Privacy Policy

Policy Title	Privacy Policy
Classification	Student Policy Library, Administrative
Reference Code	SPL00005
Version	3
Approval By	Academic Board
Approval Date	19 May 2023
Effective Date	19 May 2023
Review Date	19 May 2026

Scope

This policy applies to all members of NTI, including students and all staff as defined below.

Definitions

Disclosure of Information	Communication or transfer of information outside of NTI.
Health Information	Personal information, whether or not recorded in a health record relating to the health, an illness or a disability of the individual; or collected by a health service provider in relation to the health, an illness or a disability of an individual.
Law Enforcement	Law enforcement agencies include: a) Police Force of NSW or of another State or Territory of Australia b) NSW Crime Commission c) Australian Federal Police d) Australian Crime Commission e) Director of Public Prosecutions of NSW, another State or Territory of Australia or the Commonwealth f) Department of Corrective Services g) Department of Juvenile Justice h) Office of the Sheriff of NSW i) Australian Security Intelligence Organisation j) Australian Signals Directorate k) jurisdictions beyond Australia
NTI Staff	For the purposes of this policy – all employees of NTI, including:

	a) casual employees; b) conjoint and visiting appointees; c) consultants and contractors; d) agency staff; e) emeriti; f) members of NTI committees; and g) any other person appointed or engaged by NTI to perform duties or functions for NTI, e.g. volunteers
Personal Information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not.
Sensitive Information	In relation to an individual – information or an opinion about an individual's racial or ethnic origin, immigration status, political opinions, memberships of political, professional and trade associations and unions, religious and philosophical beliefs, sexual orientation or practices, criminal history, health information, and genetic and biometric information. In relation to NTI – organisational financial data, assessment material and results, internal directories and organisational charts, internal planning documents, research data containing personal information, data considered commercial in confidence.
Use of Information	Communication or handling of information within NTI.

Policy Statement

Nan Tien Institute (NTI) is committed to protecting the privacy of its students, employees and others who interact with it, while undertaking learning, teaching, research, engagement, and associated administrative activities or support services.

This policy outlines NTI's ongoing obligations in respect of how it manages personal information.

NTI is subject to and must comply with Privacy and Personal Information protection Act 1998 and the NSW Health Records and Information Privacy Act 2002 when collecting, using, disclosing, storing and disposing of an individual's personal and health information.

Systems and Procedures

COLLECTION OF INFORMATION

1. NTI will only collect, hold, use and disclose personal information to enable NTI to meet legal and compliance obligations and where it is reasonably necessary or related to NTI's functions and activities.
2. NTI collects and holds personal information in a number of ways, including:
   a) because it is required to provide a service which has been requested – e.g. to implement a reasonable adjustment plan
   b) because it has been provided to NTI – e.g. by applying for admission or employment, participating in online forums, registering to attend an event, making a complaint
   c) because of an individual's previous or current relationship with NTI – e.g. through alumni relations
   d) because NTI is required by law to collect it – e.g. because of higher education and immigration

laws

3. NTI will ensure that the personal and health information it collects from individuals is relevant to its functions, accurate, up to date and not excessive, and that collection does not intrude to an unreasonable extent on the personal affairs of the individual.
4. NTI collects information from individuals directly, unless they have authorised collection of the information from someone else, or they lack capacity (including temporarily) to provide the information directly.

AUTOMATED COLLECTION OF INFORMATION

5. NTI also collects information by automated means including:
   a) security cameras located throughout the NTI campus;
   b) swipe cards utilised to access sites throughout NTI campus;
   c) digital and online means (this includes NTI's website and social media);
   d) NTI's network and other technology and communications systems (such as WiFi) that record login and other identifiers of users or their devices;
   e) audio, video or images taken or live streaming of learning and teaching activities and events (including graduation ceremonies, lectures and tutorials).
6. Where possible, NTI will take steps to ensure that automatic collections are open and transparent through relevant notices or signage, terms and conditions or other methods of communication.

