Personal Information shall not be removed from premises of Te Pūkenga, except as permitted under the Privacy Policy or this procedure. Where information is removed from premises of Te Pūkenga (excluding kaimahi files which should never be removed from premises of Te Pūkenga except in accordance with these procedures or the approval of the relevant business division Privacy Lead or the Privacy Officer), that information shall be kept safely and securely at all times, including without limitation:

a) information must be stored in zipped up laptop bags or other enclosed storage
b) information must not be left in a car
c) if the kaimahi is in transit or has no choice but to leave the information in a car, place it under the seats or in the boot
d) do not leave information unattended at any time if you are travelling
e) upon reaching your destination, the information must be brought inside and kept behind a locked door and not in a communal area.

4.28. Personal Information shall not be kept for longer than is required for the purposes for which Te Pūkenga collected the information.

4.29. The Chief People Officer (or their delegate) is responsible for ensuring that kaimahi files containing Personal Information are retained and disposed of within the timeframes set out in points 4.34 and 4.35.

Online security of Personal Information

4.30. The Digital team are responsible for the security of the electronic management systems used to collect and manage Personal Information relating to Te Pūkenga kaimahi and must ensure that:

Ākonga and kaimahi information

a) Access to electronic management systems for Te Pūkenga shall be granted to kaimahi only to the extent that each kaimahi requires access to the relevant electronic management system in order to carry out their Te Pūkenga responsibilities.
b) Stored Personal Information (Te Pūkenga ākonga and kaimahi) must be backed up in an appropriate manner.

Kaimahi information

a) Managers are given access only to the details of the kaimahi they are responsible for.
b) Appropriate access is given to managers who require Te Pūkenga wide information in order to meet Te Pūkenga business requirements, provided that the access is generic in nature and does not identify any kaimahi, unless identification is necessary for the particular business transaction.
c) The only means of access to the Personal Information of any kaimahi record, held and managed electronically, is by way of appropriate identifications set out in point 4.6.

4.31. Kaimahi must ensure that, when viewing ākonga or kaimahi information, no unauthorised person is able to view the information.

Offsite storage

4.32. Records containing Personal Information may be sent offsite for safe and secure storage. A record of information sent offsite must be kept, including the date the information was sent offsite. This will be documented in the Information and Records Management Policy adopted by Te Pūkenga following the finalisation and implementation of the Information Systems Strategic Plan (ISSP).

Retention periods

4.33. In accordance with the Public Records Act 2005, and in broad terms, the retention periods for documents are as set out below. However, pending the adoption of a final Information and Records Management Policy, the position of Te Pūkenga is that no records should be archived offsite or destroyed during the transition period.

4.34. Retention periods – ākonga files

Information	Retain for…
Details of qualifications, courses studied and final assessment results	Permanently
Ākonga files (hard and electronic copies)	10 years from last information entry then destroy
Scholarship applications, examination scripts and other similar documents	12 months then destroy

4.35. Retention periods – kaimahi files

Information	Retain for…
Kaimahi files for Chief Executive and second-tier managers	10 years from last information entry date then transfer to Archives NZ
Kaimahi who received national honours or national/international academic awards (e.g. honorary doctorates)	10 years from last information entry date then transfer to Archives NZ
Summaries of Kaimahi histories (recording name, date of birth, positions held and salary, dates of employment)	10 years from last information entry date then transfer to Archives NZ
Kaimahi files for all other Kaimahi who have left Te Pūkenga	7 years from last information entry date then destroy

Use of Personal Information

4.36. All ohu kaitiaki and kaimahi shall comply with Information Privacy Principle 10 prescribed in section 22 of the Act (refer to the Appendix in Te Pūkenga Privacy Policy).

4.37. Ohu kaitiaki and kaimahi must only use Personal Information relating to any ākonga, ohu kaitiaki, kaimahi or other person for the purpose for which that information was collected, unless permitted under one of the exceptions listed in the Act, for example:

a) the purpose for which the information is to be used is directly related to the purpose for which the information was collected
b) the information is to be used in a form in which the individual concerned is not identified
c) the information is to be used for statistical or research purposes and will not be published in a form that would identify the individual concerned, or
d) they have the written consent of the individual concerned.

