Controlled Document – Refer to NMIT website or intranet for latest version

NMIT PRIVACY PROCEDURE

MOKAMOKA WHAKAAETANGA | APPROVAL DETAILS

Section	Executive		
Approval Date	11.08.2026	**Sponsor**	Director Digital and Information
Next Review	01.01.2029	**Approved by**	SLT

NGĀ WHAKATIKATIKA | AMENDMENT HISTORY

Version	Effective Date	Created/ Reviewed by	Reason for review / comment
1	01.07.2026	Privacy Officer	New

Mō wai me te whānuitanga | Audience and scope

These procedures apply to:

(a) All employees of NMIT, including contracted staff and secondees providing services for NMIT; and those on fixed term contracts (collectively referred to as kaimahi in this policy); and

(b) All governors of NMIT including members and advisors of NMIT Council and governance committees or boards (collectively referred to as governors in these procedures).

Te Pūtaki | Purpose

These procedures give effect to the NMIT Privacy Policy which should be read in conjunction with this document and the Data Breach Response Plan.

The purpose of these procedures is to ensure NMIT 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.

All principles stated in the Policy apply to these procedures.

Ngā Haepapa | Responsibilities

Role	Responsibilities
Chief Executive Officer	Ensures the Privacy Procedures are reviewed periodically, remain fit for purpose and compliant with legislation.
NMIT Managers and Programme Team Leads	Ensures that ākonga personal information held within their area of responsibility are managed in accordance with these procedures. Responds to requests from ākonga to access personal information held within their area (for example, ākonga files, academic results). Ensures that ākonga personal information is only accessed by authorised kaimahi and is stored securely.
People and Wellbeing Manager	Ensures that kaimahi files containing personal information are retained and disposed of within the timeframes set out in these procedures.
People and Wellbeing kaimahi	Update changes to personal information as soon as notified. Handle requests from governors and kaimahi to access their files. Handle all personnel files as described in these procedures.

Privacy Officer	Submit Notifiable Privacy Breaches to the Privacy Commissioner. Respond to compliance notices and cooperates with investigations or compliance proceedings from the Privacy Commissioner. Notify and confer with the Chief Executive Officer on privacy breaches, to determine whether it is a Notifiable Privacy Breach. Record all Privacy Breaches in the Privacy Breach Register.
NMIT kaimahi	Promptly report any privacy breaches to the Privacy Officer. Promptly forward any compliance notices or other correspondence received from the Privacy Commissioner to the Privacy Officer. If responsible for engaging contractors or consultants, ensure contractors and consultants understand their obligations under the Act and undertake to comply with the Policy and these procedures. If responsible for managing ākonga personal information within their area, ensure it is accurate and up to date, and managed in accordance with these procedures. Notifies their manager of any requests for access to ākonga personal information.

Ngā Hātepe | Procedure

1. HEALTH INFORMATION PRIVACY CODE 2020

1.1 When NMIT provides health services the Health Information Privacy Code 2020 (the **Privacy Code**) applies to all information obtained while providing this service. Where the Privacy Code applies, its rules replace the Information Privacy Principles in this procedure to the extent of any inconsistency.

1.2 NMIT kaimahi and ākonga involved in providing health services on behalf of NMIT must comply with the Privacy Code, this procedure, and any associated policies or procedures.

1.3 Managers and kaimahi responsible for supervising ākonga providing a service must ensure the ākonga they supervise:

- understand their obligations under the Privacy Code;
- protect the confidentiality of personal and health information obtained while providing the service;
- collect, use, access, disclose, store, retain, and dispose of health information only as authorised by law and relevant policy and procedures; and
- inform clients how their personal and health information will be collected and managed in accordance with the Privacy Code.

2. COLLECTION OF PERSONAL INFORMATION

2.1 All kaimahi shall comply with Information Privacy Principles 1 to 4 prescribed in section 22 of the Act.

2.2 Any forms that collect personal information about governors, kaimahi, ākonga or any other individuals (including both physical and electronic forms, and security surveillance tapes) 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 NMIT Privacy Notice should be used in the context of ākonga.

2.3 Where personal information about governors, kaimahi, ākonga or any other individuals is collected indirectly (i.e. from a source other than the individual concerned), kaimahi must take reasonable steps to notify the individual of the indirect collection of personal information and ensure the collection complies with Information Privacy Principle 3A of the Act, unless an exception under the Act applies.

