

**Lara Hirschmann's Shining Stars OT Practice
(the "Practice")**

Protection of Personal Information Policy (the "Policy")

1. Protection of personal information

1.1. Purpose and scope

This Policy is prescribed in terms of the Protection of Personal Information Act 4 of 2014 (the "POPI Act"), as amended or substituted from time to time.

The Practice is a registered occupational therapy practice with the Board of Healthcare Funders (BHF) and with the Health Professions Council of South Africa (HPCSA). Through the provision of these services, the Practice is necessarily involved in collecting, using and disclosing certain aspects of the personal information of its clients, employees, and other stakeholders. As a responsible party, the Practice must comply with the POPI Act. The POPI Act requires the Practice to inform its clients and employees about the way their personal information is used, disclosed and destroyed.

The Practice is committed to effectively managing personal information in accordance with the POPI Act. The Practice is committed to protecting the privacy of its clients and employees and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.

This Policy sets out the way the Practice deals with its clients' and employees' personal information and stipulates the purpose for which the information is used and how it is used. The Policy is referenced in the legal contracts via the Privacy Notice (or otherwise) of the Practice and is made available on request.

The purpose of this Policy is to:

1.1.1. protect the Practice from the compliance risks associated with the protection of personal information, which includes:

- breaches of confidentiality
- reputational damage

1.1.2. demonstrate the Practice's commitment to protecting the privacy rights of data subjects:

- through stating desired behaviour and directing compliance with the provisions of the POPI Act
- by cultivating a culture that recognises privacy as invaluable
- by developing and implementing internal controls for the purpose of managing the compliance risks associated with the protection of personal information
- by creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of the Practice
- by assigning specific duties and responsibilities to control owners, including the appointment of an information officer and, where necessary, deputy information officers, in order to protect the interests of the Practice and data subjects
- by raising awareness through training and providing guidance to individuals who process personal information for the Practice so that they can act confidently and consistently.

1.2. Legislative framework

The reference to legislation, subordinate legislation and supervision documents includes, amendments made from time to time (included but not limited to).

- Protection of Personal Information Act 4 of 2014 (the "POPI Act")
- Promotion of Access to Information Act 2 of 2000 (the "PAIA")
- Health Professions Act 56 of 1974
- National Health Act 61 of 2003
- Medical Schemes Act 121 of 1998
- Children's Act 38 of 2005
- Mental Healthcare Act 17 of 2002
- Basic Conditions of Employment Act 75 of 1997
- Constitution of the Republic of South Africa, 1996 (the "Constitution").

1.3. Definitions

- 1.3.1. **Biometrics** means a technique of personal identification that is based on physical, physiological or behavioural characterisation, including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition
- 1.3.2. **Child** means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning himself or herself
- 1.3.3. **Competent person** means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child (i.e. the child's legal guardian)
- 1.3.4. **Consent** means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information
- 1.3.5. **Data subject** means the person to whom **personal information** relates
- 1.3.6. **De-identify** and **de-identified**, in relation to personal information of a **data subject**, means to delete any information that:
- identifies the data subject
 - can be used or manipulated by a reasonably foreseeable method to identify the data subject
 - can be linked by a reasonably foreseeable method to other information that identifies the data subject
- 1.3.7. **Direct marketing** means to approach a data subject, either in person, by mail or electronic communication, for the direct or indirect purpose of:
- promoting, or offering to supply, in the ordinary course of business, any goods or services to the data subject
 - requesting the data subject to make a donation of any kind and for any reason
- 1.3.8. **Electronic communication** means any text, voice, sound, image or message, sent over an electronic communications network, which is stored in the network or in the recipient's terminal equipment, until it is collected by the recipient
- 1.3.9. **Filing system** means any structured set of personal information, whether centralised, decentralised, or dispersed, on a functional or geographical, basis, which is accessible according to specific criteria
- 1.3.10. **Head of a private body** means:
- in the case of a natural person, that natural person or any person duly authorised by that natural person
 - in the case of a partnership, any partner of the partnership or any person duly authorised by the partnership
 - in the case of a **juristic person**:
 - the **chief executive officer** or equivalent officer of the juristic person, **or any person duly authorised by that officer**
 - the person who is acting as such or any person duly authorised by such acting person
- 1.3.11. **Information matching programme** means the comparison, whether manually or by means of any electronic or other device, of any document that contains personal information about ten (10) or more data subjects, with one (1) or more documents that contain personal information of ten (10) or more data subjects, for the purpose of producing or verifying information that may be used for the purpose of taking any action in regard to an identifiable data subject

