PRIVACY POLICY

Prepared in terms of section 51 of the Promotion of Access to Information Act 2 of 2000 (as amended)

HOPE@WORK
PRACTICE

PERSONAL INFORMATION PROTECTION POLICY

Practice Name	**HOPE@WORK PRACTICE**
Registration Number	**SACSSP – 10-26634 | Practice – 089 000 0392766**
Date reviewed	**01.07.2023**

1. INTRODUCTION

1.1. Hope@Work Practice ("the Company") is an authorised mental health services provider whose business includes the collection of Personal Information from its clients, suppliers and employees. The Company endeavours to comply with all the relevant legislation and regulations relating to the protection of Personal Information.

1.2. This Personal Information Protection Policy (the "Policy") documents and records the principles and policies the Company follows when collecting and Processing Personal Information, describes the required business activities relating to Personal Information Processing and specifies the responsibilities of the Company when complying with the relevant legislation and regulations.

1.3. The Company acknowledges that it must comply with South African legislation, in the form of the Protection of Personal Information Act, 2013 (Act no. 4 of 2013) ("POPIA") as it Processes Personal Information in South Africa. In addition, the Company acknowledges that it has to comply with the European Union General Data Protection Regulation ("GDPR") as GDPR impacts South African based companies that process Personal Information of EU residents, and since the convergence of these various data protection legislation and regulations are imminent.

2. DOCUMENTS OF REFERENCE

2.1. Protection of Personal Information Act, 2013 (Act no. 4 of 2013);

2.2. European Union General Data Protection Regulation ("GDPR");

2.3. Data Retention Policy;

3. DEFINITIONS

3.1. "Anonymisation" or "De-identify" means irreversibly De-identifying Personal Information such that the person cannot be identified by using reasonable time, cost and technology. Personal Information Processing principles do not apply to Anonymized data.

3.2. "Data Subject" means the person to whom the Personal Information relates.

3.3. "Encryption" means scrambling the entire contents of a set of information using mathematical techniques.

3.4. "Operator" means a natural or juristic person, public authority or any other institution which Processes Personal Information on behalf of the Responsible Party.

3.5. "Personal Information" is defined in the Protection of Personal Information Act (Act no. 4 of 2013) ("POPIA") as follows:

"Information relating to 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, wellbeing, disability, religion, conscience belief, culture, language and birth of the person;

(b) information relating to the education or the medical, financial, criminal, or the employment history of the person;
(c) any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignments 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
(i) disclosure of the name itself would reveal information about the person."

3.6. "Processing" is defined in POPIA as follows:

"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 through transmission, distribution or making available in any form; or
(c) merging, linking, as well as restriction, degradation, erasure or destruction of information."

3.7. "Pseudonymisation" means the Processing of Personal Information in such a manner that the Personal Information can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately.

3.8. "Re-identify" means to resurrect any information that has been De-identified.

3.9. "Responsible Party" means a public or private body or any other person that, alone or in conjunction with others, determines the purpose and means for Processing Personal Information.

4. PRINCIPLES REGARDING PERSONAL INFORMATION PROCESSING

4.1. Accountability

The Company acknowledges that, as a Responsible Party, it must ensure compliance with the relevant regulations. Accordingly, the Information Officer has been designated with this responsibility.

4.2. Lawful Processing of Personal Information

The Company will ensure that Personal Information is Processed lawfully, fairly and transparently concerning the Data Subject. Personal information collected must not be excessive, must be legally justifiable and not collected from third parties without good reason.

4.3. Purpose limitation

Personal information collected is limited and relevant concerning the specific purpose for which it is processed. Accordingly, the Company will apply Anonymisation or Pseudonymisation to Personal Information, where possible, to reduce the risk to the Data Subject. Personal information will not be stored for any longer than necessary.

4.4. Data minimisation

The Company will ensure that Personal Information is adequate and limited to what is necessary for the purpose for which it is processed.

4.5. Information quality

All Personal Information collected will be complete and accurate, and the Company will take reasonable steps to ensure that inaccurate data is corrected in a timely manner.

4.6. Lawful processing of personal information

The Company will ensure that Personal Information is processed lawfully, fairly and transparently. Personal information collected must not be excessive, must be legally justifiable and not collected from third parties without good reason.

4.7. Security safeguard relating to integrity and Personal Information confidentiality

The Company will ensure that Personal Information is Processed securely and will use appropriate information technology measures to protect Personal Information against accidental or unlawful destruction, loss, amendment or unauthorised access. Notification of any data breaches will occur timeously.

