Privacy Policy

|  |  |
| --- | --- |
| **Policy title** | Privacy Policy |
| **Policy owner** | CEO |
| **Version no** | V1 |
| **Version issue date** | 1 May 2022 |
| **Original issue date** | 1 May 2022 |
| **Review date** | 30 November 2023 |

# Purpose

* 1. ATNZ (“**the Organisation**”) collects and uses personal information of individuals in the workplace in accordance with the Privacy Act 2020 (“**the Act**”).
	2. This policy applies to all of the Organisation’s employees and all other workplace participants, for example – job candidates, contractors, volunteers, consultants and visitors (collectively referred to as **Employees** in this policy document.)
	3. The Organisation may collect personal information about an individual either directly from the individual, or from a third party in certain circumstances under the Act.
	4. The Act governs how the Organisation collects, uses, discloses, stores and provides access to ‘personal information’ which is defined as information that is about an identifiable person. The Act sets out twelve ‘information privacy principles’ which specify how personal information should be collected, protected, used and disclosed. These are listed in the Appendix.
	5. The Act requires that the Organisation may only collect, use and/or disclose personal information for a lawful purpose in connection with a function, or activity of the Organisation and where the collection of that information is necessary for that purpose.
	6. Employees and other individuals have rights under the Act, including the right to access and request correction of personal information (subject to certain legislative exemptions).
	7. All staff members must ensure that they comply fully with the information privacy principles and the other provisions of the Act.
	8. This policy should be read in conjunction with the Privacy Guidelines, the Record Management Policy and the Data Breach Response Plan documents. (Data Breach Response Plan is still to come.)

# Policy

### Employer Responsibilities

* 1. The Organisation’s responsibilities under the Act broadly involves the following:
		+ Telling individuals what the Organisation does with their personal information and why;
		+ Keeping personal information safe and secure from any loss and/or unauthorised access, use, modification or disclosure;
		+ Obtaining only the relevant personal information the Organisation needs from individuals in order to provide our services and/or in connection with lawful functions and/or activities of the Organisation;
		+ Only using personal information if the Organisation is reasonably sure it is accurate;
		+ Respecting an individual’s right to access, review and request correction of their personal information.
		+ Notifying the Privacy Commissioner and person(s) affected by any Privacy Breach that has or may cause serious harm.

### Employee Responsibilities

* 1. Employees are responsible for:
		+ Disclosing all relevant information about them as part of their pre-employment application process and any matter relevant to their employment;
		+ Maintaining up-to-date contact information and providing any supporting documentation if required;
		+ Ensuring the privacy of other employees, customers, clients, agents, contractors or any other person or entity that has dealings with the Organisation is protected and is not breached;
		+ Complying with all obligations set out in the Act.
		+ Notifying the Chief Executive Officer of any Privacy Breach immediately that they become aware or suspect that such a breach has occurred.

### General Information

* 1. **Who does the Organisation collect your personal information from?**

The Organisation collects personal information about you from:

* + - You, when you provide that personal information to us, including via our website and any related service, through any registration process and/or through any contact with the Organisation, including telephone or email;
		- Third parties where you have authorised this, or where the information is publicly available;
		- From you directly.

### How the Organisation uses your personal information?

The Organisation may use your personal information:

* + - To verify your identity;
		- To market or provide our services and products to you, including contacting you electronically, for example - by text or email;
		- To undertake pre-employment checks about you;
		- To bill you and to collect money that you owe the Organisation, including authorising and processing credit card transactions;
		- To respond to communications from you, including a complaint;
		- To conduct any formal employment process, for example – performance management, disciplinary action, etc.;
		- To protect and/or enforce the Organisation’s legal rights and interests, including defending any legal claim;
		- For any other purpose authorised by you and/or the Act.

### Disclosing your personal information

* 1. The Organisation may disclose your personal information to:
		+ Any business that supports our services, including any person that hosts, or maintains any supporting IT system or data function, including cloud-based software, storage and/or systems which are associated with the Organisation’s functions and/or activities;
		+ A credit reference agency for the purpose of credit checking you in certain circumstances;
		+ The Ministry of Justice and/or New Zealand Police, or other parties, including former employers for the purposes of pre-employment checks, for example - reference checking;
		+ An agency or other entity that can require us to supply your personal information, for example

– the Privacy Commissioner, Government agencies, law enforcement, etc.

* + - Any other person authorised by you, for example – a legal representative or union.
		- A business that supports our services and products may be located outside New Zealand. This may mean your personal information is held and processed outside New Zealand, for example, cloud storage.