- 1.3.12. **Information officer** of, or in relation to, a:
- **public body** means an information officer or deputy information officer, as contemplated in terms of section 1 or 17 of the **PAIA**
 - **private body** means the **head of a private body**, as contemplated in section 1 of the PAIA
- 1.3.13. **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
- 1.3.14. **Person** means a natural person or a juristic person
- 1.3.15. **Personal information** means information about an identifiable, living, natural person, and, where it is applicable, an identifiable, existing juristic person, including, but not limited to:
- information about 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
 - information relating to the educational, medical, financial, criminal or employment history of the person
 - any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier, or other particular assignment to the person
 - the biometric information of the person
 - the personal opinions, views or preferences of the person
 - 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
 - the views or opinions of another individual about the person
 - the name of the person if it appears with other personal information about the person or if the disclosure of the name itself would reveal information about the person
- 1.3.16. **Private body** means:
- a natural person who carries or has carried on any trade, business or profession but only in the capacity as a natural person
 - a partnership which carries or has carried on any trade, business or profession
 - any former or existing **juristic person but excludes a public body**
- 1.3.17. **Processing** means any operation or activity or any set of operations, whether or not by automatic means, pertaining to personal information, including:
- the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use
 - dissemination by means of transmission, distribution, or making available in any other form
 - merging, linking, restriction, degradation, erasure, or destruction of information
- 1.3.18. **Public body** means:
- any department of state or administration in the national or provincial sphere of government, or any municipality in the local sphere of government
 - any other functionary or institution when:
 - exercising a power or performing a duty in terms of the Constitution or a provincial constitution
 - exercising a public power or performing a public function in terms of any legislation
- 1.3.19. **Public record** means a record that is accessible in the public domain and which is in the possession of, or under the control of, a public body, whether or not it was created by that public body

- 1.3.20. **Record** means any recorded information:
- regardless of form or medium, including:
 - writing on any material
 - information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware, or software or both, or other device, and any material subsequently derived from information produced, recorded or stored
 - label, marking or other writing that identifies or describes anything of which it forms part or to which it is attached, by any means
 - book, map, plan, graph or drawing
 - photograph, film, negative, tape or other device, in which one (1) or more visual images are embodied to be capable, with or without the aid of some other equipment, of being reproduced
 - in the possession or under the control of a responsible party
 - whether or not it was created by a responsible party
 - regardless of when it came into existence
- 1.3.21. **Regulator** means the Information Regulator, established in terms of section 39 of the POPI Act
- 1.3.22. **Re-identify** and **re-identified**, in relation to personal information of a data subject, means to resurrect any information that has been de-identified that:
- identifies the data subject
 - can be used or manipulated by a reasonably foreseeable method to identify the data subject
 - can be linked by a reasonably foreseeable method to other information that identifies the data subject
- 1.3.23. **Responsible party** means a public or private body, or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information
- 1.3.24. **Restriction** means to withhold or restrict from circulation, use or publication, any personal information that forms part of a filing system but not to delete or destroy the information
- 1.3.25. **Special personal information** means personal information, as referred to in section 26 of the POPI Act:
- religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health, sex life or biometric information of a data subject
 - criminal behaviour of a data subject, to the extent that the information relates to:
 - alleged commission by a data subject of any offence
 - proceedings about any offence allegedly committed by a data subject or the disposal of those proceedings
- 1.3.26. **Unique identifier** means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject for that responsible party.

1.4. Lawful processing of personal information

- 1.4.1. The Practice, as the responsible party or as the operator, **MUST** adhere to the 8 conditions for the lawful processing of personal information:
- Condition 1: Accountability
 - Condition 2: Processing limitation
 - Condition 3: Purpose specification
 - Condition 4: Further processing limitation
 - Condition 5: Information quality

- Condition 6: Openness
- Condition 7: Security safeguards
- Condition 8: Data subject participation

1.5. Condition 1: Accountability – responsible party to ensure conditions for lawful processing

- 1.5.1. The Practice, as the responsible party, must ensure that it complies with the conditions and the measures that give effect to the conditions when it determines the purpose of processing, how it processes, and during the processing.
- 1.5.2. Where the Practice is acting as the operator, the responsible party must ensure that the Practice complies with the relevant conditions and the measures that give effect to the conditions when it determines the purpose of processing, how it processes, and during the processing.

1.6. Condition 2: Processing limitation – lawfulness of processing

- 1.6.1. The Practice **MUST** only process personal information lawfully and reasonably, in a way that does not infringe the privacy of the data subject.

1.7. Condition 2: Processing limitation - minimality

- 1.7.1. The Practice may only process personal information that is adequate, relevant and not excessive, based on the purpose for processing that information.
- 1.7.2. The Practice collects and processes data subjects' personal information in terms of several other laws associated with the functions performed by the Practice (see 2.2: Legislative framework). As health practitioners providing **occupational therapy** services, the Practice may obtain personal information of potential and existing clients to determine the client's needs and objectives, among other regulatory and client personal requirements.
- 1.7.3. Employees of the Practice are also data subjects and the Practice collects personal information of potential and existing employees in terms of other laws, including employment laws.
- 1.7.4. Examples of personal information that the Practice collects from data subjects includes:
- Identity number, passport number, date of birth, nationality, full name, physical and postal addresses, marital status, income tax number, number of dependants, race, gender
 - Description of residence, business, assets, liabilities, financial information, banking details
 - Qualifications, education, employment history, criminal history
 - Any other information required by the Practice, its product suppliers and third-party service providers
- 1.7.5. The Practice also collects and processes clients' personal information for marketing purposes, to ensure that our products and services remain relevant to its clients and potential clients.
- 1.7.6. From the effective date of the regulations to the POPI Act, if the Practice wants to engage in direct marketing, it must use the prescribed Form 4 as contained in the regulations, to apply for the consent of a data subject.
- 1.7.7. The Practice aims to have agreements in place with all product suppliers, and third-party service providers to ensure a mutual understanding regarding the protection of clients' personal information. The Practice's product suppliers will be subject to the same regulations, as applicable to the Practice, in terms of the protection of clients' personal information.