4.8. Restriction on further processing

Personal information may only be processed for the purpose for which it was collected under specific conditions.

4.9. Transparency

The Company will transparently process Personal Information.

4.10. Data Subject participation

Data Subjects will be allowed to access their Personal Information and request that it is corrected or deleted if inaccurate. The Company acknowledges that Personal Information that is inaccurate, irrelevant, inappropriate, ambiguous or unlawfully obtained is to be corrected or deleted.

4.11. Storage period limitation

Personal information must be stored for no longer than necessary for the purposes for which it is processed.

5. INFORMATION PROTECTION PROCESSES

5.1. Communication to Data Subjects

The Company is responsible for communicating to Data Subjects which types of Personal Information is collected, the purposes of processing the Personal Information, the Processing methods, the Data Subjects' rights, and the retention periods. In addition, the Information Officer will ensure that the Data Subjects are notified when Personal Information is shared with third parties.

The Information Officer will authorise which Personal Information is processed. In addition, the Company will perform a Data Protection Impact Assessment for each Personal Information Processing activity.

5.2. Data Subject's consents

The Information Officer will be responsible for retaining the records of the Data Subject's consents regarding the Processing of Personal Information. In addition, the Information Officer will ensure that any request to correct, change or destroy Personal Information is dealt with within a reasonable time frame and keep records thereof. The Company will ensure that any consents given by the Data Subjects are voluntary, specific, and an informed expression of will.

5.3. Personal Information collection

The Company will attempt to collect the minimum amount of Personal Information possible. If any Personal Information is collected from a third party, the Information Officer will ensure that the information is collected lawfully.

5.4. Personal Information use, retention and deletion

All Personal Information will be used, retained and deleted or destroyed in a manner consistent with the purpose described in the Company's Privacy Policy. In addition, the Company will ensure that Personal Information remains accurate and confidential when being Processed.

5.5. Data Subject's access rights

The Company's Information Officer will ensure that Data Subjects are provided with reasonable access to their Personal Information. The Company will further ensure that its Data Subjects can update, correct, delete or transfer their Personal Information if required.

5.6. Personal Information transferability

Data Subjects have the right to receive a copy of their Personal Information provided to the Company. The Information Officer will ensure that the Data Subject's Personal Information can be transmitted to another party if required and ensure that such requests are processed timeously.

5.7. Third-party disclosures

In instances where the Company utilises third parties to Process Personal Information, the Information Officer will ensure that the third parties have adequate security measures to safeguard Personal Information.

5.8. Right to delete or destroy Personal Information

The Company will ensure that Personal Information of the Data Subject can be deleted or destroyed upon the Data Subject's request. Personal Information destruction will occur as soon as reasonably practical after the request has been made.

5.9. Privacy Policy

A Privacy Policy will be available to Data Subjects of the Company and will be written in clear, plain language. The Privacy Policy will be made available through the Company's website and will include details of how Personal Information is Processed.

The Privacy Policy will also include the name and contact details of the Company's Information Officer, the nature of Personal Information collected, the purpose for its collection and the rights of the Data Subject.

5.10. Security measures

The storage and transfer of Personal Information will occur in a secure environment. The Company will ensure that a risk assessment is completed to identify all reasonably foreseeable internal and external risks to Personal Information under its control. Technical measures will be utilised to secure Personal Information, and such measures may consist of De-identification (anonymisation) or Encryption. The Company will ensure that the Information Regulator is notified of any data breaches as soon as reasonably possible and notify all Data Subjects affected by such breaches.

6. RESPONSIBILITIES OF THE COMPANY

6.1. As the Responsible Party, the Company is committed to accountability, transparency and consensual and responsible Processing of Personal Information.

6.2. The Company intends that this Policy will protect a Data Subject's Personal Information from being compromised in any way, and this Policy is consistent with the privacy laws applicable in South Africa.

6.3. The board of directors of the Company is responsible for approving this Policy, and the Information Officer is responsible for managing and implementing the Personal Information protection processes.

6.4. The Company's Compliance Officer will monitor Personal Information protection regulation to ensure that all developments are incorporated into the Company's business activities.

6.5. The Information Officer of the Company will ensure that employees' awareness of Personal Information protection is raised and will further ensure that employee Personal Information protection occurs.