### Protecting and holding your personal information

* 1. The Organisation will take reasonable steps to keep your personal information safe from loss, unauthorised activity/disclosure, or other misuse.
	2. The Act does not stipulate how long personal information should be kept. However, it does state that personal information should not be kept for longer than is required for the purposes for which the information may be lawfully used. Generally, employee records and personnel files will be kept for up to six (6) years following which it will be destroyed.

### Accessing and correcting your personal information

* 1. Subject to certain grounds for refusal set out in the Act, you have the right to access your personal information about you that the Organisation holds and to request a correction to your personal information.
	2. Before you exercise these rights under the Act, the Organisation may require evidence to confirm that you are the individual to whom the personal information relates.
	3. If the Organisation is of the view that the correction is reasonable and it is reasonably able to change your personal information, it may make the correction. If the Organisation does not make the correction, it will take reasonable steps to note on the applicable personal information that you requested the correction.
	4. If you want to exercise either of the above rights, email the Organisation. Your email should provide evidence of who you are and set out the details of your request in writing, for example - the personal

information your request relates to, the correction that you are requesting, what outcome you want, etc.

* 1. While generally free, the Organisation reserves the right to charge you reasonable costs of providing you copies of your personal information or correcting that information and will notify you of any corresponding charges before processing your request.

### Privacy Officer

* 1. The Organisation will appoint a Privacy Officer to assist it to comply with its obligations under the Act, including dealing with privacy related requests. If the Privacy Officer leaves employment, another Privacy Officer will be appointed.
	2. The role of the Privacy Officer is to:
		+ Ensure that the Organisation complies with the Act so far as practically possible;
		+ Deal with privacy requests made to the Organisation for access to, or correction of, personal information;
		+ Be familiar with the Privacy Principles under the Act;
		+ Deal with any complaints made under the Act;
		+ Liaise with the Privacy Commissioner where appropriate;
		+ Work with the Privacy Commissioner during the investigation of complaints;
		+ The current Privacy Officer is the Chief Executive Officer

### Further Information

* 1. Further information can be found via the following links:

#### Privacy Act 2020

* + - <https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html>

#### Office of the Privacy Commissioner

* + - <https://www.privacy.org.nz/the-privacy-act-and-codes/the-privacy-act/>

### Privacy Breach

### A privacy breach occurs when ATNZ or an individual either intentionally or accidentally:

### Provides unauthorised or accidental access to someone's personal information.

### Discloses, alters, loses or destroys someone's personal information

### A privacy breach also occurs when someone is unable to access their personal information due to, for example, their account being hacked.

### Where ATNZ or an individual associated with ATNZ breaches privacy and this has or may lead to serios harm, ATNZ must advise the person(s) effected and the Privacy Commissioner within 72 hours of becoming aware of the breach. This notification will be made by the Chief Executive Officer.

###

### The unwanted sharing, exposure or loss of access to people’s personal information may cause individuals or groups serious harm. Some information is more sensitive than others and therefore more likely to cause people serious harm.

### Examples of serious harm include:

### Physical harm or intimidation

### Financial fraud including unauthorised credit card transactions or credit fraud

### Family violence

### Psychological, or emotional harm

### Policy Amendments

* 1. The Organisation is entitled to amend and vary its policies from time to time at the Organisation’s sole discretion and all employees are required to observe such policies.

### Appendix - Information Privacy Principles (IPP) Information Privacy Principle 1

#### Purpose of collection of personal information

1. Personal information must not be collected unless:
	1. the collection is for a lawful purpose connected with a function or activity of the agency; and
	2. the collection of the information is necessary for that purpose.
2. If the lawful purpose for which personal information about an individual is collected does not require the collection of an individual’s identifying information, the agency may not require the individual’s identifying information.

### Information Privacy Principle 2

#### Source of personal information

1. If an agency collects personal information, personal information must be collected from the individual concerned.
2. It is not necessary for an agency to comply with subclause (1) if the agency believes, on reasonable grounds:
	1. that non-compliance would not prejudice the interests of the individual concerned; or
	2. that compliance would prejudice the purposes of the collection; or
	3. that the individual concerned authorises collection of the information from someone else; or
	4. that the information is publicly available information; or
	5. that non-compliance is necessary:
		1. to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences; or
		2. for the enforcement of a law that imposes a pecuniary penalty; or
		3. for the protection of public revenue; or
		4. for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or
		5. to prevent or lessen a serious threat to the life or health of the individual concerned or any other individual;
	6. that compliance is not reasonably practicable in the circumstances of the particular case; or
	7. that the information:
		1. will not be used in a form in which the individual concerned is identified; or
		2. will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

