POLICY ON DATA PROTECTION AND PRIVACY OF INFORMATION

(Please read this policy with the Information Security, Records and Website Privacy Policies)

1. INTRODUCTION

This policy sets out iNFUSSION's commitment to ensuring that any personal data, including special category personal data, which iNFUSSION processes, is carried out in compliance with data protection laws. iNFUSSION processes the personal data of staff, clients and suppliers, but is committed to ensuring that all the personal data that it processes is done in accordance with data protection law.

This policy is part of the overall protection and disclosure of information policies and should be read together with the following policies where applicable:

- Information Security Policy
- Website privacy policy and statement
- Records Retention & Destruction Policy
- Public Access to Information and the Protection of Personal Information Manual

2. SCOPE

2.1 This policy applies to all personal data processed by iNFUSSION and is part of our approach to compliance with data protection laws. All iNFUSSION's staff are expected to comply with this policy and failure to comply may lead to disciplinary action for misconduct, including dismissal.

2.2 Data protection laws refer to the legal rules that regulate how organisations can process personal information, in specific Protection of Personal Information Act 4 of 2013 (POPIA) – to the extent that we process personal information in South Africa;

3. DEFINITIONS

In this document:

3.1 "**confidential information**" shall include:

3.1.1 all information that the Company has an interest or obligation to keep confidential by law, contract or otherwise; and

3.1.2 secret knowledge, trade secrets, intellectual property, know-how, processes and techniques, technical detail, method of operating, cost and source of material, pricing and purchasing policies and other matters which relate to iNFUSSION's' business in respect of which information is not readily available in the ordinary course of business to a competitor of iNFUSSION;

3.1.3 personal information;

3.2 ''**data subject''** means the person to whom personal information relates;

3.3 "**electronic communication**" means any communication of information by electronic means;

3.4 "**electronic communications systems**" means all systems used by the Company that enable electronic communications, including (without limitation) the Internet, voice mail, electronic mail and facsimiles;

3.5 "**employee**" means a part- or fulltime employee of iNFUSSION, including any contractor with access to iNFUSSION's information systems;

3.6 **"information**" means representations of information in any form generated, sent, received or stored and includes:

3.6.1 voice, where the voice is used in an automated transaction; and

3.6.2 a stored record;

3.7 "**information system**" means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes electronic communications systems;

3.8 "**intellectual property**" shall include all copyright, rights in business names, trade marks, trade names, service marks, patents, designs and/or inventions, as well as all rights to source codes, trade secrets, and all other rights of a similar character (regardless of whether such rights are registered and/or capable of registration) and all applications and rights to apply for protection of any of the same;

3.9 "**interconnect**" means to link two telecommunications systems so that users of either system may communicate with users of, or utilise services provided by means of, the other system or any other telecommunication system

3.10 "**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;

3.11 "**owner**" means, in respect of information, the person nominated as custodian of such information in terms of this policy, being the DIRECTOR;

3.12 "**personal information**" has the meaning given to it in POPIA, being information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

3.12.1 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;

3.12.2 information relating to the education or the medical, financial, criminal or employment history of the person;

3.12.3 any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

3.12.4 the biometric information of the person;

3.12.5 the personal opinions, views or preferences of the person;

3.12.6 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;

3.12.7 the views or opinions of another individual about the person; and

3.12.8 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;

3.13 "**processing**" means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

3.13.1 the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

3.13.2 dissemination by means of transmission, distribution or making available in any other form; or

3.13.3 merging, linking, as well as restriction, degradation, erasure or destruction of information;

3.14 "**records coordinator**" means the person nominated by board of directors as such from time to time, being the ISO; and

3.15 "**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;

3.16 "**sensitive information**" means information designated as "internal use only", "confidential", or "secret" in terms of this policy.

4. LEGISLATIVE REQUIREMENTS

POPIA was assented to on 26 November 2013. The purpose of POPIA is to give effect to section 14 of the Constitution, being the constitutional right to privacy by protecting Personal Information and regulating the free flow and Processing of Personal Information. POPI sets minimum conditions which all Responsible Parties, as defined in POPIA must comply with so as to ensure that Personal Information is respected and protected.