7. WHAT PERSONAL INFORMATION DOES THE COMPANY REQUIRE?

The Company is a Responsible Party in respect of the Personal Information you (Data Subject) provide to the Company. The Company processes the following types of Personal Information from you:

- Identification number
- Residential or business operating address
- Contact numbers
- Email addresses
- Banking details
- Any other information that may be requested from the Data Subject, if required.

8. WHY DOES THE COMPANY REQUIRE YOUR PERSONAL INFORMATION?

8.1 This Personal Information is required in terms of the Financial Intelligence Centre Act, 38 of 2001 and the Company's Risk Management and Compliance Programme.

8.2. As an authorized mental health services provider, we collect and process your personal information for a purpose you would reasonably expect, including:

- Complying with obligations contained in the contract concluded between yourself and Hope@Work Practice;
- To verify your identity and to confirm, verify and update your details;
- Sending relevant/legally required communications or materials to clients or interested parties;
- Complying with legal and regulatory obligations in terms of applicable laws and industry requirements;
- Managing relationships with clients and/or their representatives;
- Managing any claims or enforcement actions taken against Hope@Work Practice;
- Managing subscriptions to Hope@Work Practice newsletters and marketing material as well as other data dissemination arrangements.

9. HOW IS YOUR PERSONAL INFORMATION PROCESSED?

Hope@Work Practice does not use personal information for any reason other than is required to comply with the law, effectively render its services to clients, and to carry on its business in the mental health services industry. All personal information, in addition to being processed in accordance with Hope@Work Practice's POPIA Policy, is treated with the strictest confidence. Maintenance of confidentiality and compliance with Hope@Work Practice's POPIA Policy are conditions of employment for all staff. Hope@Work Practice will not sell personal information, nor will it exchange or process personal information with/to any third party for any purpose other than as provided for in Hope@Work Practice's POPIA Policy and in compliance with POPIA.

9.1 Your Personal Information is processed at 58a Kerk Street, Paarl, 7646. Storage of your Personal Information takes place on a cloud-based server hosted by Health Bridge.

9.2 No third-party providers have direct access to your Personal Information unless specifically required by law and to satisfy client due diligence principles.

9.3 To manage client relationships with service providers and their staff/representatives;

9.4 To manage interactions with potential clients and other interested parties via "live chat", subscriptions, email or telephone for quality assurance purposes, the protection of their rights and record keeping;

9.5 To verify client details/identity for crime and prevention, detection and related purposes;

9.6 To the extent required, to comply with audit requirements;

9.7 For historical, statistical and research purposes.

10. HOW LONG DOES THE COMPANY KEEP YOUR PERSONAL INFORMATION?

Under South African law, the Company must keep your Personal Information for a six (6) year period following the date of termination of the business relationship according to the Company's Personal Information Retention Policy. After this period, your Personal Information will be irreversibly destroyed. For more information on the Company's Personal Information retention schedule, please refer to our Personal Information Retention Policy, which can be accessed at hello@hopeatworkpractice.com.

11. WHAT ARE YOUR RIGHTS?

11.1 Should you believe that any of your Personal Information held by the Company is incorrect or incomplete, you have the right to request to view this information, rectify it or have it deleted. Please contact the Company's Information Officer on hello@hopeatworkpractice.com should this be required.

11.2 In addition, if you wish to complain about how the Company has handled your Personal Information, please contact the Information Officer at hello@hopeatworkpractice.com. The Company's Compliance Department will investigate your complaint and contact you within two (2) business days of the complaint being lodged and work with you to resolve the matter.

11.3 If your query relating to your Personal Information is not, in your opinion, adequately dealt with, you can contact the Information Regulator on +27 12 406 4818 or inforeg@justice.gov.za to file an official complaint.

12. INFORMATION OFFICER/CONTACT DETAILS

Any questions relating to the Company's Privacy Policy or the treatment of an individual's Personal Information should be addressed to the Information Officer, whose contact details are:

Information Officer	: YOLANDA HUIJSAMER
Telephone number	: +27 (0) 84 302 1608
Physical Address	: 58A Kerk Street, Paarl 7646
E-mail address	: hello@hopeatworkpractice.com

PERSONAL INFORMATION ACCESS REQUEST PROCEDURE

Practice Name	**HOPE@WORK PRACTICE**
Registration Number	**SACSSP – 10-26634 | Practice – 089 000 0392766**
Date reviewed	**01.07.2023**

1. INTRODUCTION

Hope@Work Practice (the "Company") acknowledges that it is a Responsible Party in terms of the Protection of Personal Information Act, 2013 (Act no. 4 of 2013) ("POPIA"). This document describes how the Company responds to requests from Data Subjects for access to their Personal Information. This process will ensure that the Company complies with its legal obligations when Data Subjects request access to their Personal Information from the Information Officer.