1.8. Condition 2: Processing limitation – consent, justification, and objection

- 1.8.1. The Practice **MAY ONLY** process personal information IF the:

- **data subject**, or a competent person (only where the data subject is a child), **consents to the processing**. For example, consent is obtained from clients before and/or during the assessment stage of the client relationship
 - processing is necessary to carry out actions for the conclusion, or performance, of a **contract to which the data subject is party**. For example, to conduct an accurate assessment of the client's needs and objectives
 - processing **complies with an obligation imposed by law on the responsible party**. For example, as required by employment related legislation, tax related legislation etc.
 - processing **protects a legitimate interest of the data subject**. For example, it is in the client's best interest to have a full and proper needs assessment performed to provide them with an applicable and beneficial service
 - processing is necessary for **pursuing the legitimate interests of the Practice, or third-parties, to whom the information is supplied**. For example, to provide the Practice's clients with products or services, the Practice, its product suppliers, its service providers and other relevant third parties require certain personal information from the clients to make an expert decision about the unique and specific product or service required.
- 1.8.2. The Practice must classify all the personal information processed according to the reasons for which personal information is processed to ensure that it only processes personal information for permitted reasons and to identify the instances where the data subject may object to the processing of their personal information.
- 1.8.3. If the Practice identifies that it is processing personal information for a reason that is not a permitted reason, it must take corrective action.
- 1.8.4. The Practice, as the responsible party, **MUST** have proof of the data subject's consent where consent is required.
- 1.8.5. Where the Practice is acting as the operator, the responsible party **MUST** ensure that it provides the Practice with the proof of the data subject's consent, where consent is required.
- 1.8.6. Where the data subject's consent for processing their personal information is required, the Practice **MUST** allow the data subject to withdraw their consent at any time as long as the lawfulness of the processing before the withdrawal of consent, or the processing where consent is not required, will not be affected by the withdrawal of consent.
- 1.8.7. If a data subject objects to the processing of their personal information (using the prescribed Form 1, and on reasonable grounds relating to their situation), where the reason for the processing:
- protects a legitimate interest of the data subject
 - processing is necessary for the proper performance of a public law duty by a public body
 - processing is necessary for pursuing the legitimate interests of the responsible party
 - processing is necessary for pursuing the legitimate interests of a third party to whom the information is supplied,
- the Practice **MUST STOP** processing the data subject's related personal information, **UNLESS**:
- legislation provides for the processing
 - processing is for purposes of direct marketing that is not by means of unsolicited electronic communications.

1.9. Condition 2: Processing limitation – collection directly from data subject

- 1.9.1. The Practice **MUST** collect personal information directly from the data subject, except if:
- information is contained in or derived from a public record or has deliberately been made public by the data subject

- **data subject, or a competent person (only where the data subject is a child), consents to the collection of the information from another source**
- **collection of the information from another source would not prejudice a legitimate interest of the data subject**
- collection of the information from another source is necessary:
 - to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences
 - **to comply with an obligation imposed by law** or to enforce legislation about the collection of revenue (in terms of the South African Revenue Service Act)
 - for the conduct of proceedings in any court or tribunal, which have commenced or are reasonably contemplated
 - in the interests of national security
 - to maintain the legitimate interests of the responsible party
 - to maintain the legitimate interests of a third party to whom the information is supplied
- **compliance would prejudice a lawful purpose of the collection**
- **compliance is not reasonably practicable in the circumstances of the case.**

1.10. **Condition 3: Purpose specification - collection for specific purpose**

- 1.10.1. The Practice **MUST** only collect personal information of data subjects for the specific, explicitly defined and lawful purpose, based on the relevant function or activity of the Practice where it is the responsible party, or based on the relevant function or activity of the responsible party where the Practice is acting as the operator.

1.11. **Condition 3: Purpose specification - retention and restriction of records**

- 1.11.1. The Practice **MUST NOT** retain records of personal information for any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, **UNLESS**:
- retention of the record is required or authorised by law
 - the responsible party reasonably requires the record for lawful purposes related to its functions or activities
 - retention of the record is required by a contract between the parties thereto
 - the data subject, or a competent person (only where the data subject is a child), consents to the retention of the record.
- 1.11.2. The Practice **MUST** determine and should document, in the **Retention of Documents Policy**, the maximum document retention timeframes necessary for achieving the purpose for which the information was collected or subsequently processed.
- 1.11.3. The Practice **MAY** retain records of personal information for longer than is necessary for achieving the purpose for which the information was collected or subsequently processed **FOR** historical, statistical or research purposes **IF** the responsible party has established appropriate safeguards against the records being used for any other purposes.
- 1.11.4. Where the Practice is acting as the responsible party and retains records of personal information for longer than is necessary for achieving the purpose for which the information was collected or subsequently processed **FOR** historical, statistical or research purposes, it **MUST** establish appropriate safeguards against the records being used for any other purposes.
- 1.11.5. Where the Practice is acting as the operator and retains records of personal information for longer than is necessary for achieving the purpose for which the information was collected or subsequently processed **FOR** historical, statistical or research purposes, the responsible party

must ensure that it establishes and provides the Practice with appropriate safeguards against the records being used for any other purposes.