UNSOLICITED PERSONAL INFORMATION

7. NTI may receive personal information about a member of the NTI community that it has not actively collected and sought, from third parties such as law enforcement agencies. NTI will treat this as unsolicited information and does not have to comply with the Australian Privacy Principles in relation to its collection. However, the requirements of this policy will apply to the storage, use or disclosure of unsolicited information containing personal information.

USE AND DISCLOSURE OF PERSONAL INFORMATION

8. NTI will not use or disclose personal information it holds unless:
   a) the use or disclosure of the information is directly related to the primary purpose for which the information was collected and there is no reason to believe that the individual concerned would object; or
   b) the individual concerned is reasonably likely to be aware or has been made aware of the disclosure; or
   c) the use or disclosure of the personal health information is necessary to deal with a serious and imminent threat to an individual's life or health; or
   d) the disclosure of the personal information is necessary to assist in a state of emergency, or to prevent a threat to public health and safety; or
   e) the individual provides consent to any other use or disclosure. (consent may be withdrawn at any time)
9. NTI will only use or disclose personal information without an individual's consent in limited circumstances, including where the use or disclosure relates to law enforcement and related matters such as:
   a) disclosing information to a law enforcement agency for the purpose of ascertaining the whereabouts of an individual who has been reported or police as a missing person; or
   b) disclosing information to a law enforcement agency in order to investigate an offence where there are reasonable grounds to believe that an offence may have been committed; or

c) where the use or disclosure of personal information is permitted or required under an Act or any other law;
d) where the use or disclosure of health personal information is necessary for the training of employees.

DIRECT MARKETING

10. NTI will not use or disclose personal information for direct marketing, unless:
    a) consent has been obtained from the individual consent may be withdrawn at any time)
    b) the marketing is directly related to the purpose for which the information was collected; or
    c) the individual would reasonably expect NTI to use or disclose the personal information for that purpose.
    d)

TRANSBORDER DATA FLOW OF PERSONAL INFORMATION

11. In the course of its business, NTI may provide or receive personal information to or from organisations outside of New South Wales (including outside Australia). This includes information regarding overseas students. NTI will only provide this information to those organisations where:
    a) NTI believes the recipient is subject to a law, binding scheme or contract that upholds principles for fair handling of the information that are substantially similar to the information principles under the Privacy and Personal Information Privacy Act 1998; or
    b) an individual expressly consents to the transfer of the information; or
    c) the transfer is necessary for the performance of a contract between the individual and NTI; or
    d) the transfer is necessary for the performance of a contract in the interests of an individual between NTI and a third party (e.g. arrangements with a third party providers of cloud-based technologies, data storage facilities or digital services); or
    e) the transfer is otherwise required or permitted by law.
12. NTI will not transfer personal information to organisations outside New South Wales, except as permitted under the Privacy and Personal Information Privacy Act 1998, and the circumstances referred to in clause 11 of this policy.

QUALITY OF PERSONAL INFORMATION

13. NTI will take all reasonable steps to ensure that information it collects, uses or discloses is accurate, complete, and up to date, having regard to the purpose for which the information is collected, used or disclosed.
14. NTI relies on the individuals providing that personal information to provide information that is accurate and to notify NTI of any changes to their personal information. Individuals will be normally informed of their obligations at the time the information is collected.

ACCESS TO PERSONAL INFORMATION

15. NTI must, when requested to do so, provide an individual with access to their personal information or health information it holds.
16. NTI must be able to verify the identity of an individual when requests are made to access or amend personal or health information.
17. NTI will allow an individual to access their own personal information held by NTI without unreasonable delay or expense, unless:

a) NTI believes that giving access would pose a serious threat to the health or safety of any individual or to public health and safety, or impact on the privacy of other individuals; or
b) the request for access is frivolous or vexatious; or
c) the information relates to existing or anticipated legal proceedings between NTI and the individual and would not be discoverable in those proceedings; or
d) giving access would prejudice commercially sensitive negotiations; or
e) giving access would be unlawful; or
f) giving access would be likely to prejudice enforcement related activities, or action in relation to serious misconduct.