2. REFERENCE DOCUMENTS

- The Protection of Personal Information Act, 2013 (Act no. 4 of 2013); and
- European Union General Data Protection Regulation ("GDPR").

3. DEFINITIONS

3.1 "Data Subject" means the person to whom the Personal Information relates.

3.2 "Operator" means a person who processes Personal Information for the Responsible Party in terms of a contract;

3.3 "Personal Information" means any information relating to an identifiable, living natural person, or to the extent applicable, a juristic person. This includes, but is not limited to, information relating to race, gender, sex, pregnancy, marital status, ethnic and social origin, colour, sexual orientation, age, physical or mental health, religion, disability, language, information relating to educational, medical, financial, criminal or employment history, any identifying number, e-mail address, physical address, telephone number, location information, online identifier or biometric Personal Information.

3.4 "Personal Information Access Request" means a process designed to ensure the Company complies with its legal obligations when providing Data Subjects with access to their Personal Information.

3.5 "Processing" means any activity concerning 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, or merging, linking, as well as restriction, degradation, erasure or destruction of Personal Information.

3.6 "Responsible Party" means a public or private body or any other person that, alone or in conjunction with others, determines the purpose and means for Processing Personal Information.

4. PERSONAL INFORMATION ACCESS REQUEST FROM THE DATA SUBJECT

4.1 A personal Information Access Request is a request made by an individual or a juristic entity via its authorised representative for the Company's personal information.

4.2 The Personal Information Access Request provides the Data Subject with the right to view or request copies of Personal Information Process by the Company.

4.3 The Personal Information Access Request must be made in writing to the Information Officer of the Company.

4.4 The Data Subject can make a Personal Information Access Request by:

- Sending an e-mail to the Information Officer at hello@hopeatworkpractice.com
- Sending a Personal Information Access Request by post to the Information Officer at:
  58a Kerk Street
  Paarl 7646

5. PERSONAL INFORMATION ACCESS REQUEST PROCESS

5.1 The individual requesting access to their Personal Information will need to complete a Personal Information Access Request form and provide it to the Information Officer.

5.2 The Information Officer will verify the identity of the individual making the Personal Information Access Request to ensure that the individual has the right to view the Personal Information.

5.3 The Information Officer will notify the Data Subject that their Personal Information Access Request will be attended to within 30 (thirty) days.

5.4 The Information Officer will ensure all relevant Personal Information is sourced internally or from third parties, if so required.

5.5 The Information Officer will respond to the Data Access Request Form and the Personal Information via a secure method.

6. PERSONAL INFORMATION ACCESS REQUEST REJECTIONS

Personal Information Access Requests may be rejected if:

- The Personal Information is stored only for statistical purposes, and the identification of the Data Subject from the Personal Information is not possible; or
- The Personal Information Access Request is made for other non-Personal Information protection purposes.

7. EXCLUSIONS

A Data Subject does not have the right to access Personal Information recorded about another Data Subject unless Personal Information is being accessed by the authorised representative of the Data Subject.

The following information will not be disclosed by the Company:

- Information about other Data Subjects;
- Publicly available information;
- Privileged documents; and
- Information protected by copyright law.

Information Officer

YOLANDA HUIJSAMER

Signature

PERSONAL INFORMATION ACCESS REQUEST FORM

Practice Name	**HOPE@WORK PRACTICE**
Registration Number	**SACSSP – 10-26634 | Practice – 089 000 0392766**
Date reviewed	**01.07.2023**

DATA SUBJECT INFORMATION:

Name	
Surname	
Identity number	
Physical address	

DETAILS OF PERSONAL INFORMATION REQUESTED:

Print name:	
Date:	
Signature:	

PLEASE ENCLOSE A COPY OF YOUR IDENTIFICATION DOCUMENT AND PROOF OF RESIDENCE. EMAIL THE COMPLETED FORM TO THE INFORMATION OFFICER AT hello@hopeatworkpractice.com

PERSONAL INFORMATION BREACH PROCEDURE

Practice Name	**HOPE@WORK PRACTICE**
Registration Number	**SACSSP – 10-26634 | Practice – 089 000 0392766**
Date reviewed	**01.07.2023**

1. INTRODUCTION

This document describes the process followed by Alantra Hope@Work Practice (the "Company") when responding to a breach of Personal Information. The process includes notification to the Data Subject and the Company's obligations to the relevant Regulatory Authorities.