4.1 Conditions for Lawful Processing

Chapter 3 of POPI provides for the minimum Conditions for Lawful Processing of Personal Information by a Responsible Party. These conditions may not be derogated from unless specific exclusions apply as outlined in POPI. Below is a description of the eight Conditions for Lawful Processing as contained in POPI:

4.1.1 Accountability - the Responsible Party has an obligation to ensure that there is compliance with POPI in respect of the Processing of Personal Information.

4.1.2 Processing limitation - Personal Information must be collected directly from a Data Subject to the extent applicable; must only be processed with the consent of the Data Subject and must only be used for the purposes for which it was obtained.
4.1.3 Purpose specification - Personal Information must only be processed for the specific purpose for which it was obtained and must not be retained for any longer than it is needed to achieve such purpose.
4.1.4 Further processing limitation - further processing of Personal Information must be compatible with the initial purpose for which the information was collected.
4.1.5 Information quality - the Responsible Party must ensure that Personal Information held is accurate and updated regularly and that the integrity of the information is maintained by appropriate security measures.
4.1.6 Openness - there must be transparency between the Data Subject and the Responsible Party.
4.1.7 Security safeguards - a Responsible Party must take reasonable steps to ensure that adequate safeguards are in place to ensure that Personal Information is being processed responsibly and is not unlawfully accessed.
4.1.8 Data Subject participation - the Data Subject must be made aware that their information is being processed and must have provided their informed consent to such processing.

4.2 Data Protection Principles

When processing personal data, it ensures that:

4.2.1 It is processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')
4.2.2 It is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation')
4.2.3 It is all adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
4.2.4 It is all accurate and, where necessary, kept up to date and that reasonable steps will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'). The data subject must ensure that correct and updated information is provided.
4.2.5 It is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation')
4.2.6 It is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')
4.2.7 Requests from a data subject who wishes to exercise their rights under data protection law as appropriate, always communicating in a concise, transparent, intelligible and easily accessible form and without undue delay.

4.3 Processing of Personal information

4.3.1 Personal information is any information that relates to the data subject as an identifiable living human being or existing juristic person (to the extent that applicable law allows).
4.3.2 You are identifiable where someone could identify you for example, by reference to your name, identification number or other identifier. Personal information can include your:
4.3.2.1 Demographic information – 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 or birth;
4.3.2.2 Historical information – information relating to your education, medical, financial, criminal or employment history;
4.3.2.3 Identifying information – identifying symbol, number, email address, physical address, phone number, location information, online or other identifier;
4.3.2.4 Biometric information – information related to unique physical or other biological traits about your body, such as your fingerprint or eye colour pattern;
4.3.2.5 Self-opinion information – personal opinions, views or preferences;

4.3.2.6 External opinion information – assessments in terms of other peoples' views or opinions about you; and

4.3.2.7 Name (under certain circumstances) – name, if it appears with the other personal information relating to you or if the disclosure of the name itself would reveal information about you;

4.4 Special category personal data

4.4.1 iNFUSSION processes special category data of clients and third parties as is necessary in terms of regulatory requirements.

4.4.2 iNFUSSION processes special category data of employees as is necessary to comply with employment and social security law. This policy sets out the safeguards we believe are appropriate to ensure that we comply with the data protection principles set out above. iNFUSSION also has a data retention policy which sets out how long special category data will be held onto.

4.4.3 This includes the following personal data which may reveal :

4.4.3.1 Racial or ethnic origin

4.4.3.2 The processing of genetic data, biometric data for the purpose of uniquely identifying a natural person

4.4.3.3 An individual's health

4.4.3.4 Criminal convictions or offences

4.4.3.5 This list is not exhaustive.

4.4.4 Personal information includes the information that is collected in the following manner:

4.4.4.1 automatically as our employee, contractor or affiliate;

4.4.4.2 accept on registration or submission; or

4.4.4.3 you provide voluntarily; but

4.4.4.4 excludes anonymous, de-identified, statistical, and public information.

4.4.5 Personal Information may only be processed for a specific purpose. The purposes for which the Company processes or will process personal information is only for record and communication purposes.

4.4.6 The Company shall under no circumstances use any personally identifiable information as obtained through its recruitment, administrative or related process, for any other purpose but its disclosed intended purpose.

