Ngāti Apa ki te Rā Tō Charitable Trust
Privacy Policy

Policy Statement
NAKTRT will comply with the Privacy Policy stated in this document regarding collection, use, disclosure, storage, and access to Personal Information, in accordance with the Privacy Act 2020.

Rationale
NAKTRT regularly deals with individuals' personal information. As such it has a duty to ensure this personal information is treated appropriately.

Definitions
Personal Information – information about an identifiable individual, – A person's name, address, relationships, employment records, and unique identifiers such as IRD or NHI numbers, or information about their financial position.

Use and Source of Private Data
The likely sources and uses of Personal Information within NAKTRT are listed below, although this may not be considered an exhaustive list:

- Whakapapa records and the membership database
- Scholarship and other financial grant records
- Job Interview records
- Talent database records
- Human Resources records/Employee files

Privacy Training
New staff joining NAKTRT will be a briefed on the requirements of the Privacy Policy (to the degree necessary and relevant to their position) upon their induction. In addition, staff that work directly with Personal Information as part of their role will undergo refresher training as required.

Privacy Breaches
Any requests or complaints received relating to potential breaches of this Policy or issues around Personal Information should be directed to the General Manager who will liaise with the relevant staff member's manager, for determination of a suitable response.

Where necessary / appropriate, a matter may be referred to external authorities or to a formal dispute resolution
procedures.

Employee Monitoring
From time-to-time NAKTRT may choose to monitor its operations for genuine business reasons.

NAKTRT shall be overt regarding any potential monitoring and will inform its employees prior to the implementation of any monitoring systems or surveillance. Potential uses of any monitoring data will be communicated to employees at the time of installation and could include but are not limited to the following: managing work distribution, health and safety, disciplinary purposes, or in the investigation of criminal offences.

Policy Principles
The Privacy Act 2020 has 13 privacy principles that govern the collection, handling and use of personal

information. NAKTRT is committed to always operating withing these principles.

NAKTRT will

- only collect personal information if it is for a lawful purpose and if the information is necessary for that purpose
- only collect personal information directly from the person it is about. Where this is not possible, information will be collected from a 3rd party if:
    - the person concerned gives us permission
    - collecting it in another way would not prejudice the person's interests
    - collecting the information from the person directly would undermine the purpose of collection
    - we are getting it from a publicly available source
- take reasonable steps to make sure that the person knows:
    - why it is being collected
    - who will receive it?
    - whether giving it is compulsory or voluntary
    - what will happen if they do not give you the information

- only collect personal information in ways that are lawful, fair, and not unreasonably intrusive. We will ensure we take particular care when collecting personal information from children and young people.

- make sure that there are reasonable security safeguards in place to prevent loss, misuse, or disclosure of personal information. This includes limits on employee browsing of other people's information.

- where possible, provide access to members own personal information. NAKTRT acknowledges that People have a right to ask for access to their personal information. In most cases we will promptly provide information, however, sometimes there may be good reasons to refuse access. For example, if releasing the information could:
    - endanger someone's safety
    - create a significant likelihood of serious harassment
    - prevent the detection or investigation of a crime
    - breach someone else's privacy

- ensure any persons can correct the information that has been provided to us. A person has a right to ask an organisation or business to correct their information if they think it is wrong. Even if we do not agree that it needs correcting, we must take reasonable steps to attach a statement of correction to the information to show the person's view.

- before using or disclosing personal information, take reasonable steps to check it is accurate, complete, relevant, up to date and not misleading.

- not keep personal information for longer than is necessary.

- generally, only use personal information for the purpose we have collected it. However, we may use it in ways that are directly related to the original purpose, or we may use it another way if the person gives us permission, or in other limited circumstances.

- only disclose personal information in limited circumstances. For example, if:
    - disclosure is one of the purposes for which you got the information

  - the person concerned authorised the disclosure
  - the information will be used in an anonymous way
  - disclosure is necessary to avoid endangering someone's health or safety
  - disclosure is necessary to avoid a prejudice to the maintenance of the law

- only send personal information to someone overseas if the information will be adequately protected. For example:
  - the receiving person is subject to the New Zealand Privacy Act because they do business in New Zealand
  - the information is going to a place with comparable privacy safeguards to New Zealand
  - the receiving person has agreed to adequately protect the information – through model contract clauses, etc. If there are not adequate protections in place, you can only send personal information overseas if the individual concerned gives you express permission, unless the purpose is to uphold or enforce the law or to avoid endangering someone's health or safety.

- only assign a unique identifier to individuals where it is necessary for operational functions i.e., an iwi membership number. A unique identifier is a number or code that identifies a person, such as an IRD or driver's licence number. We will not assign the same identifier as used by another organisation and ensure that the risk of misuse of any unique identifier (such as identity theft) is minimised.