- 1.11.6. Where the Practice, as the responsible party or acting as the operator, has used a record of personal information of a data subject to decide about the data subject, IT MUST:
- retain the record for the period as may be required or prescribed by law or a code of conduct
 - if there is no law or code of conduct prescribing a retention period, retain the record for a period that will afford the data subject a reasonable opportunity, taking all considerations about the use of the personal information into account, to request access to the record.
- 1.11.7. The Practice, as the responsible party, MUST destroy, delete or de-identify a record of personal information as soon as reasonably practicable after the Practice is no longer authorised to retain the record.
- 1.11.8. Where the Practice acts as the operator, on behalf of the responsible party, the responsible party must ensure that the Practice (as operator) is instructed to destroy, delete or de-identify a record of personal information as soon as reasonably practicable after the responsible party is no longer authorised to retain the record.
- 1.11.9. When the Practice destructs, deletes or de-identifies a record of personal information, IT MUST be done in a way that prevents its reconstruction in an intelligible form.
- 1.11.10. The Practice, as the responsible party, MUST restrict processing of personal information, IF:
- its accuracy is contested by the data subject, for long enough to enable the Practice to verify the accuracy of the information
 - the Practice no longer needs the personal information to achieve the purpose for which the information was collected or subsequently processed, but it MUST be maintained for purposes of proof
 - the processing is unlawful and the data subject opposes its destruction, deletion or de-identification and requests the restriction of its use
 - the data subject requests to transmit the personal data to a third party in conjunction with the termination of the services provided by the Practice.
- 1.11.11. Where the Practice is acting as the operator, the responsible party must ensure that the Practice restricts the processing of personal information, when required.
- 1.11.12. Where processing of personal information is restricted, the Practice MUST ONLY process the personal information (except for storage):
- for purposes of proof
 - with the data subject's consent, or a competent person (only where the data subject is a child)
 - for the protection of the rights of another person
 - if the processing is in the public interest
- 1.11.13. Where processing of personal information is restricted and the Practice is the responsible party, the Practice MUST inform the data subject BEFORE lifting the restriction on processing.
- 1.11.14. Where processing of personal information is restricted and the Practice is acting as the operator, the responsible party MUST inform the data subject BEFORE lifting the restriction on processing.

1.12. Condition 4: Further processing limitation - further processing to be compatible with purpose of collection

- 1.12.1. Where the Practice performs further processing of personal information, it MUST be according to, or compatible with, the specific, explicitly defined and lawful purpose for which it was collected,

which relates to a function or activity of the Practice, where it is the responsible party, or relates to a function or activity of the responsible party, where the Practice is acting as the operator on behalf of the responsible party.

1.12.2. Where the Practice is the responsible party, IT MUST assess whether further processing is compatible with the purpose of collection by considering the:

- relationship between the purpose of the intended further processing and the purpose for which the information was collected
- nature of the information concerned
- consequences of the intended further processing for the data subject
- way the information was collected
- contractual rights and obligations between the parties.

1.12.3. Where the Practice is acting as the operator, the responsible party must ensure that the Practice considers the required aspects when it assesses whether further processing is compatible with the purpose of collection.

1.12.4. When the Practice is assessing whether further processing is compatible with the purpose of collection, it may consider the following aspects to be compatible:

- the data subject, or a competent person (only where the data subject is a child), consents to the further processing of the information
- the information is available in or derived from a public record or has deliberately been made public by the data subject
- further processing is necessary:
 - to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences
 - to comply with an obligation imposed by law or to enforce legislation about the collection of revenue (in terms of the South African Revenue Service Act)
 - for the conduct of proceedings in a court, or tribunal, which have commenced, or are reasonably contemplated
 - in the interests of national security
- the further processing of the information is necessary to prevent or mitigate a serious and imminent threat to:
 - public health or public safety
 - the life or health of the data subject or another individual
- the information is used for historical, statistical or research purposes and the responsible party ensures that the further processing is carried out solely for those purposes and will not be published in an identifiable form
- the further processing of the information is according to an exemption granted by the Regulator.

1.13. Condition 5: Information quality - quality of information

1.13.1. The Practice, as the responsible party, MUST take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated, where necessary, based on the purpose for which the personal information is collected or further processed.

1.13.2. Where the Practice is acting as the operator, the responsible party must ensure that the Practice takes reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated, where necessary, based on the purpose for which the personal information is collected or further processed.

