DATA PROTECTION POLICY

(PROTECTION OF PERSONAL INFORMATION)

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Whereas Likwid Properties ("the Organisation") is obliged to comply with POPIA and data protection standards.

1.2 Whereas the Organisation provides a range of services to its clients, as well as the management of its own Employees, requiring access to and processing of Personal Information/data of individuals and juristic persons ("Persons").

1.3 Whereas the Organisation is committed to protecting a Person's privacy and ensuring that their Personal Information is used appropriately, transparently, securely and in accordance with applicable laws.

1.4 Wherefore this Policy sets out how the Organisation shall process, handle and store Personal Information/Personal Data to comply with its data protection and privacy standards and as well as legislation. This Policy must also be read with the Data Breach Management Protocol as well as the Risk Management, and the Information Technology and Electronic Communications Policies.

2. DEFINITIONS AND INTERPRETATION

2.1. Unless otherwise expressly stated, or the context otherwise requires, the words and expressions listed below shall, when used in this Policy bear the meanings ascribed to them below and cognate expressions bear corresponding meanings:

2.1.1. "Board" means the Board of Directors of the Organisation serving from time to time;

2.1.2. "Confidential Information" means confidential information relating to the Organisation, including but not limited to: trade secrets, confidential information (i.e. information that is not known in public), technical know-how and data, drawings, system, methods, software processes, client lists, programs, marketing and/or financial information except where such information must be shared between the Organisation and an Employee or between Employees for the purpose of employment or association with the Organisation;

2.1.3. "Consent" means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of Personal Information;

2.1.4. "Data Register" means a register of all processing activities and systems of the Organisation concerning Personal Data set in a format similar to Annexure "**A**";

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

2.1.6. "Directors" means those persons appointed as executive or non-executive directors to the Board according to the Organisation's Memorandum of Incorporation and the ruling policies and procedures applicable to the Organisation from time to time;

2.1.7. "Disaster Recovery Team" means the chief executive officer, chief financial officer, human resources manager, Information Officer and IT Manager of the Organisation;

2.1.8. "Equipment" means computers, laptops, mobile phones, servers, access controls, software, cloud storage and other electronic devices;

2.1.9. "Employee" means an employee of the Organisation, whether permanent or temporary;

2.1.10. "Information Officer(s)" means the Information Officer(s) appointed by the Organisation from time to time;

2.1.11. "Information Regulator" means the information regulatory body established under section 39 of POPIA contactable at:

Email: inforeg@justice.gov.za / Tel: 012 406 4818 / Fax: 086 500 3351.

2.1.12. "IT Manager" means _____ and its designated assignee(s);

2.1.13. "Level of Risk" means the magnitude of a risk expressed in terms of the combination of consequences and their likelihood assessed in terms of the Organisation's Risk Management Policy;

2.1.14. "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;

2.1.15. "Organisation" means Likwid Properties;

2.1.16. "PAIA Manual" means the Organisation's manual in terms of section 51 of the Promotion of Access to Information Act 2 of 2000, as amended from time to time;

2.1.17. "Person" means a natural person or juristic person and may include a customer, franchisee, vendor, independent contractor, job applicants and Employees;

2.1.18. "Personal Information" / "Personal Data" means information or data relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to-

2.1.18.1. 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;

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

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

2.1.18.4. the biometric information of the person;

2.1.18.5. the personal opinions, views or preferences of the person;

2.1.18.6. 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;

2.1.18.7. the views or opinions of another individual about the person; and

2.1.18.8. 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;

2.1.19. "POPIA" means the Protection of Personal Information Act 4, 2013, as amended from time to time;

2.1.20. "Privacy Committee" means the committee established in terms of section 6 to this Policy;

2.1.21. "Privacy Policy" means the Organisation's Privacy Policy as amended from time to time;

2.1.28. "Processing" means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—

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

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

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

2.1.22. "Responsible Party" means the person who determines what information is required and processes that information including where such person outsources part or all of the processing to an Operator;

2.1.23. "Risk Assessment" means the process to comprehend the nature of the risk and to determine the 'Level of Risk' in accordance with the Organisation's Risk Management Policy.

2.1.24. "This Policy" means this Data Protection Policy;

2.2. In this Policy:

2.2.1. table of contents and paragraph headings are for purposes of reference only and shall not be used in interpretation;

2.2.2. unless the context clearly indicates a contrary intention, any word connoting any gender includes the other genders, and the singular includes the plural and vice versa;

2.2.3. When a number of days are prescribed such number shall exclude the first and include the last day unless the last day is not a business day, in which case the last day shall be the next succeeding business day.

