JENNIFER BRUETON OCCUPATIONAL THERAPY

DATA PROTECTION POLICY

1. INTRODUCTION AND PURPOSE

The Organisation is committed to processing personal data in accordance with its responsibilities under the Protection of Personal Information Act (POPIA) and may be subject to similar information protection dispensations in other jurisdictions. These data protection laws impose strict guidelines to secure an employee's right to privacy with regard to their personal information.

Under these data protection principles, organisations are accountable for, and must be able to demonstrate that any personal data they handle is:

- Processed lawfully and transparently, and accessible to the data subject
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and kept up to date
- Kept for no longer than is necessary where data subjects are identifiable
- Processed securely and protected against unauthorised or accidental loss, destruction or damage

The Organisation, ***Jennifer Brueton Occupational Therapy***, lawfully requires certain personal information about its clients and employees and needs to process personal information relating to such individuals and legal entities.

The Organisation is committed to protecting and safeguarding all personal information in its possession or under its control and to take appropriate and reasonable measures (technological as well as organisational) to ensure the integrity and confidentiality thereof in respect of all its business activities in accordance with the law as well as ongoing risk assessments.

This Data Protection Policy is intended to:

- Ensure that the Organisation complies with legal standards for the receipt, processing and storing of personal data of individuals and legal entities and to explain how this should be achieved
- Ensure that the Organisation protects the rights of data subjects in respect of the privacy of personal information
- Ensure that the Organisation provides a transparent system of personal information protection
- Protect the Organisation against the risks and consequences of data breaches.

2. DEFINITIONS

Organisation	Means *Jennifer Brueton Occupational Therapy*, a sole proprietor, registered under Practice Number *0434167*.
Information Officer	Means Jennifer Brueton
Data Subject	means the person (individual or legal entity) to whom the data relates
Responsible party	Means the person/entity (either alone or jointly with others) who determines the purpose and manner in which personal information of a data subject is to be processed
Operator	Means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party
Personal information* *For the purpose of this policy, reference to 'personal information' shall include 'special personal information' as described hereunder	Means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to— (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; (b) information relating to the education or the medical, financial, criminal or employment history of the person; (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; (d) the biometric information of the person; (e) the personal opinions, views or preferences of the person; (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; (g) the views or opinions of another individual about the person; and (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person,
Special personal information	Means - (a) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or (b) the criminal behaviour of a data subject to the extent that such information relates to— (i) the alleged commission by a data subject of any offence; or (ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

Processing	Means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including— (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; (b) dissemination by means of transmission, distribution or making available in any other form; or (c) merging, linking, as well as restriction, degradation, erasure or destruction of information.
De-identify	Means to delete any information that: identifies, or can be used/manipulated to identify, the data subject; or that can be linked to other information that identifies the data subject by a reasonably foreseeable method.

3. SCOPE

3.1. This policy applies to all personal information processed by the Organisation – whether by employees or by third-party Operators on its behalf. It will also apply to ancillary workers such as contractors, consultants, locums, etc. who may from time to time provide services to the Organisation and be exposed to personal information in its possession or under its control.

3.2. The Information Officer will be registered with the office of the Information Regulator and shall take responsibility for the Organisation's ongoing compliance with this policy.

3.3. This policy shall be reviewed at least annually.

4. GENERAL DATA PROTECTION PRINCIPLES

4.1. All personal data relating to data subjects and/or to the Organisation, shall be deemed confidential information and be handled as such.

4.2. The processing conditions for lawful processing of personal information as required in terms of POPIA, will be complied with (see below par 6)

4.3. The only person/s entitled to access data covered by this policy, will be those who need to access it for the execution of their direct work services or required outputs.

4.4. Under no circumstances will personal information be shared outside the scope of required work outputs, or informally. In the event of any doubt, an employee or Operator must first obtain authorisation from the Information Officer before accessing confidential information where any work output requiring access is unusual or out of the ordinary.

4.5. Employees will receive induction and on-the-job training in relation to all security standards applicable to such employee's service delivery and work outputs involving personal information of data subjects.

4.6. Employees shall keep all personal data secure by taking sensible practical precautions and complying with all rules, practices and protocols. This pertains to both physical and digital security including the use of passwords, communications, device security, remote access, physical access control, authorisation protocols, etc.

4.7. The Organisation will develop and implement an Incident Response Plan in case of a data breach or a security compromise. This must be communicated to relevant employees and Operators and must be strictly complied with.

5. THE RIGHTS OF DATA SUBJECTS

5.1. Data subjects have the right to know what personal information is held by the Organisation and for what purpose(s) it is processed.

5.2. Data subjects may request access to their personal information. They may also request amendments to or deletion of the information if it is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, obtained unlawfully and/or no longer authorised to be kept.