Disclosure of Personal Information

4.38. All ohu kaitiaki and kaimahi shall comply with Information Privacy Principles 11 and 12 prescribed in section 22 of the Act.

4.39. Ohu kaitiaki and kaimahi must not disclose any Personal Information relating to any ākonga or kaimahi to any person or agency (other than to authorised members of Te Pūkenga kaimahi), including parents, partners and employers of that ākonga or kaimahi, unless permitted under one of the exceptions listed in the Act, for example:

a) the disclosure is one of the purposes for which the information was collected or is directly related to one of the purposes for which the information was collected
b) they have the written consent of the individual concerned, or
c) they are required to by law (e.g. to assist the Police with detecting, investigating or prosecuting an offence).

4.40. Ohu kaitiaki and kaimahi must exercise particular care not to divulge Personal Information when using social media.

4.41. When a kaimahi receives a request for Personal Information that relates to someone other than the requester, they must consult with the relevant business division Privacy Lead or Te Pūkenga Privacy Officer if they are unsure whether or not to disclose that information.

Disclosure of Personal Information relating to Te Pūkenga ākonga

4.42. Kaimahi shall seek the advice of the relevant business division Privacy Lead or Te Pūkenga Privacy Officer before disclosing any personal information. Any requests for Personal Information relating to ākonga (whether prospective, current or former) must be referred to the business division where the ākonga information originated.

4.43. Kaimahi must not include any Personal Information about ākonga in any material issued, unless they have the prior written consent of that ākonga.

4.44. Te Pūkenga may be required from time to time to provide Personal Information relating to ākonga to the Privacy Commissioner acting within their authority under the Act (unless the information is held by a business division in which case the request should be referred to the business division).

4.45. Kaimahi may disclose whether ākonga have obtained a qualification from Te Pūkenga network if the qualification was awarded at a public graduation ceremony and/or the qualification was published in the graduation booklet (and the disclosure is made by the business division who awarded the qualification, and it aligns with that business division's privacy policies and procedures).

4.46. If a qualification was not awarded at a public ceremony (whether in person or in absentia) and/or published in the graduation booklet, the written permission of the ākonga must be obtained before the information can be released. This should be obtained by the business division where the ākonga was enrolled.

4.47. Examination results must be published only by the business division where the ākonga is enrolled, according to the business division's privacy policies (including using appropriate ākonga ID numbers

rather than ākonga names or other identifiers, unless published directly to the ākonga and no other person).

Disclosure of Personal Information related to kaimahi

4.48. Any requests for Personal Information relating to kaimahi (whether prospective, current or former) must be referred to the People, Culture and Wellbeing team. In cases of doubt, People, Culture and Wellbeing kaimahi shall seek the advice of the relevant business division Privacy Lead or Te Pūkenga Privacy Officer before disclosing any information.

4.49. Te Pūkenga may include details of kaimahi (such as name, work contact details, title and areas of expertise of that kaimahi) in Te Pūkenga publications including promotional brochures and Te Pūkenga website.

4.50. Te Pūkenga is sometimes required as a matter of law to provide Personal Information relating to kaimahi to government agencies such as the Tertiary Education Commission and the Inland Revenue Department.

4.51. Te Pūkenga also provides Personal Information as necessary to meet its obligations as an insured party under its kaimahi insurance policy.

Information collected from Te Pūkenga website and online marketing

4.52. Te Pūkenga collects and stores information (such as IP address, details of visit, type of internet browser used) about its website visitors for statistical purposes, to improve the website and to assist in the promotion of Te Pūkenga and its programmes. That information is unlikely to constitute Personal Information under the Act, unless the visitor voluntarily provides information which enables them to be personally identified or uses a third-party service which requires logging in to a restricted account.