3. AIM OF THIS POLICY

3.1. This Policy seeks to ensure that the Organisation:

3.1.1. complies with international legal standards and best practice for the Processing of Personal Data of Data Subjects, both as received from its clients, and as held in respect of its Employees;

3.1.2. protects the rights of its Employees, clients and third parties concerning their Personal Data; and

3.1.3. transparently renders how it Processes Personal Data.

3.2. This Policy also seeks to protect the Organisation against various data security risks including:

3.2.1. breaches of confidentiality through data breaches;

3.2.2. malicious or negligent Employees;

3.2.3. hacking risks; and

3.2.4. the risks of liability in relation to Personal Data in respect of its clients, Employees and third parties.

4. SCOPE AND APPLICATION

4.1. This Policy applies to all Personal Data processed by the Organisation including, Personal Data relating to the Organisation's clients, Employees, suppliers and agents, irrespective of whether the Personal Data is stored electronically, digitally, on paper, or on other materials, or through other methods.

4.2. This Policy applies to all Employees of the Organisation.

4.3. Where practical, Operators processing Personal Data on behalf of the Organisation should be held to the standards set in this Policy.

4.4. This Policy shall be reviewed at least annually.

5. FUNCTIONARIES

5.1. Information Officer(s)

5.1.1. The Organisation's risk and compliance manager shall be appointed and registered as the Information Officer under POPIA.

5.1.2. The Information Officer shall, among others:

5.1.2.1. execute, and bear responsibility for reporting to executive management about compliance with all technological and operational data protection standards and protocols, and related audits;

5.1.2.2. advise executive management of any risk of breach at the earliest opportunity with a view to avoiding any risk or breach, or limiting any damage resulting from it;

5.1.2.3. ensure that all operational and technological data protection standards are complied with;

5.1.2.4. to provide advice where requested concerning data protection impact assessments and implementation of policies and procedures;

5.1.2.5. to inform and advise executive management and the Board of their obligations and responsibilities pursuant to POPIA and any other applicable laws relating to data protection;

5.1.2.6. arrange data protection training and provide advice and guidance to all Employees on this Policy and their data protection obligations;

5.1.2.7. be entitled and have authorisation to initiate disciplinary proceedings against any Employee who at any time breaches any technological and/or organisational and/or operational data protection standard, rule, custom, instruction, policy, practice and/or protocol (verbal, in writing or otherwise) ("**Data Protection Rules**") applicable in any department or area of the operations of the Organisation;

5.1.2.8. review and approve any contracts or agreements with third parties to the extent that they may handle or process Persona Information in respect of the Organisation's Employees, clients, customers, suppliers and/or service providers;

5.1.2.9. attend to requests from individuals to access Personal Information which the Organisation holds about them ("**subject access requests**"); and

5.1.2.10. cooperate with and be the contact point between the Organisation and Information Regulator.

5.1.2.11. issue appropriate, clear, regular rules and directives, whether for the Organisation as a whole or a particular part of it, department, person or level of person in relation to any aspect of the Organisation's organisational security measures.

5.2. **IT Manager**

5.2.1. The IT Manager shall:

5.2.1.1. ensure that all IT systems and Equipment used for Processing and/or storing Personal Data adhere to acceptable and appropriate technical security standards, and is regularly updated;

5.2.1.2. issue appropriate, clear, regular rules and directives, whether for the Organisation as a whole or a particular part of it, department, person or level of person in relation to any aspect of the Organisation's work, including password protocols, data access protocols, levels of persons who enjoy access to certain data sign-on procedures, password safeguarding protocols, sign-on and sign-off procedures, log-on and log-off procedures; the description of accessories, applications and Equipment that will or may be used, and/or that may not be used under any circumstances, and the like;

6. PRIVACY COMMITTEE

6.1. Composition

6.1.1. The Organisation hereby establishes a Privacy Committee, which shall consist of the Information Officer, IT Manager, a financial manager and a human resources manager of the Organisation.

6.2. Aims and Objectives

6.2.1. The Privacy Committee is a key role player in the implementation of the Organisation's Privacy Policy, this Policy and the Data Breach and Incident Management Protocol, by means of ensuring that such policies are adopted, reviewed and complied with.