5.3. Data subjects may further object in the prescribed manner to the processing of their personal information (except where processing is based on an obligation in terms of the law, or to perform in terms of a contract to which the data subject is a party), or may withdraw consent previously given to process the information.

5.4. Data Subject Access requests must be referred to the Information Officer via email, who will be responsible to attend to the request timeously and to communicate with the data subject in this regard. The identity of the data subject must always be verified before granting access to the information.

5.5. The Organisation may in certain circumstances be legally obliged to disclose personal information to law enforcement or similar institutions, without the consent of the data subject. This will however only be done after verifying that the request is lawful and legitimate. Only the Information Officer will be authorised to furnish such information.

5.6. Data subjects may lodge a complaint with the Information Regulator it they are concerned about the security of their personal information or its processing by the Organisation. Data subjects are however encouraged to first contact the Information Officer to report their concerns to the organisation directly, in terms of its relevant complaints procedure.

6. LAWFUL. JUSTIFIED AND TRANSPARENT DATA PROCESSING

6.1. All processing of personal information by the Organisation and/or its Operators, must be done in accordance with the processing principles and conditions as set out in the relevant privacy legislation, specifically POPIA in South Africa.

6.2. All personal information processed by the Organisation must be done on one of the following lawful bases: consent of the data subject, contractual obligation, legal obligation, performance of a public task or to protect the legitimate interests of the Organisation and/or the data subject. It must be clearly recorded on what basis any and all personal information is being processed and the Information Officer must implement and coordinate an appropriate system to facilitate this, and must ensure that it is regularly reviewed and updated.

The organisation's legitimate business interests must always be balanced against the data subject's privacy rights.

Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal information. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and such revocation must be clearly and accurately reflected in the Organisation's systems.

6.3. The lawful processing of personal information must also be done in accordance with eight specific processing conditions:

6.3.1. Accountability

The Organisation as the Responsible Party determines the purpose, means and processing of the personal information and must put measures are in place to ensure that all the processing conditions are complied with at the time of determining the purpose and means of processing and during the processing itself.

All employees (and Operators) shall continually be responsible for ensuring the safeguarding, protection and avoidance of any unauthorised disclosure or breach of personal information in the execution of employment duties and services to the Organisation, or otherwise in the course of rendering services or being associated with the Organisation. Instructions and guidance in this regard may include: this policy, departmental policies and procedures, instructions from management or from the Information Officer, training and general communications.

Persons with particular responsibilities connected to data protection in the Organisation, are: *(Optional, depending on organisational environment)*

- The Information Officer, who is responsible for assessing, overseeing, coordinating and ensuring data security and compliance with POPIA; for arranging data protection training for employees; for reviewing and approving agreements with third-party Operators; for reporting to executive management about compliance with all technological and operational data protection standards and protocols; to advise of any risk of breach at the earliest opportunity; and to put measures in place to respond to any data breach or security compromise. The Information Officer may also initiate disciplinary proceedings against employees for breaches or rules and standards in this regard and must attend to all request Internal or external) for access to personal information.

6.3.2. Minimality / Processing Limitation

Processing of personal information must be limited to lawful and justified processing (on one of the bases as set out above) in a reasonable manner, that does not unnecessarily infringe on the privacy of the data subject. Only the minimum amount of personal information that is necessary for the stated purpose, must be collected and processed.

There are also further specific limitations that apply to particular types of personal information / activities, such as cross-border transfer of information, direct marketing, automated decision making, directories, special personal information and information relating to children.

6.3.3. Purpose Specification

Personal information must be collected for a specific, explicitly defined and lawful purpose related to a legitimate function / activity of the Organisation and this purpose should generally be disclosed to the data subject.

Personal information should also not be retained for longer than is necessary for achieving the purpose for which the information was collected and processed, unless certain exceptions apply. A retention register / archiving policy / is kept by the Organisation to ensure that information is not kept longer than is necessary. This policy sets out what data must be retained, for how long and why.

All records containing personal information must be securely destroyed at the end of the retention period, or the information must be de-identified. The Organisation has implemented the following measures / protocols to comply with this condition:

- Treatment records will be kept for six years from the last treatment date.
- Treatment records of minors will be kept until their 21st birthday.
- Treatment records of clients who are mentally impaired should be kept until the client's death.

6.3.4. Further processing limitation

Personal information that has been collected for a specific purpose, may not be processed further unless it is for a reason compatible to the original purpose, or if the data subject consents, or if specific circumstances exist that permit such further processing in terms of the law.

6.3.5. Information quality

The Organisation must take reasonable steps to ensure that the personal information processed by it is complete, accurate, not misleading and updated where necessary.

Personal information should therefore as far as possible be collected directly from the data subject, unless certain exceptions apply for collecting it from a different source. Procedures to ensure that personal information is regularly reviewed and updated,

should also be put in place, communicated to the relevant employees and Operators and complied with.