4.4.7 The company shall duly endeavor to adhere to all the current in-effect policies related to remarketing or any other form of advertising in all of its marketing campaigns. (In instances of possible non-conformity to such, the Company shall endeavor to rectify such in a prompt manner).

4.5 Information security measures

iNFUSSION undertakes to institute and maintain the data protection measures to ensure confidentiality, integrity and availability of personal information under its care. Measures include but are not limited to Firewalls, virus protection software and updates, logistical and physical access control, secure setup of IT infrastructure. (Refer to Information Security Policy)

4.5.1 **Access Control of Persons:** iNFUSSION shall implement suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment where the data is processed.

4.5.2 **Data Media Control**: iNFUSSION undertakes to implement suitable measures to prevent the unauthorized manipulation of media, including reading, copying, alteration or removal of the data media used by the Company and containing personal data of students, clients, personnel (or other data subjects).

4.5.3 **Data Memory Control:** iNFUSSION undertakes to implement suitable measures to prevent unauthorized input into data memory and the unauthorized reading, alteration or deletion of stored data.

4.5.4 **User Control:** iNFUSSION shall implement suitable measures to prevent its data processing systems from being used by unauthorized persons by means of data transmission equipment.

4.5.5 **Access Control to Data:** iNFUSSION represents that the persons entitled to use iNFUSSION's data processing system are only able to access the data within the scope and to the extent covered by their respective access permissions (authorization).

4.5.6 **Organization Control:** iNFUSSION shall maintain its internal organization in a manner that meets the requirements of this Manual.

4.6 Objection to the Processing of Personal Information by a Data Subject

Section 11 (3) of POPIA and regulation 2 of the POPIA Regulations provides that a Data Subject may, at any time object to the Processing of his/her/its Personal Information in the prescribed manner as set out in the Act. The data subject must follow procedures set out in POPIA.

4.7 Request for correction or deletion of Personal Information

Section 24 of POPI and regulation 3 of the POPI Regulations provides that a Data Subject may request for their Personal Information to be corrected/deleted in the prescribed form and within contractual parameters.

5. PROCEDURES FOR PERSONAL INFORMATION COLLECTION AND PROCESSING

5.1 The Company may request data subjects to provide certain identifying information (including first name, surname and email address).

5.2 The Company may request certain optional information on a voluntary basis.

5.3 The Company must obtain written consent from the data subject to collect personal information in accordance with applicable law.

5.4 The Company must obtain the data subject's permission to process the information. Processing includes gathering your personal information, disclosing it, and combining it with other personal information.

5.5 The Company generally collects personal information directly wherever possible, but may sometimes collect it indirectly through third parties.

5.6 If a Data Subject provides Personal Information on behalf of another, the Company will not be able to process the query or request unless such query or request is accompanied with the required permission and consent from the owner of that Personal Information

5.7 If a Data Subject is under the age of 18, such person's Personal Information will only be processed if the minor's parent or legal guardian gives the required consent or permission to the processing of the provided Personal Information.

5.8 iNFUSSION must only use personal information in a manner consistent with the purpose for which it was collected.

5.9 Processing means gathering, disclosing or combining it with other information. The following types of personal information is generally processed:

Purpose	Data	Consent
Enquiring about our organisation and its work	Name, email, message and phone number	Legitimate interest – the information enables us to respond correctly.
Subscribing to updates/ information relevant to the work	Name and email/ whatsapp/ etc	Consent - you have given your active consent.
Applying for, or taking up employment with us	Age, demographical information, birth dates, identity numbers, passport numbers, occupation information, personal and work email and contact details and bank accounts.	Contract - you have entered into a contractual relationship with us; or consent - you have given your active consent.
Collaborating with us	Demographical information, birth dates, identity numbers, passport numbers, personal and work email and contact details.	Contract - you have entered into a contractual relationship with us; or consent - you have given your active consent.
Personal Information for client application	Age, demographical information, birth dates, identity numbers, passport numbers, occupation information, personal email and contact details	Contract - you have entered into a contractual relationship with us; or consent - you have given your active consent.
Conducting business with us as a supplier	Work email and contact details, certain financial information relating to references, bank accounts.	Contract - you have entered a contractual relationship with us.
Conducting business with us as a client	Client details, contact details, financial information relating to.	Contract - you have entered a contractual relationship with us.