4.53. Third-party vendors (such as Google) display advertisements for Te Pūkenga on internet sites and use cookies (small text files) to customise the visitor's experience and provide statistical information to the vendor. A visitor to such a site has the right to opt out by disabling the use of cookies on their browser.

Disclosure of Personal Information outside Aotearoa New Zealand

4.54. Te Pūkenga shall only disclose Personal Information to a foreign person or entity in the circumstances permitted under information privacy principle 12, for example:

a) the individual authorises the disclosure (after being expressly informed by Te Pūkenga that the recipient may not be required to protect the information in a way that provides comparable safeguards to Aotearoa New Zealand's privacy laws);
b) the recipient is carrying on business in Aotearoa New Zealand and would accordingly be subject to the Act;
c) the recipient is subject to privacy laws that provide comparable safeguards to Aotearoa New Zealand's privacy laws; or
d) Te Pūkenga has an agreement with the recipient that requires the recipient to comply with sufficient privacy and confidentiality safeguards.

Collection and use of personal information from outside Aotearoa New Zealand

4.55. Where Te Pūkenga collects and uses Personal Information/personal data from outside of New Zealand, there is the potential that the privacy/data protection regimes of other countries may apply to the collection and use of that Personal Information. Given the potential for extraterritorial application of certain regimes, this can be a complex and challenging area. Therefore, where initiatives/changes in processes are proposed that would notably alter how Personal Information from overseas is collected and used, the relevant business division Privacy Lead and/or the Privacy Officer should be consulted.

Projects involving personal information – use of Privacy Impact Assessments

4.56. A Privacy Impact Assessment (**PIA**) is a useful tool to help assess and mitigate risk for changes involvi ng personal information. For any project that is collecting, using or disclosing personal information it is recommended that a PIA is completed. A PIA must be completed for any projects where all of the following applies:

- Does the proposed change involve or alter the collection, storage, use or disclosure of personal information?
- Is the personal information considered sensitive?
- Would the change be contrary to 'customer' expectations or put a significant amount of information at risk?

If kaimahi are unsure whether a PIA is required, the Legal team should be consulted for guidance.

Breaches of privacy

4.57. In accordance with section 114 of the Act, Te Pūkenga is required to report Notifiable Privacy Breaches to the Privacy Commissioner. Section 115 of the Act also requires that Te Pūkenga notify the individual(s) affected by the Notifiable Privacy Breach that the breach has occurred or, where this is not reasonably practicable, give public notice of the breach.

4.58. All kaimahi must promptly report any privacy breaches at Te Pūkenga to the relevant business division Privacy Lead or Te Pūkenga Privacy Officer. The relevant business division Privacy Lead and/or Te Pūkenga Privacy Officer (as applicable), in conjunction with the Data Breach Response Plan Team, will assess whether or not any reported privacy breach is a Notifiable Privacy Breach and the appropriate action that should be taken having regard to the requirements of section 115 of the Act and the exceptions set out in section 116 of the Act. Where the breach relates to a technological matter, the Chief Information Security Officer must be informed immediately so that they can activate the Data Breach Response Plan and ensure immediate remedial action. Business division Privacy Leads must notify all privacy breaches to Te Pūkenga Privacy Officer so that a central breach register may be maintained.

4.59. Where a Notifiable Privacy Breach has occurred:

- within a business division, the relevant business division Privacy Lead will notify Te Pūkenga Privacy Officer; and
- In all cases, Te Pūkenga Privacy Officer will notify the Chief Executive and the Executive Leadership Team.

The relevant business division Privacy Lead and/or Privacy Officer (as applicable) will follow the Data Breach Response Plan when determining the correct strategy to apply in the circumstances, and any

notifications that should be made to the Privacy Commissioner, affected individual(s), or whether to make a public notification.

4.60. Any public notifications of privacy breaches shall be made available on Te Pūkenga website.

Requests under the Privacy Act 2020

4.61. Section 40 of the Act allows any individual or their representative to request access to their Personal Information held by Te Pūkenga.

Time limits

4.62. In accordance with section 44 of the Act, Te Pūkenga must respond to a privacy request as soon as reasonably practicable and no later than 20 working days after receiving the request.