1.14. Condition 6: Openness – Documentation

- 1.14.1. The Practice, as the responsible party, MUST maintain the documents of all processing operations that it is responsible for, and which information must be included in the **PAIA Manual**, relating to the:
- purpose of the processing
 - description of the categories of data subjects and of the information or categories of information relating thereto
 - recipients, or categories of recipients, to whom the personal information may be supplied
 - planned transborder flows of personal information
 - general description, allowing a preliminary assessment of the suitability of the information security measures to be implemented by the Practice, to ensure the confidentiality, integrity and availability of the information that is to be processed.
- 1.14.2. The Practice MUST update its **PAIA Manual**, to include the required information for protecting personal information and publish the updated **PAIA Manual**, as required.
- 1.14.3. Where the Practice is acting as the operator, the responsible party must ensure that the Practice maintains the required documents of all processing operations that it is responsible for.

1.15. Condition 6: Openness – notification to data subject when collecting personal information

- 1.15.1. The Practice, as the responsible party, MUST ensure that the data subject is aware of the:
- information that is collected
 - source from which the information is collected, where the information is not collected directly from the data subject
 - name and address of the Practice, as the responsible party
 - purpose for collecting the information
 - fact that the information they supply is either voluntary or mandatory
 - consequences of failing to provide the information
 - law authorising or requiring the collecting of the information
 - fact that, where applicable, the Practice, as the responsible party, intends to transfer the information to a third country or international organisation, and the level of protection afforded to the information by that third country or international organisation
 - other relevant information which is necessary in the specific circumstances in which the information is, or is not, to be processed to enable processing for the data subject to be reasonable, such as:
 - recipient, or category of recipients, of the information
 - nature or category of the information
 - existence of the right of access to and the right to rectify the information collected
 - existence of the right to object to the processing of personal information
 - right to lodge a complaint to the Information Regulator and the contact details of the Information Regulator
- 1.15.2. The Practice, as the responsible party, MUST make the data subject aware of the required information BEFORE the personal information is collected IF it is collected directly from the data subject, UNLESS the data subject is already aware of the required information.
- 1.15.3. The Practice, as the responsible party, MUST make the data subject aware of the required information BEFORE the personal information is collected, or as soon as reasonably practicable after it has been collected, IF it is NOT collected directly from the data subject.
- 1.15.4. Where the Practice, as the responsible party, has previously made the data subject aware of the required information, IT complies with the awareness requirement for subsequent collection from the data subject of the same information, or information of the same kind, IF the purpose of collection of the information remains the same.

- 1.15.5. Where the Practice is acting as the operator, the responsible party must ensure that the data subject is aware of the required information within the prescribed timeframe.
- 1.15.6. The Practice, as the responsible party or acting as the operator, DOES NOT need to comply with the awareness requirement, IF:
- data subject, or a competent person (only if the data subject is a child), consents to the non-compliance
 - non-compliance would not prejudice the legitimate interests of the data subject
 - non-compliance is necessary:
 - to avoid prejudice to the maintenance of the law by a public body, including the prevention, detection, investigation, prosecution and punishment of offences
 - to comply with an obligation imposed by law, or to enforce legislation about the collection of revenue (in terms of the South African Revenue Service Act)
 - for the conduct of proceedings in a court or tribunal which have been commenced or are reasonably contemplated
 - in the interests of national security
 - compliance would prejudice a lawful purpose of the collection
 - compliance is not reasonably practicable in the circumstances of the case
 - information will:
 - not be used in a form in which the data subject may be identified
 - be used for historical, statistical or research purposes.
- 1.15.7. The Practice collects and further processes information of clients, as data subjects, for functions or activities, including, but not limited to:
- Performing the initial assessments as well as ongoing assessments
 - Providing the products or services, or related products or services, to clients, and/or carrying out services reasonably related thereto
 - Confirming, verifying and updating information
 - Conducting market or client satisfaction research
 - Audit and record keeping
 - Legal or similar proceedings
 - Activities relating to maintaining and improving the client relationship
 - Providing communication about the Practice, Therapists, its products, services and regulatory matters which may affect clients
 - Sharing information with other relevant health practitioners, educators, product suppliers and service suppliers with whom we have relationships, to process information on our behalf, or to those who provide services to us and/or the client.
 - Complying with legal and regulatory requirements or when it is otherwise allowed by law.
- 1.15.8. The Practice collects and further processes information of employees, as data subjects, for functions or activities including, but not limited to:
- Determining the fitness and propriety of the person; ordinarily in relation to employees
 - Confirming, verifying and updating information, including aspects such as qualifications, education, employment history, and criminal history
 - Legal or similar proceedings
 - Audit and record keeping
 - Sharing information with other relevant health practitioners, product suppliers and service suppliers, with whom we have client relationships, to process information on our behalf, or to those who provide services to us
 - Complying with legal and regulatory requirements or when it is otherwise allowed by law.

