Privacy Procedures

Audience and scope

These procedures are relevant to all employees of Manukau Institute of Technology and Unitec (**MIT and Unitec**), including contracted staff, consultants and secondees providing services for MIT and Unitec, and those on fixed-term contracts (collectively referred to as **staff** in this procedure). Where relevant, these procedures should also be followed by all those operating at a governance level, including Council members and members of Council's advisory committees (collectively referred to as **Council members** in this procedure).

This procedure applies to Personal Information collected and held by MIT and Unitec in respect of any identifiable individual.

Document management and control

Version number	1.1	**Date of approval**	15 April 2026
Approval authority	Executive Leadership Team	**Date of next review**	1 April 2028
Policy sponsor	Legal Director - Tāmaki	**Policy contact person**	Legal Director - Tāmaki

Amendment history

Version	Effective date	Created/reviewed by	Reason for review/comment
1.0	1 January 2026	Director Legal	New procedure
1.1	15 April 2026	Legal Director - Tāmaki	Minor updates

Table of Contents

Privacy Procedure

1. Purpose

1.1. The purpose of this procedure is to ensure MIT and Unitec 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.

1.2. This procedure should be read in conjunction with the Privacy Policy.

2. Collection of Personal Information

2.1. All staff shall comply with information Privacy Principles 1 to 4 prescribed in section 22 of the Act (refer to the Appendix in the Privacy Policy).

2.2. Any forms that collect Personal Information about Council members, staff, students 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. MIT and Unitec's standard Privacy Notice should be used in the context of students.

Recruitment of staff

2.3. The Director People and Culture 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.

2.4. Without limiting the foregoing, Council members and staff 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 staff member of MIT and Unitec, Council members and staff may consult the applicant's personnel file.

Information collected from MIT and Unitec's website and online marketing

2.5. MIT and Unitec 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 MIT and Unitec 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.

2.6. Third-party vendors (such as Google) display advertisements for MIT and Unitec 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.

3. Access to Personal Information

3.1. All Council members and staff shall comply with Information Privacy Principle 6 prescribed in section 22 of the Act (refer to the Appendix in the Privacy Policy). Any requests by any

individual or their representative for access to their Personal Information held by MIT and Unitec shall be dealt with in accordance with section 10 of this procedure.

4. Maintaining Personal Information

4.1. All Council members and staff shall comply with Information Privacy Principles 7 and 8 prescribed in section 22 of the Act (refer to the Appendix in the Privacy Policy).

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

4.3. All Council members and staff must ensure that their current name and contact details provided to MIT and Unitec are correct and must notify People and Culture staff when any changes occur.

Corrections to files

4.4. Staff and Council members may at any time request corrections to their Personal Information. A request for correction must be noted in the individual's record.

4.5. 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 MIT and Unitec to take reasonable steps to ensure that the information is accurate, up to date, complete, and not misleading.

4.6. If the person who maintains the file does not agree to the correction, they must ensure that any statement provided by the relevant Council member, student or staff member is able to be viewed alongside the original information.

Maintaining staff files

4.7. Staff who require access to staff or Council member information to carry out their employment duties / role responsibilities may maintain Personal Information relating to staff and Council members to the extent that the information is required to carry out their employment duties / role responsibilities.

5. Storage and Security of Personal Information

5.1. All Council members and staff must comply with Information Privacy Principles 5 and 9 prescribed in section 22 of the Act, the Public Records Act 2005 and the applicable Records Management Policy.

5.2. 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.

5.3. Hard copy files containing Personal Information shall not be removed from premises of MIT and Unitec, except as permitted under the Privacy Policy or this procedure.

Access to student files

5.4. Staff may access Personal Information relating to students only if that is necessary for the staff to carry out their employment responsibilities.

5.5. No person may remove any student 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 student files removed from a campus must be

kept safely and securely at all times in accordance with section 5.6 of these Privacy Procedures.

5.6. Where information is removed from MIT and Unitec's premises (excluding staff files which should never be removed from MIT and Unitec's premises except in accordance with these procedures or the approval of 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 staff member 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.