AMENDMENTS TO PERSONAL INFORMATION

18. NTI will amend personal and health information it holds about an individual at the request of the individual to ensure it is accurate, up to date, complete and not misleading, and taking into account the purpose for which that information was collected.
19. When requested by an individual, NTI will notify any other organisation to which it has disclosed the information of any amendments, unless it is impracticable or unlawful to do so.
20. NTI may refuse to amend information in certain circumstances, including but not limited to:
    a) when the change cannot be made due to system limitations or design;
    b) when the amendment is contentious (e.g. when an employee or a student seeks a change in an NTI decision that they disagree with);
    c) when the change conflicts with any laws, or with NTI requirements with respect to governance and record keeping;
    d) when the change would result in the information being out of date, inaccurate or misleading.
21. If NTI refuses to amend the personal information as requested by an individual, NTI will provide a written statement of reasons and information on mechanisms for complaining about its actions.

SECURITY OF PERSONAL INFORMATION

22. NTI will take all reasonable steps to ensure that personal information is:
    a) held for no longer than necessary (personal information that is no longer necessary to fulfil the identified purposes will be destroyed or erased);
    b) disposed of securely in accordance with approved methods; and
    c) protected to the extent reasonable in the circumstances from loss, unauthorised access, use, amendments or disclosure, and against all other misuse.

COMPLAINTS AND ENQUIRIES IN RELATION TO PRIVACY MATTERS

23. If an individual has concerns about the way NTI is managing their personal information or believes that NTI may have breached their privacy, the matter should be referred to NTI President via email at privacy_enquiry@nantien.edu.au for an internal review.
24. An internal review application must be:
    a) in writing; and
    b) made by the person whose personal information is said to have been the subject of the conduct of NTI; and
    c) addressed to NTI President.
25. Applications for internal review must be lodged within six (6) months from the time the complainant first became aware of the conduct that is the subject of the application.
26. The internal review must be completed by NTI within sixty (60) days from the day on which the application was received. Once a review has been completed, NTI may decide to do one or more of the

following and advise the applicant of the outcome:

a) take no further action; or
b) make a formal apology; or
c) take appropriate remedial action; or
d) give an undertaking that the conduct will not recur; or
e) implement measures to prevent recurrence of the conduct; or
f) escalate the matter to an external investigator.

27. If a complainant is not satisfied with the outcome of the review, or if NTI has not dealt with the matter within sixty (60) days, they may make an application for review to the NSW Civil and Administrative Tribunal.

BREACHES OF PRIVACY

28. A privacy breach occurs when there is unauthorised access to or collection, use or disclosure, loss or disposal of personal information held by NTI (or a third party on behalf of NTI) in contravention of the Privacy and Personal Information Protection Act 1998.
29. Any NTI employee who becomes aware of an actual or potential privacy breach must immediately inform their supervisor and NTI President.
30. NTI President is responsible for ensuring appropriate steps are taken to limit the extent and effect of any breach, and for assessing risks associated with the breach.
31. A breach which is assessed as likely to result in serious harm to individuals whose personal information is involved, is a notifiable data breach. Such data breaches must be notified to the affected individuals and the Office of the Australian Information Commissioner as soon as possible.

ROLES AND RESPONSIBILITIES

32. NTI is responsible for making staff and students aware of this policy.
33. All staff are responsible for complying with NTI's privacy obligations and practices, as specified in this Privacy Policy, and NTI's Code of Conduct, when managing information provided to, or collected by, NTI. This includes attending training or completing online privacy training, as required.
34. NTI President is responsible for NTI's overall compliance with its privacy obligations and for:
    a) providing privacy advice and education to staff; and
    b) responding to enquiries or complaints from individuals on privacy matters; and
    c) implementing and maintaining this Privacy Policy.
35. System owners have the responsibility to:
    a) control access to the systems; and
    b) implement formal procedures for access to the systems; and
    c) regularly conduct a review of user privileges and adjust user roles appropriately; and
    d) close or disable accounts that are no longer required or appropriate.

Legislation and Regulation

The Privacy Act 1988
Australian Privacy Principles
Privacy and Personal Information Protection Act 1998
NSW Health Records and Information Privacy Act 2002
Privacy Amendment (Enhancing Privacy Protection) Act 2012