1.16. Condition 7: Security safeguards - security measures on integrity and confidentiality of personal information

1.16.1. The Practice, as the responsible party, or acting as the operator, MUST 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, damage to, or unauthorised destruction of personal information
- unlawful access to or processing of personal information

by taking reasonable measures to:

- identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control
- establish and maintain appropriate safeguards against the risks identified
- regularly verify that the safeguards are effectively implemented
- ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

1.16.2. Where the Practice is acting as the operator, the responsible party must ensure that the Practice secures the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable, technical, and organisational measures.

1.16.3. The Practice, as the responsible party, MUST have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

1.16.4. Where the Practice is acting as the operator, on behalf of the responsible party, the responsible party must ensure that the Practice has due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

1.17. Condition 7: Security safeguards - information processed by operator, or person acting under authority

1.17.1. Where the Practice is acting as the operator, IT MUST:

- only process the information with the knowledge or authorisation of the responsible party
- treat personal information that comes to its knowledge as confidential and must not disclose it,

unless required by law or during the proper performance of its duties.

1.18. Condition 7: Security safeguards - security measures regarding information processed by operator

1.18.1. Where the Practice is acting as the operator, the responsible party must, in terms of the written contract between the responsible party and the Practice, ensure that the Practice establishes and maintains the required security measures.

1.18.2. Where the Practice is acting as the operator, IT MUST notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.

1.19. Condition 7: Security safeguards - notification of security compromises

1.19.1. Where the Practice is the responsible party and there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, it MUST NOTIFY (in writing):

- Regulator
- data subject, unless the identity of the data subject cannot be established,

as soon as reasonably possible after the discovery of the compromise, considering the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the Practice's information system.

- 1.19.2. The Practice, as the responsible party, may only delay notifying the data subject IF a public body responsible for the prevention, detection or investigation of offences, or the Regulator, determines that notification will impede a criminal investigation by the public body or the Regulator.
- 1.19.3. Where the Practice is acting as the operator, IT MUST immediately notify the responsible party and provide the responsible party with the required information so the responsible party can notify the Regulator and the data subject.
- 1.19.4. The Practice MUST notify, in writing, the data subject about a personal information compromise in at least one (1) of the following ways:
 - mailed to the data subject's last known physical or postal, address
 - sent by e-mail to the data subject's last known e-mail address
 - placed in a prominent position on the website of the responsible party
 - published in the news media
 - as may be directed by the Regulator.
- 1.19.5. The Practice MUST ensure that the notification to the data subject provides sufficient information to allow the data subject to take protective measures against the potential consequences of the personal information compromise, including:
 - description of the possible consequences of the security compromise
 - description of the measures that the responsible party intends to take or has taken to address the security compromise
 - recommendation about the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise
 - if known to the responsible party, the identity of the unauthorised person who may have accessed, or acquired, the personal information.
- 1.19.6. The Practice, as the responsible party, MUST publicise, in a way specified by the Regulator, a personal information compromise if directed to do so by the Regulator.
 - The Regulator will direct a responsible party to publicise a personal data compromise if it has reasonable grounds to believe that the publicity would protect a data subject who may be affected by the compromise.

1.20. Condition 8: Data subject participation – access to personal information

- 1.20.1. A data subject that provides the Practice with adequate proof of identity may ask the Practice, as the responsible party, to confirm, free of charge, whether or not the Practice holds personal information about the data subject.
- 1.20.2. A data subject that provides the Practice with adequate proof of identity may ask the Practice, as the responsible party, for the record or a description of the personal information about the data subject held by the Practice including information about the identity of all third parties, or categories of third parties, who have or have had access to the information:
 - within a reasonable time
 - at a prescribed fee, if any
 - in a reasonable way and format
 - in a form that is generally understandable.
- 1.20.3. If the Practice communicates personal information to a data subject in response to a request from the data subject, it MUST advise the data subject of their right to request their personal information to be corrected.

- 1.20.4. If the Practice, as the responsible party, requires a data subject making a request to pay a fee for services provided to the data subject to enable the responsible party to respond to a request, the Practice:
- must give the applicant a written estimate of the fee before providing the services
 - may require the applicant to pay a deposit for all, or part, of the fee.
- 1.20.5. The Practice, as the responsible party, MAY OR MUST refuse, as the case may be, to disclose information requested by the data subject to which the grounds for refusal of access to records are set out in the applicable sections of the PAIA.
- Refer to the PAIA manual for details.
- 1.20.6. The Practice, as the responsible party, must apply the applicable provisions of the PAIA, for access to health, or other, records.
- Refer to the PAIA manual for details.
- 1.20.7. Where a data subject requests access to personal information and part of that information MAY OR MUST be refused in terms of the PAIA, the Practice MUST disclose all other parts of the requested information.
- 1.20.8. The Practice will take reasonable steps to confirm a data subject's identity before providing details of their personal information.