4.63. The time limit for responding to an information privacy request may be extended in accordance with section 48 of the Act by the Chief Executive (or delegate), Te Pūkenga Privacy Officer or the relevant business division Privacy Lead if:

a) the request is for a large quantity of information, or requires a search through a large quantity of information, and meeting the original time limit would unreasonably interfere with the operations of Te Pūkenga
b) consultations needed to make a decision are such that a decision on the request cannot be made within the original time limit, or
c) the processing of the request raises issues of such complexity that a response cannot reasonably be given within the original time limit.

4.64. If an extension is required, the kaimahi dealing with the information request must notify the Chief Executive (or delegate), the relevant business division Privacy Lead or Te Pūkenga Privacy Officer as soon as practicable and, in any event, before the expiry of the original time limit.

Exceptions – withholding of Personal Information

4.65. A request by an individual for access to their information held by Te Pūkenga must be granted unless good reasons exist (as set out in the Act) to withhold the information. Sections 49 to 53 of the Act set out the basis on which a request for Personal Information can be refused. This includes withholding Personal Information where:

a) the disclosure of the information would be likely to pose a serious threat to the life, health or safety of any individual or to the public health or public safety
b) the disclosure of the information would create a significant likelihood of serious harassment of an individual
c) the disclosure of the information would involve the unwarranted disclosure of the affairs of another individual or of a deceased individual
d) the disclosure of the information would breach legal professional privilege
e) the request is frivolous or vexatious, or the information requested is trivial, or
f) the information requested does not exist or cannot be found.

4.66. Requests for Personal Information by any other person or agency other than the individual to whom the information relates are not IPP6 requests (i.e. requests under the Privacy Act 2020) but should be

more properly considered as requests for information under the Official Information Act 1982 (OIA) and disclosure must be considered within the context of the OIA. This does not apply where the requester is an agent or representative of the individual to whom the information relates and the relevant criteria under section 57 of the Act are met.

Before responding to a request

4.67. Before responding to a privacy request, Te Pūkenga must meet the criteria specified in section 57 of the Act, including without limitation, the requirements specified in sections 4.67 to 4.69 (inclusive) of this procedure.

4.68. Te Pūkenga must satisfy itself as to the identity of the requestor, specifically:

a) where information is supplied by email, the email address must match the email address held on records Te Pūkenga holds for that individual (if any)
b) where information is supplied by post, the postal address must match the postal address held on records Te Pūkenga holds for that individual (if any) and the envelope must be clearly marked as private and confidential, and
c) where information is supplied in person, the requestor must first produce identification, such as a current New Zealand driver licence, passport, or 18+ card.

4.69. Information shall be supplied by email or in person to the maximum extent possible.

4.70. Where information is requested by a representative or agent of the individual, before supplying information to the requestor Te Pūkenga shall require a signed authorisation, email confirming authority or other sufficient authority from the individual.

The Privacy Commissioner

4.71. The Privacy Commissioner can investigate complaints about actions that may be a breach of the Act. For an explanation of the Privacy Commissioner's complaints process, please visit: https://privacy.org.nz/your-privacy/how-to-complain/.

4.72. All enquiries, correspondence, or other communications received by Te Pūkenga from the Office of the Privacy Commissioner regarding compliance with the Act must be promptly forwarded by kaimahi to the relevant business division Privacy Lead or Te Pūkenga Privacy Officer (whichever applies). Business division Privacy Leads must also forward a copy of any enquiries, correspondence, or other communications from the Office of the Privacy Commissioner to Te Pūkenga Privacy Officer.