6.3. **Roles and Responsibilities**

6.3.1. The roles and responsibilities of the Privacy Committee are as follows:

6.3.1.1. to review Organisation's Privacy Policy, this Policy and the Data Breach and Incident Management Protocol as the Organisation evolves in the way it does business and new organisational and technical security risks arise;

6.3.1.2. Evaluate any third-party services the Organisation is considering or may acquire to process or store data, e.g. cloud computing services, payroll services and accreditation agencies;

6.3.1.3. to assist and support the Information Officer in the execution of its regulatory functions and duties;

6.3.1.4. to assist the Information Officer in making data privacy and protection recommendations to the Board for approval.

6.3.1.5. to assist and support the Information Officer manage any suspected or actual data breaches; and

6.3.1.6. to assist and support the Information Officer in monitoring compliance with this Policy and conducting the training of Employees in accordance with the aforementioned policies.

7. RESPONSIBLE PARTIES

7.1. All Employees and Operators shall be responsible for ensuring the safeguarding, protection and avoidance of any unauthorised disclosure or breach of Personal Information in the execution of their employment duties or rendering services to or for the Organisation.

7.2. The Information Officer shall take responsibility for the Organisation's ongoing compliance with this Policy.

8. DATA CATEGORISATION

8.1. The Organisation may process the following categories (types) of Personal Data:

8.1.1. **Identity Information – including names, company names, marital status, title, date of birth, gender, race and legal status, copies of identity documents or passport, photographs, identity number, signatures, and registration number;**

8.1.2. **Contact Information – including billing addresses, delivery addresses, e-email address and telephone numbers;**

8.1.3. **"Credit and Criminal Information" – including credit reports, credit and criminal history, employment information, defaults on credit agreements, and judgements, as maintained by credit bureaus;**

8.1.4. **Financial Information - including bank account details, insurance information, financial statements, tax numbers;**

8.1.5. **Location Information - including data identifying the actual location of a physical address using GPS data and geocodes;**

8.1.6. **Technical Information - including internet protocol (IP) addresses, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technology on the devices used to access our website.**

8.1.7. **Usage Information - including information as to the access and use of our website, products and services.**

8.1.8. **Marketing and Communications Information - including customer and prospective customer preferences in respect of receiving marketing information from us and your communication preferences.**

8.1.9. **Sensitive Information – including** information relating to a customer, supplier, service provider, or Employee's religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information or criminal behaviour.

8.2. For purposes of this Policy, the importance of Personal Data shall be determined with reference to the:

8.2.1. type of Personal Data;

8.2.2. purpose of the Personal Data;

8.2.3. relationship between the Organisation and the Data Subject;

8.2.4. Level of Risk of unauthorised disclosure or access to the Personal Data;

8.2.5. requirements of the ruling regulatory framework applicable to that Personal Data and relationship.

8.3. Financial Information and Sensitive Information shall always be categorised as highly important and high risk.

9. DATA REGISTER

9.1. To ensure its processing of Personal Data is lawful, fair and transparent, the Organisation shall maintain a Data Register.

9.2. The Data Register shall be reviewed at least annually.

9.3. The Data Register template is annexed hereto marked "**A**".

9.4. The Data Register shall record:

9.4.1. the processing activity;

9.4.2. categories of the Data Subjects and Personal Data;

9.4.3. why the Organisation is processing the Personal Data;

9.4.4. the legal basis for processing the Personal Data;

9.4.5. categories of recipients (excluding public authorities) to whom the Personal Data is disclosed or shared;

9.4.6. the data retention period;

9.4.7. whether Personal Data is transferred outside of South Africa and the location thereof; and

9.4.8. a brief description of the technical and organisation security measures applied to the activity or Personal Data.

9.5. A list of the Organisation's Operators shall also be maintained in the Data Register and shall record the contact details of the Operator's Information Officer.

10. REQUESTS FOR ACCESS TO OR ALTERATION OF DATA

10.1. Where an Employee or individual contacts the Organisation requesting access to his/her Personal Information, it shall be referred to as a "**Subject Access Request**".

10.2. Employees and individuals who are the subject of the Personal Information held by the Organisation are entitled to:

10.2.1. enquire what information is held about them and the purpose for holding it;

10.2.2. enquire how to gain access to their own Personal Information; and

10.2.3. be informed of any special measures the Organisation uses to keep such data up to date.

10.3. Subject Access Requests should be made by e-mail, in accordance with the Organisation's PAIA Manual and addressed to the Information Officer, who shall consider and respond to the request in consultation with the Privacy Committee within 30 days.

10.4. The identity of a person making a Data Subject request shall be verified using appropriate security questions before handing over any information requested.