1.21. Condition 8: Data subject participation – correction of personal information

- 1.21.1. A data subject may, using the prescribed Form 2, request the Practice, as the responsible party, to:
- correct or delete personal information about the data subject in its possession or under its control which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully
 - destroy, or delete, a record of personal information about the data subject, which the Practice, as the responsible party, is no longer authorised to retain because it is no longer necessary for achieving the purpose for which the information was collected or subsequently processed
- 1.21.2. Where the Practice, as the responsible party, receives a request to correct or delete, personal information, it MUST, as soon as reasonably practicable:
- correct the information
 - destroy, or delete, the information
 - provide the data subject, to their reasonable satisfaction, with credible evidence, in support of the information having been corrected or deleted
 - where agreement cannot be reached between the Practice and the data subject and if the data subject requests, take reasonable steps in the circumstances to attach to the information, in a way that it will always be read with the information, an indication that a correction of the information has been requested, but has not been made
- 1.21.3. Where the Practice, as the responsible party, has taken steps that result in a change to the data subject's personal information and the changed information has an impact on decisions that have been, or will be, taken in respect of the data subject in question, it MUST, if reasonably practicable, inform each person, body or responsible party to whom the personal information has been disclosed, of those steps.
- 1.21.4. The Practice, as responsible party, MUST notify a data subject who has made a request to correct or delete their personal information, of the action taken due to the request.

- 1.21.5. The Practice will take reasonable steps to confirm a data subject's identity before correcting or deleting their personal information.

1.22. Condition 8: Data subject participation – manner of access

- 1.22.1. The Practice **MUST** consider that the provisions of the PAIA, about the form of requests, apply to requests for access to personal information.
- Refer to the PAIA manual for details.
- 1.22.2. The Practice should ensure that requests from data subjects are received using the prescribed forms for the type of request as prescribed by the Regulator.

1.23. Processing of special personal information

- 1.23.1. The Practice, as the responsible party, **MAY NOT process personal information about:**
- religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex, life or biometric information of a data subject
 - criminal behaviour of a data subject to the extent that the information relates to:
 - alleged commission by a data subject of an offence
 - proceedings about an offence allegedly committed by a data subject or the disposal of the proceedings,

UNLESS the prohibition on processing special personal information does not apply.

- 1.23.2. The Practice must be aware that the prohibition on processing special personal information **DOES NOT APPLY**, IF the:
- processing is carried out with the consent of a data subject
 - processing is necessary for the establishment, exercise or defence of a right or obligation in law
 - processing is necessary to comply with an obligation of international public law
 - processing is for historical, statistical or research purposes, to the extent that:
 - purpose serves a public interest and the processing is necessary for the purpose concerned
 - it appears to be impossible or would involve a disproportionate effort to ask for consent,

and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent

- information has deliberately been made public by the data subject
 - provisions applicable to obtaining authorisation about a data subject's religious or philosophical beliefs, criminal behaviour or biometric information are complied with, as applicable to the case.
- 1.23.3. The Practice, as the responsible party, may apply to the Regulator to process special personal information if the processing is in the public interest and if appropriate safeguards have been put in place to protect the personal information of the data subject.
- The Regulator may approve the application but may impose reasonable conditions related to the authorisation.
- 1.23.4. The Practice may process personal information about a **data subject's race or ethnic, origin**, **IF** the processing is carried out to:
- identify data subjects and **only when this is essential to identify data subjects**; AND
 - comply with laws and other measures designed to **protect or advance persons or categories of persons disadvantaged by unfair discrimination**.

- 1.23.5. The Practice may process personal information about a **data subject's health or sex life**, IF it is a:
- medical professional, **healthcare professional**, healthcare institution or facility, or social service, IF the processing is necessary for the proper treatment and care of the data subject, or for the administration of the institution or professional practice;
 - insurance Practice, medical scheme, medical scheme administrator and managed healthcare organisation, if the processing is necessary for:
 - assessing the risk to be insured by the insurance Practice or covered by the medical scheme and the data subject has not objected to the processing;
 - the performance of an insurance or medical scheme, agreement; or
 - the enforcement of contractual rights and obligations;
 - school, if the processing is necessary to provide special support for pupils or making special arrangements in connection with their health or sex life;
 - public or private body managing the care of a child, if the processing is necessary for the performance of its lawful duties;
 - public body, if the processing is necessary for the implementation of prison sentences or detention measures; or
 - administrative body, pension fund, employer or institution working for them, if the processing is necessary for:
 - the implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the health or sex life of the data subject; or
 - the reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity.
- 1.23.6. Where the Practice may process personal information about a data subject's health or sex life, the information may only be processed by responsible parties, subject to an obligation of confidentiality by virtue of office, employment, profession or legal, provision, or established by a written agreement between the responsible party and the data subject.
- 1.23.7. Where the Practice may process information about a data subject's health or sex life and is not subject to an obligation of confidentiality by virtue of office, profession or legal provision, it must treat the information as confidential unless it is required by law, or in connection with its duties, to communicate the information to other parties who are authorised to process the information.
- 1.23.8. The prohibition on processing any of the categories of special personal information does not apply IF it is necessary to supplement the processing of personal information about a data subject's health, with a view to the proper treatment or care of the data subject.
- 1.23.9. Personal information about inherited characteristics may not be processed for a data subject from whom the information has been obtained, UNLESS:
- a serious medical interest prevails; or
 - the processing is necessary for historical, statistical or research activity.
- 1.23.10. The Practice may process personal information about a **data subject's criminal behaviour or biometric information** IF it is a body charged by law with applying criminal law, or IF it is a responsible party, who has obtained the information in accordance with the law.
- 1.23.11. Where the Practice may process personal information about its **employees' criminal behaviour or biometric information**, it must be done in accordance with the rules established in compliance with labour legislation.
- 1.23.12. The prohibition on processing any of the categories of special personal information does not apply IF it is necessary to supplement the permitted processing of information about criminal behaviour or biometric information.

