PRIVACY & CONFIDENTIALITY POLICY

Sticky Business – privacy@sticky.co.nz

RESPONSIBILITY FOR POLICY: Jonelle Douglas

APPROVING AUTHORITY: Jonelle Douglas

LAST REVIEWED: 03/02/2021

NEXT REVIEW DATE:

OVERVIEW

The Privacy Act 2020 is the law governing the collection, storage, use and disclosure of personal information by both the private and public sectors in New Zealand. It has implications for the type of information kept by the Company and the intended use of that information for both internal and external clients.

The Company also collects, stores, and uses confidential information conducting its business which it must protect.

PURPOSE

This policy ensures the Company complies with the requirements of the Privacy Act 2020 and how its provisions affect the work of the Company. It also covers how employees must behave to protect the privacy of individuals and the information it collects on them, and how employees must behave to protect the confidential information available to them during the course of their employment.

DEFINITIONS

Confidential Information means any information which is not public and which the Company deems to be commercially sensitive as directly or indirectly affecting the Company's business. It includes information about or comprising the Company's Intellectual Property. It includes information about other employees, trainees, assessors, providers, Board members and knowledge obtained through discussion and/or electronic and/or other documented means. It includes personal information which is not otherwise in the public domain.

Personal information means information about an identifiable individual (natural person).

Document and *documented* means a document in any form, including:

- Any writing on any material; and
- Any book, map, graph, plan, or drawing; and
- Any photograph, negative, film, tape, or other device in/on which visual images are stored or embodied so as to be capable of being reproduced; and
- Any label, logo, or marking or other writing that identifies anything of which it forms part of to which it is attached; and

- Any digitally or electronically stored information capable of being retrieved and any material subsequently derived from that information

PRIVACY

This Policy should be read in conjunction with the 13 Privacy Principles which are appended to this policy and summarised as follows:

- An individual must know the purpose of collection of the personal information and the source of that information,
- Only the minimum of personal information should be collected as is necessary for the purpose for which the information is required,
- The individual concerned must know how and consent to the collection of his/her personal information,
- All personal information must be stored securely,
- The individual concerned should have access to the information which is held by the Company about him/her, and be able to request a correction to that information.
- Personal information should only be used for the purpose for which it is collected, and
- There are limits on the disclosure of personal information.

Employees of the Company will abide by all the Information Privacy Principles when undertaking their responsibilities as follows:

- That personal information collected by the Company is collected for a lawful purpose connected with the functions of the Company, and that the collection of that information is necessary for that purpose.
- Where the Company collects personal information, the Company shall collect the information directly from the individual concerned.
- The Company shall take all steps as are, in the circumstances, reasonable to ensure the individual concerned is aware of each of the following:
  - i that information is being collected,
  - ii the purpose for which the information is being collected,
  - iii the intended recipient of that information,
  - iii how long that information will be kept,
  - iv the name and address of the Company collecting the information and the Company that will hold the information, and
  - v the rights of access to and correction of that personal information.
- The Company cannot collect information by unlawful means or in a way that is unfair or intrusive.
- The Company has a responsibility as the holder of personal information to ensure that all information is held securely, in order to prevent loss, unauthorised access, modification, disclosure or any other misuse.
- An individual shall be entitled to obtain from the Company confirmation as to whether or not it holds personal information about the individual, where the information is held and to have access to the information about him/her.

- Where the Company holds personal information, the individual concerned shall be entitled to request correction of the information. Where the correction is not made, the individual shall be entitled to request that a statement that a correction was sought but not made be attached to the record.
- Where corrections have been made, the Company must inform all the relevant parties of the correction that has been added to the information concerned.
- The Company must ensure that personal information is accurate, relevant and not misleading before using that information.
- The Company shall not keep held personal information for longer than is necessary.
- The Company can only use personal information for the purpose for which it was collected.
- The Company must not disclose that personal information to a person or another Organisation unless the Company believes:
    - disclosure of the information is one of the purposes for which the information was collected,
    - the source of the information is publicly available,
    - the disclosure is to the individual concerned, or
    - the disclosure is authorised by the individual concerned.
- The Company must not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable The Company to carry out one or more of its functions.

All employees must adhere to the Information Privacy Principles in all their dealings with their colleagues and clients and ensure they always act in accordance with the Principles when collecting, storing and disclosing personal information.

Any serious breaches of privacy that could cause potential harm to the individuals identified will be notified to the Privacy Commissioner in accordance with the Privacy Act 2020.

PRIVACY OFFICER

The Privacy Officer for the Company is Jonelle Douglas. Any requests for personal information should be directed to the Privacy Officer in the first instance.

The Privacy Officer will ensure that the Company complies with the Privacy Act.

In the event that a complaint is received either by the Privacy Officer or the Privacy Commissioner alleging a breach of privacy, the Privacy Officer will:

1. Take ownership of the complaint and ensure that it is dealt with in a timely manner.
2. Acknowledge receipt of the complaint within 24 hours and advise the complainant of their rights
3. Fully investigate the complaint.
4. Fully co-operate with the Privacy Commissioner where appropriate and within the timeframe stipulated by the Privacy Commissioner.
5. Respond, with findings, to the complainant within 14 days of receipt.
6. Keep a record of all complaints received for ongoing review of policies and procedures.