3. ACCESS TO PERSONAL INFORMATION

3.1 All governors and kaimahi shall comply with Information Privacy Principle 6 prescribed in section 22 of the Act.

Access to ākonga personal information

3.2 Kaimahi may only access personal information relating to ākonga that is necessary for kaimahi to carry out their employment responsibilities.

3.3 No person may remove any NMIT ākonga physical files from a location where it is held unless they are required to so by law or have approval from the relevant Manager or equivalent.

3.4 Kaimahi who receive a request from ākonga wishing to view their personal information (digital or physical) are responsible for promptly discussing the request with the relevant Manager who, if approved, will arrange for kaimahi to be present during the viewing.

3.5 Ākonga must not remove any information from, or alter any part of, their physical NMIT file.

3.6 Any 'evaluation material' (as referred to in section 50 of the Privacy Act) 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 Manager (or equivalent) and with the written consent of the person who supplied the evaluation material, unless otherwise required by law.

3.7 Managers responsible for managing ākonga personal information within their respective areas are responsible for ensuring the personal information is retained and disposed of within the timeframes set out section 18 of these procedures.

Access to governor or kaimahi files

3.8 Subject to the provisions of these procedures and any limitations specified in the Act, governors and kaimahi have the right to access their own personal information.

3.9 Individuals should request permission from the People and Wellbeing team if they wish to access their file.

3.10 Individuals must not remove any information from, or alter any part of, their personnel file. The original file must stay in a secure location at NMIT.

3.11 Individuals may request a copy of any document or extract from their file.

3.12 Any "evaluative material" about governors 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 governors 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.

4. CORRECTIONS TO PERSONAL INFORMATION

4.1 All governors and kaimahi shall comply with Information Privacy Principle 7 prescribed in section 22 of the Act.

4.2 Governors and kaimahi may at any time request corrections to their personal information. A request for correction must be noted in the individual's record.

4.3 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 NMIT to take reasonable steps to ensure that the information is accurate, up to date, complete, and not misleading.

4.4 If the person who maintains the file does not agree to the correction, they must ensure that any statement provided by the individual is able to be viewed alongside the original information.

5. MAINTAINING PERSONAL INFORMATION

5.1 All kaimahi shall comply with Information Privacy Principle 8 prescribed in section 22 of the Act.

5.2 Before using or sharing personal information, kaimahi must take reasonable steps to ensure the information is accurate, up to date, complete and relevant, and that the information is not misleading.

5.3 Kaimahi who require access to kaimahi information to carry out their employment duties / role responsibilities may maintain personal information relating to individuals to the extent that the information is required to carry out their employment duties / role responsibilities.

6. STORAGE AND SECURITY OF PERSONAL INFORMATION

6.1 All kaimahi must comply with Information Privacy Principles 5 and 9 prescribed in section 22 of the Act.

6.2 Physical files containing personal information must be stored in a secured and locked storage space. Kaimahi responsible for these files are also responsible for their security.

6.3 Physical files containing personal information will not be removed from the premises of NMIT except as permitted under these procedures. Where information is removed from NMIT premises (excluding kaimahi files which should never be removed from NMIT premises), it will be kept safe and secure at all times, including:

(a) Information must be stored in zipped up laptop bag 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 have the information in a car, it is placed under the seats or in the boot.
(d) Information is not left unattended at any time during travel.
(e) Upon reaching the destination, the information must be brought inside and kept behind a locked door and not in a communal area.

6.4 Electronic files containing personal information must be stored only in approved NMIT business systems and locations and must not be stored on personal devices, unauthorised applications or other locations that have not been approved by ITCS. Kaimahi responsible for electronic files are responsible for ensuring that personal information is kept secure and is only accessible to authorised individuals.

6.5 Kaimahi must ensure that, when viewing ākonga or kaimahi information either online or in physical format, no unauthorised person is able to view the information.

6.6 Personal information shall not be kept for longer than is required for the purposes for which NMIT collected the information.

6.7 The People and Wellbeing Manager is responsible for ensuring that personal information relating to kaimahi (including personnel files) is retained and disposed of within the timeframes set out in section 18 of these procedures.

6.8 Where personal information relating to kaimahi is held outside of People and Wellbeing, the Manager responsible for that area is responsible for ensuring that the information is retained and disposed of within the timeframes set out in section 18 of these procedures.