1.24. Processing of personal information of children

- 1.24.1. The Practice, as the responsible party, **MAY NOT process personal information of children UNLESS the prohibition on processing the personal information of children does not apply.**
- 1.24.2. The Practice, as the responsible party, **MAY process personal information of children IF** it is:
- **carried out with the prior consent of the legal guardian** (competent person)
 - necessary for the establishment, exercise or defence of a right or obligation in law
 - necessary to comply with an obligation of international public law
 - for historical, statistical or research purposes, to the extent that:
 - the purpose serves a public interest and the processing is necessary for the purpose concerned; or,
 - it appears to be impossible or would involve a disproportionate effort to ask for consent,
- and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent
- personal information has deliberately been made public by the child with the consent of a competent person.
- 1.24.3. The Practice will obtain consent from the competent person (legal guardian) of children BEFORE processing children's information.

1.25. Disclosure of personal information

- 1.25.1. The Practice may disclose a data subject's personal information to any of the Practice's associates, other relevant healthcare practitioners, client-relevant educators, relevant product suppliers and relevant third-party service providers. The Practice has agreements in place to ensure compliance with the confidentiality and privacy conditions.
- 1.25.2. The Practice may share a data subject's personal information with, and obtain information about a data subject from, third parties but only for the reasons specified in this Policy.
- 1.25.3. The Practice may disclose a data subject's information where it has a duty or a right, to disclose the information in terms of applicable legislation, the law or where it may be deemed necessary to protect the rights of the Practice.

1.26. Safeguarding personal information

- 1.26.1. Personal information of data subjects must be adequately protected. The Practice continuously reviews its security controls and processes to ensure that personal Information is secure.
- 1.26.2. The Practice is a responsible party that is an association of independent occupational therapists, represented by **LARA HIRSCHMANN** as the **information officer**.
- 1.26.3. The information officer's contact details are reflected elsewhere in this Policy. They are responsible for compliance with the conditions of the lawful processing of personal information and other provisions of the POPI Act and the regulations thereto.
- 1.26.4. This Policy has been put in place throughout the business of the Practice and training about this Policy and the POPI Act will be provided to employees and associates regularly where applicable and necessary.

- 1.26.5. Each new employee must sign an employment contract and each associate must sign an association contract containing relevant consent clauses for the use and storage of employee and client personal information or any other action required in terms of the POPI Act.
- 1.26.6. Archived client personal information is stored securely in hardcopy and/or electronically. Access to retrieve the archived personal information is restricted to individuals authorised by the information officer.
- 1.26.7. The agreements that the Practice has in place with its responsible parties, product suppliers and third-party service providers must stipulate that the responsible parties, product suppliers and third-party service providers, are responsible for complying with the POPI Act and the regulations thereto; alternatively, materially similar data protection laws.
- 1.26.8. Electronic files and data are backed up daily.
- 1.26.9. **The Practice** is responsible for system security, which protects against unauthorised third party access and physical threats and Electronic Information Security.

1.27. Access to, and correction of, personal information

1.27.1. Information officer contact details

Full name: Lara Hirschmann

Email address: lara.hirschmann@gmail.com

Telephone number/s: +27 82 562 1113

1.27.2. Practice's head office details

Physical address: 9 Silwood Road, Bramley, 2090

Contact email: lara.hirschmann@gmail.com

Contact telephone: +27 82 562 1113

2. Consequences of non-compliance with the policy

- 2.1.** All employees and associates are obliged to comply with the Policy as a contractual condition. Employee non-compliance is a breach of their relevant contract and such misconduct may be subject to disciplinary action which may lead to dismissal. Non-compliance by an employee will be dealt with according to the Practice's disciplinary policy. For assessing and addressing the non-compliance, reports made by the compliance officers, internal audit, external audit and the Authorities will be considered for appropriate action to be taken. Associate non-compliance may result in legal action being taken.

3. Policy review

- 3.1.** The policy will be reviewed annually, updated, if necessary, and the latest version will be adopted and approved by the **Practice as represented by the information officer.**

5. Policy approval and information

Policy owner	Lara Hirschmann			
Policy type	Compliance			
Approver's signature	LH			
Approved by (this version)	LH			
Approval date (this version)	20 June 2021			
Version number	V1			
<u>Summary of policy history</u>				
<u>Version number</u>	<u>Drafted/adapted/reviewed by</u>	<u>Creation/review date</u>	<u>Approved by</u>	<u>Approval date</u>
V01	LH	20 June 2021	LH	20 June 2021