PRIVACY AND DATA MANAGEMENT POLICY

1. Purpose

1.1. Being a health service provider, Just Skin Treatment Clinic ("the Company") routinely handles personal and sensitive health information. The Company understands that your privacy is important and therefore is committed to and adopts the Australian Privacy Principles set out in the *Privacy Act 1988 (Cth)* to protect and uphold the right to privacy and confidentiality of clients. The Company has ensured that this responsibility is incorporated as part of the Company's normal operational practice, and that the Company ensures that it comply with legislation, acts and guidelines related to its services.

1.2. This policy sets out how the Company handle your Health Information including how it collect, use, hold and disclose this information. It also contains information about how you can access the information the Company holds about you, how you can ask the Company to correct your information or make a complaint about how the Company has managed your information.

2. Definitions

2.1. **Personal Information**: Information or an opinion about employees which an employee's identity can reasonably be ascertained. This includes any Personal Information or opinions about the person, whether true or not, no matter how the information or opinions are recorded. The Company only collects Personal Information that it needs for a Relevant Purpose.

2.2. **Health Information**: Information or opinions about health of an individual, an individuals expressed wishes about the future provisions of health services to them, a health service provided or to be provided to an individual.

2.3. **Sensitive Information**: Special category of Personal Information which under the Privacy Act is categories as Health Information. Sensitive Information may have stricter requirements applied when handling such information.

2.4. **Relevant Purpose**: A purpose related to the person's employment, interaction or engagement with the Company whether it be prospective, current or retrospective. E.g., Relevant Purpose may include (but are not limited to) recruitment, selection, training, development, consulting, counselling, or engagement of services

2.5. Lawful: Collection that does not breach any State, Territory or Commonwealth law.

2.6. Fair Means: Collecting without intimidation or deception, and in a way that is not unreasonably intrusive.

3. Notice and Consent

3.1. Clients will be provided with notice that Health Information will be collected when using the service provided by the Company. This notice will be provided before or at the time of collection.

3.2. When a client uses our services, they will be required to complete a consent form, consenting to the Company collecting personal and sensitive information, and using this information in line with this policy. This consent form will include a Privacy Notice outlining what information is needed and why.

3.3. Without this consent, the Company may not be able to provide services to the individual.

4. Collected Health Information

4.1. As Personal Information is collected in the course or providing a health service, it is considered Health Information under the Privacy Act, which means this information is Sensitive Information.

4.2. Information collected about you will depend on the type of service you request or receive from us. Some of this information may include the below:

- Identifying and contact information, such as name, date of birth, address, telephone number and email address
- Demographic information, such as age and gender
- Financial information, such as banking, payment and contribution details
- Government issued identifiers, such as Medicare number
- Health and clinical information, such as your medical history, medical diagnosis, medication, specialist reports provided by the client for inclusion in the client's medical record, photographs that capture your image
- Other Health Information collected in connection with the donation, or intended documentation by an individual of his/her body parts or body substances

4.3. <u>Not Providing Personal/Sensitive Information</u>

4.3.1. You may choose not to disclose your Personal Information to the Company, but it may limit its ability to deal with you, manage emergencies effectively, provide you with services or let you know about other services that might better suit your needs.

5. How Is Health Information Collected?

5.1. Most information collected will be collected directly from you when you use our services, use our website, talk to us, provide us with feedback or make a complaint.

5.2. Information may also be collected from other sources, such as:

- Someone you have authorised to act on your behalf, like your partner, a family member or agent, power of attorney or guardian
- A third party, such as your treating hospital or other health service provider, or private health insurance fund

5.3. All Health Information will be collected by lawful and fair means.

6. How is Health Information Used?

6.1. The Company uses your Health Information for the primary purpose for which it was collected, or for secondary purposes in certain circumstances. The Company also use this information to comply with its legal obligations.

6.2. The Company may use your Health Information to contact you in relation to its services, or other requested information. This may be via email, SMS, mail or telephone. The Company respects the rights of its customers to choose how such information is received, which is why this preference is collected when Health Information is provided to the Company.