### Information Privacy Principle 3

#### Collection of information from subject

1. If an agency collects personal information from the individual concerned, the agency must take any steps that are, in the circumstances, reasonable to ensure that the individual concerned is aware of:
	1. the fact that the information is being collected; and
	2. the purpose for which the information is being collected; and
	3. the intended recipients of the information; and
	4. the name and address of:
		1. the agency that is collecting the information; and
		2. the agency that will hold the information; and
	5. if the collection of the information is authorised or required by or under law:
		1. the particular law by or under which the collection of the information is authorised or required; and
		2. whether the supply of the information by that individual is voluntary or mandatory; and
	6. the consequences (if any) for that individual if all or any part of the requested information is not provided; and
	7. the rights of access to, and correction of, information provided by the IPPs (being the Information Privacy Principles).
2. The steps referred to in subclause (1) must be taken before the information is collected or, if that is not practicable, as soon as practicable after the information is collected.
3. An agency is not required to take the steps referred to in subclause (1) in relation to the collection of information from an individual if the agency has taken those steps on a recent previous occasion in relation to the collection, from that individual, of the same information or information of the same kind.
4. It is not necessary for an agency to comply with subclause (1) if the agency believes, on reasonable grounds:
	1. that non-compliance would not prejudice the interests of the individual concerned, or
	2. that non-compliance is necessary:
		1. to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences; or
		2. for the enforcement of a law that imposes a pecuniary penalty; or
		3. for the protection of public revenue; or
		4. for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or
	3. that compliance would prejudice the purposes of the collection; or
	4. that compliance is not reasonably practicable in the circumstances of the particular case; or
	5. that the information:
		1. will not be used in a form in which the individual concerned is identified; or
		2. will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

### Information Privacy Principle 4

#### Manner of collection of personal information

An agency may collect personal information only:

1. by a lawful means; and
2. by a means that, in the circumstances of the case (particularly in circumstances where personal information is being collected from children or young persons):
	1. is fair; and
	2. does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

### Information Privacy Principle 5

#### Storage and security of personal information

An agency that holds personal information must ensure:

1. that the information is protected, by such security safeguards as are reasonable in the circumstances to take, against:
	1. loss; and
	2. access, use, modification, or disclosure that is not authorised by the agency; and
	3. other misuse; and
2. that, if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

### Information Privacy Principle 6

#### Access to personal information

1. An individual is entitled to receive from an agency upon request:
	1. confirmation of whether the agency holds any personal information about them; and
	2. access to their personal information.
2. If an individual concerned is given access to personal information, the individual must be advised that, under IPP 7, the individual may request the correction of that information.
3. This IPP is subject to the provisions of Part 4 of the Act which sets out the manner in which requests can be made and the limited circumstances in which a request may be refused (refer Privacy Procedure).

### Information Privacy Principle 7

#### Correction of personal information

1. An individual whose personal information is held by an agency is entitled to request the agency to correct the information.
2. An agency that holds personal information must, on request or on its own initiative, take such steps (if any) that are reasonable in the circumstances to ensure that, having regard to the purposes for which the information may lawfully be used, the information is accurate, up to date, complete, and not misleading.
3. When requesting the correction of personal information, or at any later time, an individual is entitled to:
	1. provide the agency with a statement of the correction sought to the information (a statement of correction); and
	2. request the agency to attach the statement of correction to the information if the agency does not make the correction sought.
4. If an agency that holds personal information is not willing to correct the information as requested and has been provided with a statement of correction, the agency must take such steps (if any) that are reasonable in the circumstances to ensure that the statement of correction is attached to the information in a manner that ensures that it will always be read with the information.
5. If an agency corrects personal information or attaches a statement of correction to personal information, that agency must, so far as is reasonably practicable, inform every other person to whom the agency has disclosed the information.
6. Subclauses (1) to (4) are subject to the provisions of Part 4 of the Act.

### Information Privacy Principle 8

#### Accuracy, etc, of personal information to be checked before use or disclosure

An agency that holds personal information must not use or disclose that information without taking any steps that are, in the circumstances, reasonable to ensure that the information is accurate, up to date, complete, relevant, and not misleading.

### Information Privacy Principle 9

#### Agency not to keep personal information for longer than necessary

An agency that holds personal information must not keep that information for longer than is required for the purposes for which the information may lawfully be used.