Website functionality	Website activity collected through cookies	Legitimate interest - it is necessary for us to store a small amount of information, usually through cookies, to deliver functionality that you would expect.

5.10 **Purpose of Processing**

The Company may possess records relating to suppliers, shareholders, contractors service providers, staff and clients. A document records and disposal policy are in place.

5.10.1 Categories of Recipients for Processing the personal information:

5.10.1.1 Capturing and organizing of data

5.10.1.2 Storing of data

5.10.1.3 Sending of emails and other correspondence to clients/ students

5.10.1.4 Conducting due diligence tests

5.10.1.5 General administration.

5.10.2 Examples include: administration of students, clients, service providers and staff, rendering service according to instructions given by clients, keeping of accounts and records and complying with tax laws

Data Subject	Type of information	Purpose
Corporates	Name, ID, contact detail, Postal Address, Corporate Telephone Number, Personal Cellular, Corporate E-Mail Address, tax and company data, confidential correspondence.	Contract data captured on system Contract securely locked in steel cabinet. Access by authorized persons only
Clients	Name, ID, contact detail, Home/ Postal Address, Home Telephone Number, Personal Cellular, Mobile Personal E-Mail Address, tax related information, gender, age, nationality, academic results	Contract data captured on system Contract securely locked in steel cabinet. Access by authorized persons only
Contracted service providers	Name, ID, contact detail, (corporate address and telephone number, financial, tax, company related documents, confidential correspondence.	Procurement records kept securely.
Recipients of personal information:	Only specific information as provided by the respective director/ records owner.	Contracting
Employees	Gender, race, marital status, language, education information, tax and financial information, ID, physical and postal address, criminal behavior, health/ wellbeing	Secured Personnel files.

5.11 Cross-border flows of Personal Information

Section 72 of POPI provides that Personal Information may only be transferred out of the Republic of South Africa under certain conditions. The Company does not transmit information Cross Border.

6. PERSONAL INFORMATION DATA ACCESS

6.1 iNFUSSION has processes in place to ensure that it can facilitate any request made by an individual to exercise their rights under data protection law.

6.2 All staff must receive training on the protection of personal information and the access thereof.

6.3 Requests by data subjects for personal information must be dealt with in terms of regulations.

6.4 The data subject has the following rights:

6.4.1 Revocable consent – where consent is required to collect, use, or disclose personal information, the data subject may withdraw his/her consent at any time, subject to legal or contractual restrictions and reasonable notice;

6.4.2 Rectification or deletion –the right to ask for rectification or deletion of information (subject to legal or contractual restrictions);
6.4.3 Access –the right of access by the data subject to access his/ her personal information;
6.4.4 Complain to supervisory authority –the right to lodge a complaint with the relevant supervisory authority if the data subject feels that his/her rights have been infringed.

7. RESPONSIBILITY FOR PROCESSING OF PERSONAL DATA

6.1 The Act states that the Responsible Party for the processing of Personal Information is the head of the organization, i.e. the DIRECTOR.
6.1.1 The Data Subject" or "DS" means the person to whom personal information relates
6.1.2 The 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;
6.1.3 "Owner" means, in respect of information, the person nominated as custodian of such information
6.1.4 Responsible Party**"** or "RP" 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.

6.2 The DIRECTOR delegates the responsibility of personal protection of information to the respective divisions, i.e. to classify, keep and destroy records. In the event of doubt, the records coordinator will nominate an owner. The records coordinator for information is set out below:
6.2.1.1 HR for Personnel Information
6.2.1.2 Operations for Client Information
6.2.1.3 Finance for all fiscal related Information including contracting and service provider personal information.
6.2.1.4 ICT for systems and cloud information protection.
6.2.1.5 Divisions for respective third party agreements in consultation with ICT, e.g. Marketing for Social Media service provider.
6.2.1.6 Compliance for company secretarial and governance related information and acts as Deputy Information Officer.

8. MONITORING AND REVIEW

This policy shall be regularly monitored and reviewed, at least every two years.