6.3. Your information may be used as required for quality assurance, or for research purposes. In this instance, only de-identified information will be used

7. Who We Disclose Information to and Why

7.1. Your personal and sensitive information may be disclosed to select third parties to assist the Company in providing you with services. Third parties may include:

- Your insurer or referring healthcare provider
- Your representatives (including a person to whom you have granted a delegated authority, or a guardian, attorney or family member)
- Hospitals and other health service providers (including your general practitioner and other allied health practitioners), including to provide you with clinical services for a specific condition, or when it is necessary to prevent or minimise harm or injury, or to allow for safe clinical handover and continuous medical management
- Payment systems operators (for example, merchants receiving cards payments)

- Other organisations the Company partners with to offer or provide services to you, or who provide analytical or marketing services to assist us to improve the delivery of products and services, and to enhance customer relationships

- The Company's professional advisers such as financial advisers, legal advisers and auditors

- Fraud bureaus or other organisations to identify, investigate or prevent fraud or other misconduct

- External dispute resolution bodies as necessary to resolve a matter you have raised

- For legal reasons, to law enforcement agencies, quality agencies, regulators, government agencies, courts or external advisors

7.2. The Company may also disclose your information to others where:

- It is required or authorised by law

- Accredited Data Recipients (ADR) where the Company has obtained clear and specific consent from you and the sharing is to be executed as agreed with you, or

- You have expressly consented to the disclosure, or the consent may be reasonably inferred from the circumstances.

8. How Information is Stored and Protected

8.1. The Company stores most of the information held about you electronically. Information is stored in secure data centres that are located in Australia and some with selected service providers (including cloud service providers) who may store your information outside Australia. Some information about you will also be stored in paper files.

8.2. The Company uses a range of physical, electronic and other security measures to protect the security, confidentiality and integrity of the Health Information we hold, including:

- Information security such as passwords to control access to computer systems

- Privacy training for the Company's employees so they know how to keep your information safe and secure

- Physical security, such as locks and security systems, over paper and electronic data stores and premises

- Access management controls, to prevent unauthorised people accessing the Company's systems

- Firewalls, and intrusion detection software security measures, for the Company's website and computer systems

- Processes designed to identify you when you deal with the Company by phone, online or face to face

8.2.1. These processes are designed to ensure we only disclose your information to you, or someone properly authorised by you.

8.2.2. Unfortunately, no data transmission over the internet or data storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with the Company is no longer secure, please contact the Company via phone, email or face to face immediately.

9. Retention of Data

9.1. The Company will keep information for a minimum of seven (7) years from the date of last entry. Once the minimum retention period has been met, records (including any personal information associated with the records) may be securely destroyed using disposal methods appropriate for the type of media and security classification of the records.

10. Research

10.1. Client Health Information may be used by the Company to conduct research and publish findings. All research will be in line with the broad principles and responsibilities outlined in the *Australian Code for the Responsible Conduct of Research*.

10.2. Please refer to the Company's *Management of Data and Information in Research Policy* for further information.

11. Handling a Data Breach

11.1. In the event of any loss, or unauthorised access or disclosure, of your Health Information that is likely to result in serious harm to you, the Company will investigate and notify the Office of the Australian Information Commissioner and other relevant regulatory bodies, and you, as required under Privacy Laws.

12. Accessing Your Health Information

12.1. You can request access to the Health Information the Company holds about you by contacting the Company via phone, email or face to face. Your request should include a detailed description of the information required. The Company will need to verify your identity before giving you access. The Company aims to provide you with requested information within 3 business days.

12.2. Information will only be provided to third parties on a client's behalf if a client's consent has been received, unless there are grounds on which to refuse such access.

12.3. If the Company is unable to provide you or a third party with access to your Health Information, it will inform you of the reasons why with a written notice.

13. Correcting Information

13.1. If you believe the information held about you is inaccurate, incomplete or out of date, please inform the Company of changes via phone, email or face to face. The Company will respond to a client's correction request within 30 days.

13.2. If the Company is unable to correct information, a notice will be provided to the individual.

14. Resolving a Privacy Concern

14.1. If you need to resolve an issue or make a complaint about how the Company manages your Health Information, you should first contact the Company to let it respond to your complaint. If you are not satisfied with the response, there are other steps you can take.

Contact the Company	Phone: 07 5348 9460 Email: admin@justskin.com.au Face to face: Maroochydore: Level 2, Tower 1, Kon-Tiki Building, 55 Plaza Parade, Maroochydore, QLD Noosa: Suite 110, 90 Goodchap St Noosaville, QLD Gympie: 6/84 Monkland St Gympie, QLD
Escalate complaint to your private health insurer	Details about your private health insurer's complaints process can be located on their website.
Contact an external body	If you have followed these steps and are not happy with the outcome you can contact the relevant external body: Office of the Australian Information Commissioner GPO Box 5218, Sydney, NSW, 2001 Phone: 1300 363 992 Fax: +61 2 9284 9666 Email: enquires@oaic.gov.au Website: www.oaic.gov.au

15. Variations

15.1. The Company reserve the right to vary, replace or terminate this policy from time to time.