### Information Privacy Principle 10

#### Limits on use of personal information

1. An agency that holds personal information that was obtained in connection with one purpose may not use the information for any other purpose unless the agency believes, on reasonable grounds:
	1. that the purpose for which the information is to be used is directly related to the purpose in connection with which the information was obtained; or
	2. that the information:
		1. is to be used in a form in which the individual concerned is not identified; or
		2. is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
	3. that the use of the information for that other purpose is authorised by the individual concerned; or
	4. that the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to use the information; or
	5. that the use of the information for that other purpose is necessary:
		1. to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences; or
		2. for the enforcement of a law that imposes a pecuniary penalty; or
		3. for the protection of public revenue; or
		4. for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or
	6. that the use of the information for that other purpose is necessary to prevent or lessen a serious threat to:
		1. public health or public safety; or
		2. the life or health of the individual concerned or another individual.
2. In addition to the uses authorised by subclause (1), an intelligence and security agency that holds personal information that was obtained in connection with one purpose may use the information for any other purpose (a secondary purpose) if the agency believes on reasonable grounds that the use of the information for the secondary purpose is necessary to enable the agency to perform any of its functions.

### Information Privacy Principle 11

#### Limits on disclosure of personal information

1. An agency that holds personal information must not disclose the information to any other agency or to any person unless the agency believes, on reasonable grounds:
	1. that the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained; or
	2. that the disclosure is to the individual concerned; or
	3. that the disclosure is authorised by the individual concerned; or
	4. that the source of the information is a publicly available publication and that, in the circumstances of the case, it would not be unfair or unreasonable to disclose the information; or
	5. that the disclosure of the information is necessary:
		1. to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences; or
		2. for the enforcement of a law that imposes a pecuniary penalty; or
		3. for the protection of public revenue; or iv. for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or
	6. that the disclosure of the information is necessary to prevent or lessen a serious threat to:
		1. public health or public safety; or
		2. the life or health of the individual concerned or another individual; or
	7. that the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions; or
	8. that the information:
	9. is to be used in a form in which the individual concerned is not identified; or
		* 1. is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
			2. that the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern.
2. This IPP is subject to IPP 12.

### Information Privacy Principle 12

#### Disclosure of personal information outside New Zealand

1. An agency (**A**) may disclose personal information to a foreign person or entity (**B**) in reliance on IPP 11(1)(a), (c), (e), (f), (h), or (i) only if:
	1. the individual concerned authorises the disclosure to B after being expressly informed by A that B may not be required to protect the information in a way that, overall, provides comparable safeguards to those in this Act; or
	2. B is carrying on business in New Zealand and, in relation to the information, A believes on reasonable grounds that B is subject to this Act; or
	3. A believes on reasonable grounds that B is subject to privacy laws that, overall, provide comparable safeguards to those in this Act; or
	4. A believes on reasonable grounds that B is a participant in a prescribed binding scheme; or
	5. A believes on reasonable grounds that B is subject to privacy laws of a prescribed country; or
	6. A otherwise believes on reasonable grounds that B is required to protect the information in a way that, overall, provides comparable safeguards to those in this Act (for example, pursuant to an agreement entered into between A and B).
2. However, subclause (1) does not apply if the personal information is to be disclosed to B in reliance on IPP 11(1)(e) or (f) and it is not reasonably practicable in the circumstances for A to comply with the requirements of subclause (1).
3. In this IPP:

**prescribed binding scheme** means a binding scheme specified in regulations made under section 213 of the Act,

**prescribed country** means a country specified in regulations made under section 214 of the Act.

### Information Privacy Principle 13

#### Unique identifiers

1. An agency (**A**) may assign a unique identifier to an individual for use in its operations only if that identifier is necessary to enable A to carry out 1 or more of its functions efficiently.

## A may not assign to an individual a unique identifier that, to A’s knowledge, is the same unique identifier as has been assigned to that individual by another agency (B), unless:

* 1. A and B are associated persons within the meaning of subpart YB of the Income Tax Act 2007; or
	2. the unique identifier is to be used by A for statistical or research purposes and no other purpose.
1. To avoid doubt, A does not assign a unique identifier to an individual under subclause (1) by simply recording a unique identifier assigned to the individual by B for the sole purpose of communicating with B about the individual.
2. A must take any steps that are, in the circumstances, reasonable to ensure that:
	1. a unique identifier is assigned only to an individual whose identity is clearly established; and
	2. the risk of misuse of a unique identifier by any person is minimised (for example, by showing truncated account numbers on receipts or in correspondence).
3. An agency may not require an individual to disclose any unique identifier assigned to that individual unless the disclosure is for one of the purposes in connection with which that unique identifier was assigned or is for a purpose that is directly related to one of those purposes.