11. LAWFUL PURPOSE

11.1. All Personal Data processed by the Organisation must be done on one of the following lawful bases: consent, contract, legal obligation, legitimate interests, or public task.

11.2. The Organisation shall note the appropriate lawful basis for each processing activity in the Data Register.

11.3. Where Consent is relied upon as a lawful basis for processing data:

11.3.1. evidence of opt-in consent shall be kept together with the Personal Data; and

11.3.2. the form or agreement in terms of which consent is given must inform the data subject of the following at the time of collecting its Personal Data:

(a) the Personal Data being collected, and if not from the data subject then the source from which it is collected (i.e. ITC platforms, body corporates, etc.);

(b) the name and address of the Organisation or any other responsible party;

(c) the purpose of collection;

(d) whether the supply of the Personal Data is voluntary or mandatory;

(e) any consequences of failure to provide such Persona Data;

(f) if the Personal Data is to be transferred to a third party or third country, and a general description of the level of protection afforded to the Personal Data;

(g) any other relevant information.

11.4. Where communications are sent to individuals based on their Consent, the option for the individual to revoke their Consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Organisation's systems (i.e. on mailing lists for direct marketing).

12. DATA MINIMISATION

12.1. The Organisation shall record in the Data Register and process the minimum Personal Data needed to perform its processing activities.

12.2. The Organisation shall ensure that no unnecessary Personal Data is requested or processed for that specific processing activity.

12.3. Should the Organisation obtain Personal Data not requested or unnecessary for the performance of an activity, such Personal Data shall be destroyed or anonymised as soon as practicable in accordance with this Policy.

13. DATA ACCURACY AND INTEGRITY

13.1. The Organisation and its Employees shall take all reasonable steps to comply with the Organisation's Data Protection Rules to ensure Personal Information is kept accurate and up to date.

13.2. Generally, the accuracy of Personal Information shall reviewed by the Privacy Committee at least annually through direct communications with the Data Subject. This may include an invitation via email or telephone to the Data Subject to update any Personal Data. These tasks may be delegated by the Privacy Committee.

13.3. The Organisation's Privacy Policy and service level agreements shall require clients, customers, Employees, and suppliers to notify the Organisation when their information is inaccurate or out of date.

13.4. If Personal Data is of a higher level of importance, greater and more frequent efforts shall be implemented to maintain its accuracy. For example:

13.4.1. Employees should make use of every reasonable opportunity to ensure that a particular component of Personal Information is accurate and up to date when the processing of that component is necessary and important for the performance of the Organisation's services. This may include:

13.4.1.1. handling a client call and confirming a physical address for purposes of an order or delivery;

13.4.1.2. telephonically confirming/updating account details before payment.

13.5. Employees shall access and update only the central, official record of any data or work output document to avoid duplication of efforts and confusion.

Personal Data must be held in as few places as necessary to ensure efficient service delivery and risk avoidance. Employees are prohibited from creating any unnecessary additional Personal Data sets.

14. ARCHIVING AND RETENTION

14.1. The Information Officer is responsible for the continuing process of identifying the records that have met their required retention period.

14.2. Where the Information Officer delegates the task of identifying such records to the Privacy Committee or any other officials, the Information Officer shall remain responsible for such duties.

14.3. Personal Data shall not be retained for longer than necessary, but this will be dependent on the importance of the Personal Data determined according to section 8.2 of this Policy.

14.4. From time to time, it may also be necessary to retain or access historic Personal Data if the Organisation faces unforeseen events like litigation or business disaster recoveries.

14.5. The general data retention period shall be for a period of 5 (five) years after the relevant contract or transaction comes to an end, whereafter such files shall be destroyed in accordance with this Policy.

14.6. Specific data retention periods are set out below:

14.6.1. Customer/business contacts – *contact information* retained while they are a customer, after which the Data Subject usually becomes a prospective customer;

14.6.2. Prospective customer contacts – *contact information retained for 5* years, or until it is identified that the prospective customer no longer has an interest in the services;

14.6.3. Employees – written particulars of Employees, including identifiable information, period of employment, remuneration paid, and any other prescribed information is to be retained while employed and for a period of 3 years after termination of employment or so long as may be prescribed by law;

14.6.4. Contractors – any Personal Data required for the purposes of the service delivery will be retained for a period of 3 years after termination of the contract or longer where legal obligations require it (i.e FICA).

14.6.5. Potential employees - *CVs and covering letters enclosing Personal Date will be retained for* 8 months after an application has completed, or longer where legal obligations or litigation necessitate it.

