



## **PROTECTION OF PERSONAL INFORMATION (POPI) & PROMOTION OF ACCESS TO INFORMATION POLICY (PAIA)**

### ***Introduction***

The company is obliged to comply with the Protection of Personal Information Act (No. 4 of 2013) (“POPI”) as well as the Promotion of Access to Information Act (No. 2 of 2000) (“PAIA”), given that it processes the personal information of its employees, clients and other data subjects from time to time as well as that there may be requesters of information relating to the company and its operations.

The company guarantees its commitment to protecting data subject and third party privacy as well as ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.

POPI requires the company to inform data subjects as to how their personal information is collected, processed, secured, disclosed, destroyed and the like.

This Policy therefore sets out the manner in which the company deals with such personal information, stipulates the general purpose for which such information is used as well as how data subjects can participate in this process in relation to their personal information.

**Appropriate stakeholders should be made aware of the contents of this Policy when their consent is requested for the processing of their personal information.**

In addition, this policy also addresses the company's responsibility under the Promotion of Access to Information Act (No. 2 of 2000) (PAIA) and the processing personal information provisions must be read along with this statutory provision. In respect of PAIA, the company has developed a manual and made it available as prescribed in section 51 of the PAIA. Where parties/ requesters submit requests for information disclosure in terms of this manual, internal measures have been developed together with adequate systems to process requests for information or access thereto.

The right of access to records of the company by a requester under PAIA requires of the company that a requester must be given access to a record if -

(a) that record is required for the exercise or protection of any rights;

(b) that person complies with the procedural requirements in PAIA and the s51 manual relating to a request for access to that record; and

(c) access to that record is not refused in terms of any ground for refusal contemplated in the PAIA statute.

The provisions of this policy must be read along with all other relevant practices and procedures that are used to operationalise the purpose hereof.

### ***Collection of personal information***

The company collects and processes data and information pertaining to its employees, suppliers, clients and other stakeholders (data subjects). The type of information will depend on the need for which it is collected and will be processed for that process only. Whenever possible, the company will inform the data subject

of the information required, the purpose thereof and the other rights contained at law. This will include whether the information is mandatory or optional.

Where necessary the company will indicate to the data subject the consequence of failing to provide such personal information. For example, the company may not be able to employ an individual without certain personal information relating to that individual or the company may not be in a position to render services to a client in the absence of certain information which is required.

Examples of the personal information the Company collects includes, but is not limited to information relating to an **identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person** -

- 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.

### ***Processing limitation***

Personal information will be processed by the company in a manner that is -

(a) lawful; and

(b) reasonable (not infringe the privacy of the data subject).

Specific limitations that the Company shall observe in processing personal information includes –

- Minimality and adequacy given the purpose for which it was originally collected;
- Obtaining consent to the processing if required in the circumstances;
- Carrying out actions for the conclusion or performance of a contract;
- Complying with an obligation imposed by law on the company;
- Protecting a legitimate interest of the data subject;
- Processing for the proper performance of a public law duty by a public body;

- Processing is necessary for pursuing the legitimate interests of the company or of a third party to whom the information is supplied.

A data subject may object, at any time, to the processing of personal information and if a data subject has objected to the processing of personal the company shall no longer process the personal information.

Collection must be directly from the data subject, except as otherwise provided for unless the information is contained in or derived from a public record or has deliberately been made public by the data subject.

The company shall not process special personal information without complying with the specific provisions of the POPI statute (and with the above section) and such information pertains to personal information concerning—

- 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
- the criminal behaviour of a data subject to the extent that such information relates to the alleged commission by a data subject of any offence or any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

### ***Collection of employee information***

For the purposes of this Policy, employees include potential, past and existing employees of the company.

The company will, when appointing new employees, require information from the prospective employee in order to process the employee's information on the company's systems. Such information is reasonably necessary for the company's record purposes as well as to ascertain if the prospective employee meets the requirements for the position to which he or she is being appointed, and is suitable for appointment as well as qualifies for certain benefits.

The company will use and process such employee information for purposes including those set out below and to make lawful decisions in respect of that employee and its business.

#### ***Use of employee information***

Employees' personal information will only be used for the purpose for which it was collected and intended. This would include, but is not limited to:

- submissions to the Department of Employment and Labour
- submissions to the Receiver of Revenue
- for audit and recordkeeping purposes
- in connection with legal proceedings
- in connection with and to comply with legal and regulatory requirements
- in connection with any administrative functions of the Company
- disciplinary action or any other action to address the employee's conduct or capacity
- in respect of any employment benefits that the employee is entitled to
- pre and post-employment checks and screening
- any other relevant purpose to which the employee has been notified of

- any compliance requirements at law.