CONFIDENTIALITY POLICY

- Employees must maintain the confidentiality of confidential information they come across in the course of their employment.
- Confidential information is not to be used for any purpose other than that which is directly related to the Company work.
- It is prohibited to use confidential information for personal gain.
- A confidentiality clause is included in employment agreements.
- At all times employees must maintain confidentiality by:
    - Not disclosing any confidential information to a third party without specific authority or unless there is a legal or professional duty to disclose
    - Restricting their discussion of confidential matters and the disclosure of confidential documents to other persons who are directly concerned and have the appropriate security clearance
    - Not using confidential information for any other purpose than for the business purposes of the company
    - Taking special care to ensure the confidentiality of information relating to another individual
    - Ensuring the security of confidential information which they have in their possession, particularly personal information
- Employees are not to, at any time during or after their employment with the Company, use or disclose to any person any confidential information relating to the Company.
- All Company policies, procedures and confidential information which employees may come into contact with during their employment is to remain the intellectual property of the Company.

Principle 1 – Purpose of Collection of Personal Information

Organisations must only collect personal information if it is for a lawful purpose connected with their functions or activities, and the information is necessary for that purpose.

Principle 2 – Source of Personal Information -

Personal information should be collected directly from the person it is about. The best source of information about a person is usually the person themselves. Collecting information from the person concerned means they know what is going on and have some control over their information.

It won't always be possible to collect information directly from the person concerned, so organisations can collect it from other people in certain situations. For instance:

- if the person concerned authorises collection from someone else
- if it's necessary to uphold or enforce the law
- if the information is collected from a publicly available source
- if collecting information from the person directly would undermine the purpose of collection.

Principle 3 – Collection of information from subject

Organisations should be open about why they are collecting personal information and what they will do with it.

When an organisation collects personal information, it must take reasonable steps to make sure that the person knows:

- why it's being collected
- who will receive it
- whether giving it is compulsory or voluntary
- what will happen if the information isn't provided.

Sometimes there may be good reasons for not letting a person know about the collection – for example, if it would undermine the purpose of the collection, or it's just not possible to tell the person.

Principle 4 – Manner of collection of personal information

Personal information must not be collected by unlawful, unfair or unreasonably intrusive means. When an organisation collects information about a person, it has to do so in a way that is fair and legal.

What is fair depends a lot on the circumstances. Threatening, coercive, or misleading behaviour is likely to be considered unfair.

If you break a law when collecting information, then you have collected information unlawfully.

What is reasonable also depends on the circumstances, such as the purpose for collection, the degree to which the collection intrudes on privacy, and the time and place it was collected.

Principle 5 - Storage and security of personal information

Organisations must ensure there are safeguards in place that are reasonable in the circumstances to prevent loss, misuse or disclosure of personal information.

Principle 6 – Access to personal information

Individuals have a right to ask for access to their own personal information. Generally, an organisation must provide access to the personal information it holds about someone if the person in question asks to see it.

People can only ask for information about themselves. The Privacy Act does not allow you to request information about another person, unless you are acting on that person's behalf and have written permission.

Refusing access

In some situations, an organisation may have good reasons to refuse a request for access to personal information. For example, the information may involve an unwarranted breach of someone else's privacy, or releasing it may pose a serious threat to someone's safety.

Principle 7 – Correction of personal information

A person has a right to ask an organisation or business to correct information about them if they think it is wrong.

If an organisation does not agree that the information needs correcting, an individual can ask that an agency attach a statement of correction to its records, and, if reasonable, the company should do so.

Principle 8 – Accuracy of personal information

An organisation must check before using or disclosing personal information that it is accurate, up to date, complete, relevant and not misleading.

Principle 9 - Retention of personal information

An organisation should not keep personal information for longer than it is required for the purpose it may lawfully be used.

Principle 10 – Use of personal information

Organisations can generally only use personal information for the purpose it was collected.

Sometimes other uses will be allowed, such as if the new use is directly related to the original purpose, or if the person in question gives their permission for their information to be used in a different way.

Principle 11 – Disclosure of personal information

An organisation may only disclose personal information in limited circumstances.

For instance, an organisation may disclose personal information when:

- disclosure is one of the purposes for which the organisation got the information
- the person concerned authorises the disclosure
- the information is to be used in a way that does not identify the person concerned
- disclosure is necessary to avoid endangering someone's health or safety
- disclosure is necessary to uphold or enforce the law.

Principle 12 - Cross-border disclosure

There are rules around sending personal information to organisations or people outside New Zealand (cross-border disclosure).

A business or organisation may only disclose personal information to another organisation outside New Zealand if the receiving organistion:

- is subject to the Privacy Act because they do business in New Zealand
- is subject to privacy laws that provide comparable safeguards to the Privacy Act
- agrees to adequately protect the information, e.g. by using model contract clauses
- is covered by a binding scheme or is subject to the privacy laws of a country prescribed by the New Zealand Government.

If none of the above criteria apply, a business or organisation may only make a cross-border disclosure with the permission of the person concerned. The person must be expressly informed that their information may not be given the same protection as provided by the New Zealand Privacy Act.

Principle 13 - Unique identifiers

An organisation can only use unique identifiers when it is necessary.

An organisation cannot assign a unique identifier to a person if that unique identifier has already been given to that person by another organisation.

Organisations must take reasonable steps to protect unique identifiers from misuse.

Unique identifiers are individual numbers, references, or other forms of identification allocated to people by organisations, such as driver's licence numbers, passport numbers, or IRD numbers.