14.7. Documents that are required to be kept for certain periods of time under the ruling regulatory framework shall be stored in a manner and place that is secure, and if possible, fire resistant.

14.8. Hard copy files shall be securely stored and retained in a locked filing room and electronic versions stored and retained on the server/cloud.

14.9. The Information Officer shall ensure that a system is developed whereby documents are archived, and to this end shall ensure that:

14.9.1. there is a chronological list of archived documents for ease of reference and retrieval, which list shall also disclose where such documents are archived; and

14.9.2. documents are destroyed only once their retention period has expired.

15. DESTRUCTION OF PERSONAL DATA

15.1. The Information Officer is responsible for the continuing process of supervising the destruction of records containing Personal Data.

15.2. Where the Information Officer delegates the task of supervising destruction of records to the Privacy Committee or any other officials, the Information Officer shall remain responsible for such duties.

15.3. Upon expiry of the retention periods, any Personal Data and/or written or electronic file containing Personal Information that is not being retained or used is to be destroyed.

15.4. The Information Officer shall, in consultation with the Privacy Committee, determine the manner of destruction taking into consideration:

15.4.1. the time, cost and need for validation of the destruction;

15.4.2. the importance of the data according to section 8.2 of this Policy;

15.4.3. the Level of Risk associated with the unauthorised access to such data.

15.5. The Organisation may use, among others, any one or more of the following methods to destroy Personal Data or records containing Personal Data:

15.5.1. shredding;

15.5.2. deletion;

15.5.3. data wiping;

15.5.4. overwriting data or anonymising data;

15.5.5. erasure; and/or

15.5.6. physical destruction or electronic shredding.

15.6. Generally, less important information or low risk Personal Data shall be deleted or anonymised whereas important or high-risk Personal Information (Sensitive Information and financial information) shall be securely destroyed electronically or by shredding if possible.

15.7. All unwanted paper records containing Personal Data must be shredded before being recycled or otherwise disposed of.

16. DATA PROTECTION RULES (SECURITY)

16.1. Data Protection Rules are confidential to the Organisation and may only be disclosed with the prior written approval of the Information Officer as its disclosure may impair or undermine the aim of this Policy.

16.2. Data Protection Rules are risk-based and may be adjusted or changed at any time whether verbally or otherwise for a particular Employee, group of Employees, member of the Organisation, or Operator, to ensure adaptive, responsive, efficient and functional IT management to address organisational and technical risks. On this basis, not all Data Protection Rules may be captured in writing.

16.3. The Organisation shall implement, among others, the following technical and organisation security measures to protect Personal Data:

16.3.1. **Technical security measures**

General

(1) Where Personal Data is stored electronically, it must be protected from unauthorised access and accidental deletion by using passwords or file permission controls, or other similar measures.

(2) Personal Data and devices should be protected by using strong passwords that:

(2.1.) are changed regularly and never shared between Employees;

(2.2.) contain special characters and numbers;

(2.3.) do not contain the names of the Employee; and

(2.4.) in all other respects comply with the Usage and Security of Electronic Communications Media Policy.

(3) Multi-factor authentication shall be used, where possible, to access email and other servers allowing access to highly important and high-risk Personal Data.

(4) Where Personal Data is stored on removable media such as a CD, DVD, USB, or external hard drives, these must at all times be locked away securely when not in immediate use.

(5) Save for exceptional circumstances, Personal Data must never be saved directly to laptops or other mobile or removable devices such as tablets or smart phones or sticks or data sticks.

(6) All data shall only be stored on designated drives and servers and shall only be uploaded to approved cloud computing services (Not on Employees' personal cloud storage accounts or USBs).

Encryption

(7) The Organisation shall ensure that its website(s) implement Hypertext Transfer Protocol Secure (including at least SSL).

(8) Wherever practical, Personal Data shall be encrypted before being transmitted electronically.

(9) The following items should also, where practical, be encrypted:

(8.1.) databases;

(8.2.) hard disks / storage;

(8.3.) laptops and mobile devices.

Servers, networks, storage and devices

(10) All servers containing Personal Data will be located in secure protected locations with access control by lock-and-key or similar measures;

(11) Servers must be backed up frequently and at least every 48 hours or in accordance with backup protocols. Such backups should be tested regularly in line with the Organisation's standard backup procedures and protocols under the direction of the IT Manager. The Information Officer will be responsible to schedule a minimum of two random tests each year;

(12) All servers, devices and networks containing or processing Personal Data shall be protected by approved security software, and one or more firewalls, malware and anti-virus protection, and password protection under the direction of the IT Manager.