Should information be processed for any other reason, the company will inform the employee accordingly.

The company acknowledges that personal information may only be processed if certain conditions are met which, depending on the merits include -

- The employee consents to the processing
- The processing is necessary to attend to the justifiable rights and obligations of the parties
- The processing complies with an obligation imposed by law on the company
- Processing protects a legitimate interest of the employee
- Processing is necessary for pursuing the legitimate interests of the company or of a third party to whom information is supplied.

### ***Collection of client and/ or supplier information***

For purposes of this Policy, clients and suppliers include potential, past and existing clients and suppliers.

The company collects and processes its clients' and suppliers personal information, for purposes such as those mentioned hereunder. The type of information will depend on the need for which it is collected and will be processed for that purpose only. Examples of personal information collected from clients and suppliers include, but is not limited to:

- Identity number, name, surname, address, postal code
- Residential and postal address
- Contact information
- Banking details

- Company registration number
- Full name of the legal entity
- Tax and/or VAT number
- Details of the person responsible for the client's account

The company also collects and processes clients' personal information for marketing purposes in order to ensure that our products and services remain relevant to our clients and potential clients.

### ***Use of client and supplier information***

The personal information of these parties will only be used for the purpose for which it was collected and as agreed. This may include, but not be limited to:

- Providing products or services to clients
- In connection with sending accounts and communication to a client in respect of services rendered
- Referral to other service providers
- Confirming, verifying and updating client details
- Conducting market or customer satisfaction research
- For audit and record keeping purposes
- In connection with legal proceedings
- In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

The company acknowledges that personal information may only be processed if any of the conditions set out hereunder are met:

- Client consents to the processing;
- The processing is necessary to attend to rights and obligations that are justifiable;



- The processing complies with an obligation imposed by law on the company;
- Processing protects a legitimate interest of the party;
- Processing is necessary for pursuing the legitimate interests of the company or of a third party to whom information is supplied.

### ***Disclosure of personal information***

The Company may share data subject's personal information with third parties as well as obtain information from such third parties for reasons set out above.

The Company may also disclose data subject's information where there is a duty or a right to disclose in terms of applicable legislation, the law or where it may be necessary to protect the company's rights.

### ***Safeguarding personal information and consent***

It is a requirement of POPI to adequately protect the personal information the company holds and to avoid unauthorised access and use of personal information. The company shall review its security controls and processes on a regular basis to ensure that personal information is secure.

It will take appropriate, reasonable technical and organizational measures to prevent loss or damage or unauthorized destruction of personal information, and unlawful access to or processing of personal information.

This will be achieved by –

- Identifying internal and external risks;
- Establishing and maintain appropriate safeguards;
- Regularly verifying these safeguards and their implementation;
- Updating the safeguards;
- Implementing generally accepted information security practices and procedures.

The Company shall appoint an Information Officer who is responsible for the encouragement of compliance with the conditions of the lawful processing of personal information and other provisions of POPI and PAIA. The responsibilities of the Information Officer include –

- That a compliance framework is developed, implemented, monitored and maintained;
- That a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;
- That a manual is developed, monitored, maintained and made available as prescribed in section 51 of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000);
- internal measures are developed together with adequate systems to process requests for information or access thereto; and

- company staff awareness sessions are conducted regarding the provisions of the Act, regulations made in terms of the Act, codes of conduct, or information obtained from the Regulator.

### **Information Officer details**

Name: Michele Cronje

Telephone number: 0448734513

Fax number:

Postal address: PO Box 9803, George, 6539

Physical address: 4 Sunningdale close, King George Park, George, 6529

Email address: college@sanguinewellness.co.za

Each new employee will be required to sign an employment contract containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI.

Every employee currently employed within the Company will be required to either sign an addendum to their employment contract containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI OR be trained on the provisions and application of POPI and PAIA.

The Company's suppliers, insurers and other third-party service providers will be required to sign a service level agreement guaranteeing their commitment to the Protection of Personal Information. This is, however, an ongoing process that will be evaluated as required.

Consent to process client information is obtained from data subjects (or a person who has been given authorisation from the client to provide the client's personal information) during the introductory, appointment and needs analysis stage of the relationship as far as is reasonably possible.

### ***Direct Marketing***

The rights of data subjects in respect of direct marketing by means of unsolicited electronic communications, directories and automated decision-making must be complied with at all times. In this regard, the company shall ensure that -

- The processing of personal information of a data subject for the purpose of direct marketing by means of any form of electronic communication, including automatic calling machines, facsimile machines, SMS's or e-mail is not allowed unless the data subject has given his, her or its consent to the processing; or is a customer of the company.
- In the event of direct marketing, it will only approach data subjects whose consent is required and who have not previously withheld such consent, **only once** in order to request the said consent. This will be done in the prescribed manner and form.