7. ONLINE SECURITY OF PERSONAL INFORMATION

7.1 The ITCS team is responsible for the security of electronic management systems used to collect and manage personal information relating to NMIT kaimahi and ākonga and must ensure that:

(a) Access to electronic management systems for NMIT 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 NMIT responsibilities.
(b) Stored personal information is backed up in an appropriate manner.

7.2 Kaimahi who are authorised to access electronic management systems containing personal information must comply with NMIT's ICT Security Policy, and:

(a) Use those systems only for authorised NMIT purposes.
(b) Access only the personal information required to perform their duties.
(c) Ensure personal information accessed through those systems is handled appropriately and securely.
(d) Be responsible and accountable for all activities undertaken using their user credentials, including any misuse of the systems or personal information accessed through them.

8. USE OF PERSONAL INFORMATION

8.1 All governors and kaimahi shall comply with Information Privacy Principle 10 prescribed in section 22 of the Act.

8.2 Governors and kaimahi must only use personal information relating to ākonga, governors, kaimahi or another person for the purpose for which that information was collected, unless permitted under one of the exceptions listed in the Act, for example:

- The purpose for which the information is to be used is directly related to the purpose for which the information was collected.
- The information is to be used in a form in which the individual concerned is not identified.
- Written consent has been obtained from the individual concerned to use the information for another purpose.
- The use of the information for another purpose is necessary to prevent or lessen a serious threat to:
  - public health or public safety; or
  - the life or health of the individual concerned or another individual.

9. DISCLOSURE OF PERSONAL INFORMATION

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

9.2 Kaimahi must not disclose any personal information relating to any ākonga or kaimahi to any person or agency (other than to authorised members of NMIT 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.
(c) Disclosure is necessary to avoid endangering someone's health or safety.
(d) They are required to by law (e.g. to assist Police with detecting, investigating or prosecuting an offence).

Where kaimahi believe an exception applies, they must raise this with their manager prior to disclosing any personal information. In exceptional circumstances, for example in response to a search warrant, approval from the Chief Executive (or delegate) may be required before disclosing personal information without consent.

9.3 Kaimahi must exercise particular care not to divulge personal information when using social media.

Disclosure of personal information about ākonga to third parties

9.4 Any requests for personal information relating to ākonga (whether prospective, current or former) must be discussed with the Manager of the relevant area where the ākonga information originated.

9.5 Kaimahi must not include personal information about ākonga in any material issued or made available to others without the appropriate authority unless disclosure is permitted or required under the Privacy Act 2020 or another legal obligation.

9.6 NMIT may be required to provide personal information without ākonga consent due to a legal obligation or lawful authority (for example, in response to a search warrant). Relevant kaimahi are required to assist the Privacy Officer with identifying, gathering and providing requested information to enable NMIT to comply with its obligations under the Act.

9.7 Kaimahi may disclose whether ākonga have obtained a qualification from NMIT if the qualification was awarded at a public graduation ceremony and/or the qualification was published in a graduation booklet.

9.8 If a qualification was not awarded at a public ceremony (whether in person or in absentia) and/or published in a graduation booklet, the written permission of the ākonga must be obtained before the information can be released.

9.9 Where personal information needs to be published or displayed to a group (for example, examination results), the least identifying information necessary should be used. Where appropriate, this may include using ākonga ID numbers instead of names or providing the information directly to the ākonga.

Disclosure of personal information about kaimahi to third parties

9.10 Kaimahi responsible for maintaining personal information including personnel files must ensure the information is retained and disposed of in accordance with the applicable retention and disposal timeframes set out in these procedures.

9.11 Any requests for personal information relating to kaimahi (whether prospective, current or former) must be referred to the People and Wellbeing team. In cases of doubt, People and Wellbeing kaimahi shall seek the advice of the Privacy Officer before disclosing any information.

9.12 NMIT 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.

9.13 Relevant kaimahi may provide personal information relating to kaimahi where necessary to enable NMIT to meet its obligations under its insurance policies, provided the disclosure is authorised and consistent with the Act.

Disclosure of information outside of New Zealand

9.15 NMIT 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 NMIT that the recipient may not be required to protect the information in a way that provides comparable safeguards to New Zealand's privacy laws);
(b) the recipient is carrying on business in New Zealand and would accordingly be subject to the Act;
(c) the recipient is subject to privacy laws that provide comparable safeguards to New Zealand's privacy laws; or
(d) NMIT has an agreement with the recipient that requires the recipient to comply with sufficient privacy and confidentiality safeguards.