2. REFERENCE DOCUMENTS

- The Protection of Personal Information Act, 2013 (Act no. 4 of 2013) ("POPIA");
- European Union General Data Protection Regulation ("GDPR").
- Personal Information Breach Register;
- Personal Information Protection Impact Assessment; and
- Personal Information Retention Policy.

3. DEFINITIONS

3.1 "Data Subject" means the person to whom the Personal Information relates.

3.2 "Operator" means a natural or juristic person, public authority or any other institution which Process Personal Information on behalf of the Responsible Party.

3.3 "Personal Information" means any information relating to an identifiable, living natural person, or to the extent applicable, a juristic person. This includes, but is not limited to, information relating to race, gender, sex, pregnancy, marital status, ethnic and social origin, colour, sexual orientation, age, physical or mental health, religion, disability, language, information relating to educational, medical, financial, criminal or employment history, any identifying number, e-mail address, physical address, telephone number, location information, online identifier or biometric Personal Information.

3.4 "Personal Information Access Request" means a process designed to ensure the Company complies with its legal obligations when providing Data Subjects with access to their Personal Information.

3.5 "Personal Information Breach(es)" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to Personal Information transmitted, stored or otherwise processed.

3.6 "Processing" means any activity concerning 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, or merging, linking, as well as restriction, degradation, erasure or destruction of Personal Information.

3.7 "Regulatory Authority" means the Information Regulator as established by POPIA or any other relevant Regulatory Authority.

3.8 "Responsible Party" means a public or private body or any other person that, alone or in conjunction with others, determines the purpose and means for Processing Personal Information.

4. PERSONAL INFORMATION BREACH RESPONSE

4.1 The Information Officer must ensure that resources, with the relevant skills and knowledge, are established to respond to any Personal Information Breaches.

4.2 Together with the Information Officer, the resources are responsible for ensuring that a Personal Information Breach response process exists and that a response to any Personal Information Breach can be executed timeously.

4.3 The Information Officer has the authority to utilise external parties' services to deal with Personal Information Breaches.

5. PERSONAL INFORMATION BREACH RESPONSE DUTIES

The Information Officer and the resources responsible for Personal Information Breaches must implement the following processes:

- Validation
- Investigation
- Requirements to mitigate
- Resolution tracking
- Reporting
- Coordination with the relevant regulatory authorities; and
- Notification to the relevant Data Subjects

6. PERSONAL INFORMATION BREACH RESPONSE PROCESS

6.1 The Information Officer and the reliable resources for Personal Information Breaches must ensure that a breach response process is initiated as soon as anyone notices that a suspected/ actual Personal Information Breach has occurred.

6.2 The Information Officer and the reliable resources for Personal Information Breaches must ensure that a breach response process is initiated as soon as anyone notices that a suspected/ actual Personal Information Breach has occurred.

6.3 The Information Officer must ensure that all information relating to the Personal Information Breach is documented.

7. PERSONAL INFORMATION BREACH NOTIFICATIONS

7.1 Notifications from the Operator to the Responsible Party

The Information Officer of the Responsible Party must report any actual or suspected breach of Personal Information to the Responsible Party.

The notification must include the following:

- A description of the Personal Information Breach;
- The types of Personal Information affected;
- The consequences of the Personal Information Breach;
- The number of Data Subjects affected by the Personal Information Breach; and
- Processes implemented to remedy any future Personal Information Breaches

7.2 Notification from the Responsible Party to the Regulatory Authority

The Information Officer must:

- Ensure that the Personal Information Breach is reported to the relevant Regulatory Authority;
- Perform a Personal Information Protection Risk and Impact Assessment;
- Record the Personal Information Breach in the Personal Information Breach Register; and
- Notify the relevant Regulatory Authority of the Personal Information Breach within 72 (seventy-two) hours of its occurrence.

7.3 Notification from the Responsible Party to the Data Subject

The Information Officer must notify Data Subjects of Personal Information Breaches. The notification must contain the following information:

- A description of the Personal Information Breach;
- Types of Personal Information affected;
- The consequences of the Personal Information breach;
- Number of Data Subjects affected by the Personal Information Breach; and
- Processes implemented to remedy any future Personal Information Breaches.

Information Officer

YOLANDA HUIJSAMER

Signature