In addition, the Company will only process the personal information of a data subject

who is a customer of the company and where the contact details of the data subject were acquired in the context of the sale of a product or service. The data subjects will only be approached for the purpose of direct marketing of the company's own similar products or services. In all instances, the data subject shall be given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of his, her or its electronic details at the time when the information is collected.

Any communication for the purpose of direct marketing will contain details of the identity of the sender or the person on whose behalf the communication has been sent and an address or other contact details to which the recipient may send a request that such communications cease.

### ***Transfer of information outside of SA***

The company will not transfer personal information about a data subject to a third party who is in a foreign country unless—

- the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection of personal information and effectively upholds principles for reasonable processing of the information.
- the data subject consents to the transfer;
- the transfer is necessary for the performance of a contract between the data subject and the company;
- the transfer is necessary for the conclusion or performance of a contract

concluded in the interest of the data subject between the company and a third party; or

- the transfer is for the benefit of the data subject, and it is not reasonably practicable to obtain the consent of the data subject to that transfer and if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

### ***CCTV***

Video footage that has been recorded, processed and stored via CCTV camera surveillance systems comprise personal information insofar as it is 'information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person.' The company will, when making use of CCTV, alert people as to the use of CCTV on the premises.

### ***Security breaches***

Should the company detect a security breach on any of its systems that contain personal information, the company shall take the required steps to assess the nature and extent of the breach in order to ascertain if any information has been compromised.

The company shall notify the affected parties should it have reason to believe that their information has been compromised. Such notification shall only be made where the company can identify the data subject to which the information relates. Where it is not possible it may be necessary to consider website publication and whatever else the Information Regulator prescribes.

Notification will be provided in writing by means of either:

- email
- registered mail
- place on our website.

The notification shall provide the following information where possible:

- description of possible consequences of the breach;
- measures taken to address the breach;
- recommendations to be taken by the data subject to mitigate adverse effects;
- the identity of the party responsible for the breach.

In addition to the above, the company shall notify the Regulator of any breach and/or compromise to personal information in its possession and work closely with and comply with any recommendations issued by the Regulator.

The following provisions will apply in this regard –

- The Information Officer will be responsible for overseeing the investigation;
- The Information Officer will be responsible for reporting to the Information Regulator within 3 working days of a breach/ compromise to personal information;
- The Information Officer will be responsible for reporting to the Data Subject(s) within 3 working days of a breach/ compromise to personal information;
- The timeframes above are guidelines and depending on the merits of the situation may require earlier or later reporting.

### ***Access and correction of personal information***

Data subjects have the right to request access to any personal information that the company holds about them.

Data subjects have the right to request the company to update, correct or delete their personal information on reasonable grounds. Such requests must be made to the company's Information Officer (see details above) or to the Company's head office (see details below).

Where an employee or client objects to the processing of their personal information, the company may no longer process said personal information. The consequences of the failure to give consent to process the personal information must be set out before the data subject confirms his/her objection.

The data subject must provide reasons for the objection to the processing of his/her personal information.

### **Head office details**

Name: Sanguine Spa and College

Telephone number: 0448734513

Fax number:

Postal address: PO Box 9803



Physical address: 4 Sunningdale close, King George Park, George, 6530

Email address: college@sanguinewellness.co.za

### ***Retention of records***

The company shall ensure the safeguarding and protection of all personal information or data. The company is obligated to retain certain information as prescribed by law. This includes but is not limited to the following:

With regard to the Companies Act, No. 71 of 2008 and the Companies Amendment Act No 3 of 2011, hard copies of the documents mentioned below must be retained for 7 years:

- Any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Act
- Notice and minutes of all shareholders meetings, including resolutions adopted and documents made available to holders of securities
- Copies of reports presented at the annual general meeting of the company
- Copies of annual financial statements required by the Act and copies of accounting records as required by the Act.

The Basic Conditions of Employment No. 75 of 1997, as amended requires the Company to retain records relating to its staff for a period of no less than 3 years.

### ***Amendments to this policy***

Amendments to this Policy will take place from time to time subject to the discretion of the Company and pursuant to any changes in the law. Such changes will be brought to the attention of employee's clients where it affects them.

### ***Requests for information***

In terms of requests to be processed under **POPI**, the following forms shall be used –

In terms of requests for information under **PAIA**, the provisions of the PAIA s51 Manual must be complied with and **Form C** completed.

Any requests and/ or advice can be directed to the **Information Officer** set out in this policy and in the s51 PAIA manual.