9.16 Where NMIT collects and uses personal information or 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. Where initiatives or changes in processes are proposed that would notably alter how personal information from overseas is collected and used, legal counsel should be consulted.

Projects involving personal information – use of Privacy Impact Assessments

9.17 A Privacy Impact Assessment (PIA) is a useful tool to help assess and mitigate risk to changes involving 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 the following applies:

(a) The proposed change alters the collection, storage and use of disclosure of personal information.
(b) The personal information is considered sensitive.
(c) The change would be contrary to 'customer' expectations or puts a significant amount of information at risk.

9.18 If kaimahi are unsure whether a PIA is required, complete the Privacy Analysis (Appendix A) in the PIA template to determine whether a full Privacy Impact Assessment is required, and consult with the Privacy Officer for further guidance.

10. USE OF UNIQUE IDENTIFIERS

10.1 All kaimahi shall comply with Information Privacy Principle 13 prescribed in section 22 of the Act.

10.2 NMIT assigns its own unique identifier to individuals only where necessary for operational purposes.

10.3 Kaimahi who assign, collect, use or disclose unique identifiers must do so only for authorised business purposes and must ensure appropriate safeguards are in place to protect them from unauthorised access, disclosure, misuse or identity theft.

11. INFORMATION COLLECTED FROM NMIT'S WEBSITE AND ONLINE MARKETING

11.1 NMIT 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 NMIT 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.

11.2 Third-party vendors display advertisements for NMIT 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.

12. BREACHES OF PRIVACY

12.1 In accordance with sections 114 and 115 of the Act, NMIT must notify the Privacy Commissioner and affected individual(s) of any Notifiable Privacy Breach or, where notification to affected individuals is not reasonably practicable, give public notice of the breach.

12.2 Where a suspected privacy breach is identified, kaimahi must immediately notify the Privacy Officer and complete the Report a Privacy Breach form. The Privacy Officer, in conjunction with the Director of Digital and Information and in consultation with the Chief Executive Officer, will assess the breach to determine whether it is a Notifiable Privacy Breach and what action is required, having regard to the requirements of sections 115 and 116 of the Act. The Privacy Breach Risk Assessment Matrix may be used to support this assessment.

12.3 Where a Notifiable Privacy Breach has occurred, the Privacy Officer will coordinate all required actions, including any notifications to the Privacy Commissioner, affected individuals, or public notification, in accordance with the Act and the Data Breach Response Plan (if activated).

12.4 Any public notifications of privacy breaches will be made available on NMIT's website.

12.5 All privacy breaches (including suspected and near-miss) are to be reported to the Privacy Officer so the Privacy Breach Register is maintained.

13. REQUESTS UNDER THE PRIVACY ACT

13.1 Section 40 of the Act allows any individual or their representative to request access to their personal information held by NMIT.

13.2 Individuals may request access to their personal information held by NMIT by emailing privacyofficer@nmit.ac.nz.

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

13.4 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 the Privacy Officer 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 NMIT operations,
(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.

13.5 If an extension is required, kaimahi dealing with the information request must notify the Privacy Officer as soon as practicable and, in any event, before the expiry of the original time limit.

14. EXCEPTIONS – WITHHOLDING OF PERSONAL INFORMATION

14.1 A request by an individual for access to their information held by NMIT 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.

14.2 Requests for personal information by any other person or agency other than the individual to whom the information relates are not Information Privacy Principle 6 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.

14.3 In these circumstances (excluding where the requester is the agent or representative of the individual of whom the information relates), kaimahi receiving the request are to forward it promptly to OIA@nmit.ac.nz.

15. BEFORE RESPONDING TO A REQUEST

15.1 Before responding to a privacy request, NMIT must meet the criteria specified in section 57 of the Act, including without limitation, the requirements specified in 14.2 to 14.4 (inclusive) of these procedures.

15.2 NMIT must take reasonable steps to verify the identity of the requester before providing personal information. Verification may include, but is not limited to:

(a) Where the requester is personally known to the kaimahi receiving the request, confirming their identity.

(b) Verifying the requestor through an NMIT-controlled contact method (e.g. where information is supplied by email or post, the email address or postal address matches the corresponding contact details held by NMIT.
(c) Requesting suitable identification where the request is made in person or where identity cannot otherwise be reasonably verified (e.g. current New Zealand drivers licence, passport, or 18+ card).
(d) Obtaining evidence of authority where the request is made by a representative or agent of the individual.