Access to Council member and staff files by other staff or Council members

5.7. Authorised personnel may access staff and Council member 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 Council members and the Chief Executive

b. members of the Executive Leadership Team

c. line managers (permitted access to the staff files of those they manage)

d. Staff employed in People and Culture team; and

e. Executive Assistants and administrators acting on the direction of those Council members and staff referred in paragraphs 2.17a) – d) (inclusive)

f. any other staff expressly authorised by the Director People and Culture or the Chief Executive.

Online security of Personal Information

5.8. The Digital team are responsible for the security of the electronic management systems used to collect and manage Personal Information relating to staff and students and must ensure that:

a. **Student and staff information**

i. Access to MIT and Unitec's electronic management systems shall be granted to staff only to the extent that each staff member requires access to the relevant electronic management system in order to carry out their responsibilities for MIT and Unitec.

ii. Stored Personal Information (student and staff) must be backed up in an appropriate manner.

b. **Staff information**

i. Managers are given access only to the details of the staff they are responsible for.

ii. Appropriate access is given to managers who require organisation-wide information in order to meet MIT and Unitec's business requirements, provided that the access is generic in nature and does not identify any staff, unless identification is necessary for the particular business transaction.

5.9. Staff must ensure that, when viewing student or staff information, no unauthorised person is able to view the information.

Offsite storage

5.10. 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.

Retention periods

5.11. Personal Information shall not be kept for longer than is required for the purposes for which MIT and Unitec collected the information.

5.12. The Director People and Culture (or their delegate) is responsible for ensuring that staff files containing Personal Information are retained and disposed of within the timeframes set out below.

5.13. In accordance with the Public Records Act 2005, and in broad terms, the retention periods for documents are as set out below.

5.14. Retention periods – student files

Information	Retain for…
Details of qualifications, courses studied and final assessment results	Permanently
Student 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

5.15. Retention periods – staff files

Information	Retain for…
Staff files for Chief Executive and second-tier managers	10 years from last information entry date then transfer to Archives NZ
Staff 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 staff 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

Information	Retain for…
Staff files for all other staff who have left MIT and Unitec	7 years from last information entry date then destroy

6. Use of Personal Information

6.1. All Council members and staff shall comply with Information Privacy Principle 10 prescribed in section 22 of the Act (refer to the Appendix in the Privacy Policy).

6.2. Council members and staff must only use Personal Information relating to any student, Council member, staff 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.

7. Disclosure of Personal Information

7.1. All Council members and staff shall comply with Information Privacy Principles 11 and 12 prescribed in section 22 of the Act.

7.2. Staff must not disclose any Personal Information relating to any student or staff member to any person or agency (other than to authorised members of MIT and Unitec's staff), including parents, partners and employers of that student or staff member, 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).

7.3. Staff must exercise particular care not to divulge Personal Information when using social media.

7.4. When a staff member receives a request for Personal Information that relates to someone other than the requester, they must consult with the Privacy Officer if they are unsure whether or not to disclose that information.

Disclosure of Personal Information relating to students

7.5. Any requests for Personal Information relating to students (whether prospective, current or former) must be referred to the Enrolments team. In cases of doubt, Enrolments staff shall seek the advice of the Privacy Officer before disclosing any information.

7.6. Staff must not include any Personal Information about students in any material issued, unless they have the prior written consent of that student.

7.7. Staff may disclose whether students have obtained a qualification from MIT and Unitec if the qualification was awarded at a public graduation ceremony and/or the qualification was published in the graduation booklet.

7.8. 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 student must be obtained before the information can be released.

7.9. Examination results must be published only using appropriate student ID numbers rather than student names or other identifiers, unless published directly to the student and no other person.

Disclosure of Personal Information related to staff

7.10. Any requests for Personal Information relating to staff (whether prospective, current or former) must be referred to the People and Culture team. In cases of doubt, People and Culture staff shall seek the advice of the Privacy Officer before disclosing any information.

7.11. MIT and Unitec may include details of staff (such as name, work contact details, title and areas of expertise of that staff) in publications including promotional brochures and MIT and Unitec's websites.

7.12. MIT and Unitec may provide Personal Information as necessary to meet its obligations as an insured party under its staff insurance policy.