Particular care should be taken that personal information is not unnecessarily duplicated and stored in different places, and that any updates are applied to all sets of the same information.

The measures implemented by the Organisation in respect of this condition include:

[Refer policies, protocols, procedures, SOP's, etc.] …….

6.3.6. Openness / Transparency

Whenever the Organisation collects personal information (except if one or more of the exclusions in s18 of POPIA apply), it must take reasonable steps to notify the data subject of certain details relating to the processing of this information:

- The information collected and the source of the information (if not from the data subject directly)
- The name and address of the Organisation
- The purpose for which it is collected,
- Whether the data subject is obliged to supply the information or if it is voluntary (e.g. what law if any prescribes, authorise or require the collection of the information)
- The consequences of failure to provide the information
- If applicable, that the responsible party intends to transfer the information trans-border and the level of protection afforded by the recipient
- Any further information, such as the recipients of the information, its nature and category, and the right of the data subject to access and rectify the information collected, to object to the processing of the information, or to complain to the Regulator.

The Organisation complies with this condition by issuing specific and relevant Privacy Notices to data subjects when personal information is collected.

Provision must also be made in respect of handling requests for access to information by data subjects and/or third parties – internally or externally. The Information Officer handles all such requests under POPIA as well as PAIA (the Promotion of Access to Information Act) and may implement procedures, policies and processes in this regard.

6.3.7. Security safeguards

The Organisation is legally obliged to secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent loss of or damage to or unauthorised destruction, unlawful access to or processing of such personal information.

In order to do this, the Organisation will regularly conduct risk assessments to identify foreseeable internal / external risks and vulnerabilities to such personal information, and will establish and maintain appropriate safeguards against these risks. Such safeguards include technological as well as organisational and physical measures, and must have due regard to international best practice, specific industry standards or applicable professional rules or regulations. These will be reviewed and updated on a regular basis and where applicable, communicated to relevant employees.

The Organisation will also ensure that any third-party Operators that process personal information on its behalf, subscribe to and comply with the same level of security and that these obligations are set out in a mandatory written agreement with each Operator.

Some of the pertinent security measures in the Organisation include:

- **Data classification, authorisation and access**
  The Organisation will design a data classification system to determine who may have access to various types of personal information and implement appropriate security measures to ensure that access to unauthorised persons is restricted and to avoid sharing of the information.
  Paper- or other physical records are kept in a secure place where only authorised persons can view or access it. Offices of personnel such as HR, finance, security and IT where sensitive personal information is usually kept, are particularly vulnerable.

- **Secure processing and storage**
  Security measures include using up to date software, secure (off-premises) storage and having appropriate back-up and recovery solutions in place for electronic data.
  Employees who work remotely must ensure that records are used and stored securely in a locked cabinet or drawer and that adequate password protection is used when accessing client's personal information on cloud-based software, such as email and EZMed.

- **Transferring personal information and communications**
  Personal information may not be transferred or sent to any person or entity not directly authorised to receive it. Employees must ensure that emails are not accidentally sent to non-authorised recipients, and that long email threads do not inadvertently disclose confidential or personal information.
  IT protocols will also be developed and implemented to ensure the proper encryption so that personal information is sent in protected form to authorised recipients.

- **Sharing personal information**
  The sharing of personal information with another employee or company representative will depend on whether that person has a job-related need to know the information, and provided that aspects such as cross-border restrictions (where applicable) are adhered to. It must also comply with the Privacy Notice

provided to the data subject and, if required, where the consent of the data subject has been obtained.

Personal information may generally only be shared with third parties when certain safeguards and/or contractual arrangements have been put in place, in particular also containing provisions relating to data protection, and subject to the same restrictions as set out above.

- **Device security and acceptable use of personal information**
  When working with personal information, employees make use of their own personal computers/devices with which they conduct aspects of their job, including but not limited to compiling reports, corresponding with clients, setting up appointments and billing. All reasonable precautions will be made to protect the personal information that employees of this practice have access to, which includes ensuring that their computer-/device screens are always locked when left unattended, individual password protection in place to access the practice management system and safe storage of paper records. Personal information may not be shared informally and paper records should not be left lying around on desks and printers.

- **Disposal of personal information**
  When personal information is deleted or de-identified, it must be done so that the data is not recoverable or re-identifiable. Office equipment must be professionally wiped when disposed of or no longer in use. Paper records must be shredded when no longer needed.

6.3.8. Data subject participation

Data subjects has the right to be involved in the processing of their personal information and have certain rights in this regard, as outlined in par 5 above.

6.4. Account numbers

Failure by the organisation to appropriately protect account numbers of data subjects, could constitute a criminal offence if it ought to have known / foreseen risks in this regard, but failed to take reasonable steps to address those risks.

Someone who knowingly or recklessly obtains, discloses or procures the disclosure of an account number in an unauthorised manner, or who sells such a number, may also be guilty of a criminal offence.