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

15.4 Where information is requested by a representative or agent of the individual, NMIT must obtain sufficient evidence of that authority before providing any personal information.

16. THE PRIVACY COMMISSIONER

16.1 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://www.privacy.org.nz/your-rights/making-a-complaint-to-the-privacy-commissioner/

16.2 All enquiries, correspondence, or other communications received by NMIT from the Office of the Privacy Commissioner regarding compliance with the Act must be promptly forwarded by kaimahi to the Privacy Officer.

17. RECORDKEEPING

17.1 The Privacy Officer will ensure full and accurate records are maintained for:

(a) the Privacy Register;
(b) all Privacy Act requests and breaches that are communicated to the Privacy Officer;
(c) all investigations and/or compliance proceedings from the Privacy Commissioner; and

that these records are saved into the relevant folder within the Privacy Register in accordance with this procedure.

18. RETENTION PERIODS

18.1 In accordance with the Public Records Act, and in broad terms, the retention periods for documents containing personal information are set out below.

Retention Periods – ākonga personal information including ākonga files

Information	Retain for …
Scholarship applications, assessment and examination scripts and other similar documents	12 months from last information entry date then destroy
Ākonga files	7 years from last information entry date then destroy
Ākonga enrolment material	10 years from last information entry date then destroy
Details of qualifications, courses studied and final assessment results	Permanently

Retention periods – kaimahi personal information including personnel files

Information	Retain for …
Chief Executive Officer and second-tier managers' personnel files	10 years from last information entry date then transfer to Archives New Zealand
Personnel files of 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 New Zealand
Kaimahi personnel files (for all other kaimahi) who left NMIT	7 years from last information entry date then destroy
Kaimahi personal information held outside of official personnel files	Destroy when administratively no longer required

Retention periods – CCTV

Information	Retain for …
Security surveillance tapes	Until administratively no longer required then destroy

18.2 In accordance with the Public Records Act the retention periods for documents relating to privacy information requests and complaints are set out below.

Retention Periods – privacy requests and complaints

Information	Retain for …
Correspondence regarding requests for information, communication with the Privacy Commissioner, investigations into complaints that set precedent	10 years then transfer to Archives New Zealand
Correspondence regarding requests for information, communication with the Privacy Commissioner, investigations into complaints that do not set precedent	7 years from last information entry date then destroy

Pūrongo me te Whakapūmau | Reporting and Assurance

Regular reports will be submitted to Council and/or a committee of Council:	
Submitted by	Chief Executive Officer (CEO)
Submitted to	Council
What must be reported	Notifiable privacy breaches, compliance notices, investigations and outcomes
Reporting cadence	Monthly Report
Is immediate escalation required for material events?	Yes; immediate escalation required by: • the Privacy Officer to Council Chair if a protected disclosure involves the CEO • the CEO to Risk and Audit Committee if a protected disclosure involves the Council Chair

Ngā Tikanga | Definitions

Term	Definition
Information Privacy Principals	The information privacy principles prescribed in section 22 of the Act.
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) whether the personal information is protected by a security measure and any other relevant matters.
Personal Information	Any information that directly or indirectly identifies an individual, regardless of format. This includes, but is not limited to, name, birth date, contact details, academic information, images, IRD number, and banking details.
Privacy Officer	One or more individuals appointed in accordance with section 201 of the Act, responsible for privacy matters arising within NMIT.

Ngā Hononga ki Tuhinga kē | Links to other documents

NGĀ KAUPAPA-HERE E HANGAI ANA | RELATED POLICIES

NMIT Privacy Policy
NMIT Information and Records Management Policy
NMIT Official Information Act Policy
NMIT ICT Security Policy

NGĀ TUKANGA ME NGĀ HĀTEPE | RELATED PROCESSES, PROCEDURES

NMIT Information and Records Management Procedure
NMIT Official Information Act Procedure
NMIT Data Breach Response Plan

TURE WHAI TAKE | RELEVANT LEGISLATION

Privacy Act 2020
Official Information Act 2020
Public Records Act 2005
Office of the Privacy Commissioner https://www.privacy.org.nz/

NGĀ TAPIRITANGA | APPENDICES

Privacy Breach Checklist
Notifiable Privacy Breach form