5. Ngā Haepapa | Responsibilities

Role	Responsibilities
Business Division Privacy Lead	• All points outlined in the Privacy Policy and this procedure are followed in line with your role. • Report any "high risk", or any 'notifiable' breaches that occur as defined by the Privacy Act 2020, to Te Pūkenga Privacy Officer. • The business division Privacy Lead is the primary contact responsible for engaging with the Privacy Commissioner in relation to privacy matters

	with respect to the applicable business division. This includes responding to compliance notices, cooperating with investigations or complaint proceedings and submitting a notice of any Notifiable Privacy Breach.
Chief People Officer	• Ensure that kaimahi files containing Personal Information are retained and disposed of within the timeframes set out in this procedure. • Recruitment procedures are followed as set out in this procedure. • All points outlined in the Privacy Policy and this procedure are followed in line with your role.
Ohu Kaitiaki	• All points outlined in the Privacy Policy and this procedure are followed in line with your role. • If you have any doubts or concerns, contact Te Pūkenga Privacy Officer.
People, Culture and Wellbeing Kaimahi	• Update changes to Personal Information as soon as you are notified. • In cases of doubt, seek the advice of the relevant business division Privacy Lead or Te Pūkenga Privacy Officer before disclosing any information. • Handle requests from ohu kaitiaki and kaimahi to access their files as laid out in this procedure. • Handle all files described in this procedure in line with this procedure and the relevant Privacy Policy. • All points outlined in the Privacy Policy and this procedure are followed in line with your role.
Te Pūkenga kaimahi	• All points outlined in the Privacy Policy and this procedure are followed in line with your role. • If you have any doubts or concerns, contact your relevant Business Division Privacy Lead or Te Pūkenga Privacy Officer. • Promptly reports any breaches to the Privacy Officer or the Privacy Lead in the context of business division kaimahi. • 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 or the Privacy Lead in the context of business division kaimahi. • If responsible for engaging contractors or consultants, ensures contractors and consultants understand their obligations under the Act and undertake to comply with this policy.
Te Pūkenga Privacy Officer	• All points outlined in the Privacy Policy and this procedure are followed in line with your role. • The Privacy Officer is the primary contact responsible for engaging with the Privacy Commissioner in relation to privacy matters with respect to head office. This includes responding to compliance notices, cooperating with investigations or complaint proceedings and submitting a notice of any Notifiable Privacy Breach.

6. Ngā Tikanga | Definitions

Term	Means
Ākonga	References our learners/students
Business Division	References a part of Te Pūkenga that substantially constitutes what was previously either: a) an ITP subsidiary prior to its dissolution pursuant to the Education and Training Act 2020; or b) a former business division of Te Pūkenga Work Based Learning Limited, being a former TITO.
Business Division Privacy Lead	One or more individuals appointed at a Business Division to manage privacy matters in accordance with Te Pūkenga Privacy Policy.
Information Systems Strategic Plan (ISSP)	Identifies a portfolio of software that will assist Te Pūkenga in executing its business strategy and outlines the scope of business goals that relate to Information Technology (IT).
Information Privacy Principles	The Information Privacy Principles prescribed in section 22 of the Privacy Act 2020 (the Act), as set out in the Appendix to the Privacy 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: a) any action taken by the agency to reduce the risk of harm following the breach b) whether the Personal Information is sensitive in nature: c) the nature of the harm that may be caused to affected individuals d) the person or body that has obtained or may obtain Personal Information as a result of the breach (if known) e) whether the Personal Information is protected by a security measure, and f) 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.
Privacy breach	In accordance with section 112 of the Act, a privacy breach means: a) unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, the Personal Information, or b) an action that prevents the agency from accessing the information on either a temporary or permanent basis, and Includes any of the things listed in paragraph (a) or an action under paragraph (b), whether or not it: a) was caused by a person inside or outside the agency, or b) is attributable in whole or in part to any action by the agency, or c) is ongoing.
Privacy Lead	One or more individuals responsible for privacy matters arising within a business division.
Te Pūkenga Privacy Officer	One or more individuals appointed in accordance with section 201 of the Act. The Privacy Officer for Te Pūkenga is Director Legal.

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

Ngā Kaupapa-Here e hāngai ana | Related policies • Privacy Policy • Official Information Policy
Ngā Tukanga me ngā hātepe | Processes, procedures • Te Pūkenga Data Breach Response Plan
Ture whai take | Relevant legislation