6.5. Direct marketing

Marketing by electronic means to potential or existing customers is subject to strict privacy rules in terms of POPIA.

Prior consent from potential recipients must be explicitly obtained (in the prescribed manner) before marketing material (including emails, newsletters, texts) may be sent to them and they may only be approached once for such consent. The option to withdraw consent, opt-out or unsubscribe must also be very clearly indicated in each subsequent communication.

The limited exception for existing customers allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, if marketing similar products or services, and if giving the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

6.6. Automated decision making and profiling

Automated decision making relates to automated decisions being taken without human oversight or intervention, such as adverse credit decisions being taken automatically, or other adverse decisions and activities such as algorithmic processing and information and result outputs.

This type of processing is prohibited under POPIA, but with some exceptions – such as when automated decision-making is governed by law or a code of conduct with suitable protections; or has been done in in connection with a contract according to the data subject's request and appropriate protective measures have been taken.

These protective measures include an opportunity for the data subject to make representations; after the organisation has provided him/her/it with sufficient information about the underlying logic of the automated processing.

7. TRANSFERRING PERSONAL INFORMATION TO A COUNTRY OUTSIDE OF SOUTH AFRICA

The organisation will as far as possible ensure that the transfer of personal information to a recipient in a foreign country only takes place if there are adequate / similar levels of data protection in place – either by way of laws applicable to that country, or in terms of Binding Corporate Rules or a binding Transborder data processing agreement.

The data subject may however nevertheless consent to the cross-border transfer of their personal information; or such a transfer may take place if it is necessary in connection with a contract between the organisation and the data subject, or a contract concluded in the data subject's interest or to their benefit.

The cross-border transfer of special personal information or personal information relating to children, may however be subject to prior authorisation from the Information Regulator if the foreign country does not provide an adequate level of protection as required in terms of POPIA.

8. DATA BREACHES / SECURITY COMPROMISES

Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the Organisation must notify the Regulator; and the affected data subject(s) (unless the identity of such data subject cannot be established or it will impede a criminal investigation).

This notification and the Organisation's response to a data breach, will be dealt with in terms of the Incident Response Plan developed by the Information Officer.

The Incident Response Plan includes a form that an employee or an Operator must complete whenever a security compromise is found or suspected, as well as specific reporting protocols. Operators may not make reports to data subjects or the Regulator directly, but must report to the Organisation as the responsible party. Employees, Operators and the like should not attempt to investigate such matters themselves, but should immediately contact the Information Officer or delegated person and preserve all evidence relating to the potential security compromise or data breach.

The Information Officer is responsible to ensure that all relevant employees and Operators are made aware of the contents of the Incident Response Plan.

9. DATA PROTECTION IMPACT ASSESSMENTS AND PRIVACY BY DESIGN

The organisation is committed to making data protection and privacy of data subjects a priority in all aspects of its business activities. To this end, the organisation's privacy strategy provides for continuous privacy- and data protection impact assessments as may be appropriate and for privacy considerations to form part of the development and implementation of all new projects, tools, programmes, equipment, etc.

10. IMPLEMENTATION OF POLICY IN REPSECT OF EMPLOYEES

This data protection policy governs every employee of the Organisation during the course of his/her services to it, and to the extent applicable, after termination of employment. It is the responsibility of every employee to familiarise him/herself with the content of this policy, and to remain up to date as to any changes to it issued by the Organisation.

To the extent that this policy sets out workplace rules and standards governing the employee in the course of his/her work and services to the company, these shall form part of the company's Disciplinary Code and Procedure and is hereby also incorporated into it.

A breach of any rule in relation to the protection of personal data set out in this policy that constitutes misconduct, shall be subject to disciplinary action and may lead to dismissal in appropriate circumstances.

The imposition of any disciplinary sanction or dismissal shall not preclude the Organisation from instituting civil proceedings against an employee who acted in breach of this policy where such breach has resulted in liability, loss, reputational damage and/or other damages to the Organisation in the course of pursuing its commercial operations.

11. RELATED DOCUMENTS

This policy must be read together with other organisational policies and standards that deals with specific areas of the business, including:

<u>Internal</u>

- Confidentiality and non-disclosure agreements

- Internal Employee Privacy Policy (dealing with how the company processes the personal information of employees)
- Privacy Notices to employees, job applicants, ……. (S18 of POPIA)
- IT and Cyber Security policies, password policy, 'Bring-your-own-device' policy,
- Incident Response Plan

External *[Examples / optional]*

- Customer Privacy Policy
- Website Privacy Policy, Cookie policy
- Privacy Notices to customers, clients, vendors, suppliers, applicants, members,

[Regulations and forms under POPIA - https://www.justice.gov.za/inforeg/docs/20181214-gg42110-rg10897-gon1383-POPIregister.pdf]