Disclosure of Personal Information outside New Zealand

7.13. MIT and Unitec 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 MIT and Unitec 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. MIT and Unitec 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 New Zealand

7.14. Where MIT and Unitec 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 Privacy Officer should be consulted.

8. Privacy Impact Assessments

8.1. A Privacy Impact Assessment (**PIA**) is a useful tool to help assess and mitigate risk for 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 of the following applies:

a. Does the proposed change involve or alter the collection, storage, use or disclosure of personal information?

b. Is the personal information considered sensitive?

c. Would the change be contrary to 'customer' expectations or put a significant amount of information at risk?

8.2. If staff are unsure whether a PIA is required, the Privacy Officer should be consulted for guidance.

9. Breaches of Privacy

9.1. In accordance with section 114 of the Act, MIT and Unitec is required to report Notifiable Privacy Breaches to the Privacy Commissioner. Section 115 of the Act also requires that MIT and Unitec 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.

9.2. All staff must promptly report any privacy breaches to the Privacy Officer. The Privacy Officer 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 (or equivalent) must be informed immediately so that they can ensure immediate remedial action.

9.3. Where a Notifiable Privacy Breach has occurred, the Privacy Officer will notify the Chief Executive and the Executive Leadership Team. The Privacy Officer will determine 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.

9.4. Any public notifications of privacy breaches shall be made available on MIT and Unitec's websites.

10. Requests under the Privacy Act 2020

10.1. Section 40 of the Act allows any individual or their representative to request access to their Personal Information held by MIT and Unitec.

Time limits

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

10.3. 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) 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 the operations of MIT and Unitec,

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.

10.4. If an extension is required, the staff member dealing with the information request must notify the Chief Executive (or delegate) or the Privacy Officer as soon as practicable and, in any event, before the expiry of the original time limit.

Exceptions – withholding of Personal Information

10.5. A request by an individual for access to their information held by MIT and Unitec 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.

10.6. 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

10.7. Before responding to a privacy request, MIT and Unitec must meet the criteria specified in section 57 of the Act, including without limitation, the requirements specified in sections 10.8 to 10.10 (inclusive) of this procedure.

10.8. MIT and Unitec 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 MIT and Unitec holds for that individual (if any)

b. where information is supplied by post, the postal address must match the postal address held on records MIT and Unitec 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.

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

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

11. The Privacy Commissioner

11.1. 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://privacy.org.nz/your-privacy/how-to-complain/.

11.2. All enquiries, correspondence, or other communications received by MIT and Unitec from the Office of the Privacy Commissioner regarding compliance with the Act must be promptly forwarded by staff to the Privacy Officer.

12. Responsibilities

Role	Responsibilities
Director People and Culture	• Ensure that staff 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.
Council members	• 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 the Privacy Officer.
People and Culture staff	• Update changes to Personal Information as soon as you are notified. • In cases of doubt, seek the advice of the Privacy Officer before disclosing any information. • Handle requests from staff to access their files as laid out in this procedure. • Handle all files described in this procedure in line with this procedure and the Privacy Policy. • All points outlined in the Privacy Policy and this procedure are followed in line with your role.
Staff	• 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 the Privacy Officer. • Promptly reports any breaches to the Privacy Officer • Assists with requests made to MIT and Unitec under the Act, where required. • Promptly forwards any compliance notices or other correspondence received from the Privacy Commissioner to the Privacy Officer

Role	Responsibilities
	• If responsible for engaging contractors or consultants, ensures contractors and consultants understand their obligations under the Act and undertake to comply with this policy.
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. This includes responding to compliance notices, cooperating with investigations or complaint proceedings and submitting a notice of any Notifiable Privacy Breach.

13. Definitions

Term	Definition
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.
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
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:

Term	Definition
	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 officer	One or more individuals appointed in accordance with section 201 of the Act. MIT and Unitec's Privacy Officer is the Legal Director - Tāmaki (or in the Legal Director - Tāmaki's absence, the Legal Counsel).

14. Relevant legislation

- Privacy Act 2020
- Public Records Act 2005
- Official Information Act 1982

15. Related documents

- Privacy Policy
- Official Information Policy
- Records Management Policy