(13) The Organisation may use external or subcontracted service providers (Operators) to provide data storage services to the Organisation; Provided that the Organisation's data centres and/or servers shall be located within the Republic of South Africa and must be at least ISO 27001 certified for information security management.

(14) Should it be necessary for an Employee to access the Organisation's network and common applications such as email using the Employee's own device, the Organisation must first ensure that the Organisation is able to remotely remove and/or restrict access to its Confidential and/or Personal Data on the Employee's device by, among others, remote wiping.

(15) Where practical, Virtual Private Networks (VPNs) shall be used to access the Organisation's networks and servers.

(16) The Organisation should, where possible, block access to its servers, networks, storage, emails, and the like, from high-risk locations, including but not limited to Russia, China, North Korea, Iran and Afghanistan.

(17) The Organisation shall ensure that devices are regularly updated with the latest operating system security updates.

16.3.2. **Organisational security measures**

General

(1) The Organisation shall ensure that Personal Data is stored securely in accordance with the technical and organisational security measures set out in this Policy, or of an equivalent or higher standard.

(2) A disaster recovery register must be kept to log any security incidents concerning Personal Data and to report on and manage said incidents. This register will be maintained by the Information Officer in accordance with the Organisation's Risk Management Policy and Data Breach and Incident Management Protocol.

(3) All Personal Data shall be deemed Confidential Information, and be handled with a higher degree of care and skill than ordinary information.

(4) Employees shall sign confidentiality and non-disclosure agreements as annexures to their employment contracts (alternatively their employment contracts must provide for similar obligations).

(5) New Employees must receive induction on and a copy of this Policy.

(6) The only person/s entitled to access Personal Data, will be those who need to access it for the execution of their direct work or required outputs. Under no circumstances will Personal Data be shared outside the scope of required work outputs, or informally. In the event of any doubt, an Employee shall be entitled to access Personal Data only after obtaining authorisation from their line manager or a senior manager, where any work output requiring access is unusual or out of the ordinary.

(7) Employees will receive induction and on-the-job training in relation to all security standards applicable to such Employee's service delivery and work outputs involving the Personal Data.

(8) Employees shall keep all Personal Data secure by taking sensible practical precautions and complying with all Data Protection Rules.

Paper records, screens and documents

(9) Where Personal Information is stored on paper, it shall always be kept in a secure place where an unauthorised person cannot access or see it. This applies to Personal Data stored electronically which has been printed out.

(10) Employees should ensure that paper and print outs are not left in places where unauthorised persons can see them, e.g. on a printer or unoccupied desk(s) or unlocked boardroom(s).

(11) Employees must lock their computer screens and clear their desks when left unattended.

(12) When not required, such papers should be kept in a locked drawer, safe or cabinet.

(13) Employees and Operators are entitled to access only those elements of IT systems that are consistent with their authorization and purpose for processing the Personal Data.

Data usage

(14) Employees are prohibited from saving or uploading any copies of Personal Information or content enclosing Personal Information onto their own personal computers, devices, or cloud storage.

(15) Personal Information shall only be used for the purposes set out in the Organisation's Privacy Policy and any subsequent privacy notices published by the Organisation from time to time.

(16) Personal Information shall not be shared informally and shall never be sent by email unless protected by appropriate passwords and/or encryption.

(17) Employees are prohibited from transferring or sending Personal Information to unauthorised Employees or persons.

Third parties

(18) The IT Manager together with the Information Officer must develop and maintain protocols for data transfer to:

(18.1.) ensure such data is protected;

(18.2.) ensure such data is sent to authorised external contacts only; and

(18.3.) avoid such data being sent to any unauthorised external or internal parties.

(19) The Organisation shall enter into operator agreements and/or data transfer agreements with its Operators which ensure appropriate technical and organisation security measures and policies are adopted and implemented by the Operator. Such agreements should, where possible, provide the Organisation with a right to audit or inspect the Operator's compliance as well as oblige the Operator to notify the Organisation of any suspected or actual data breach.

(20) A proper due diligence, considering the organisational and technical privacy measures and risks of any third party, must be undertaken prior to the Organisation sharing any Personal or Confidential Information with such third party.

17. DISCLOSURE WITHOUT CONSENT

17.1. The Organisation may be authorised by law, in limited circumstances, to disclose or provide Personal Data to regulatory authorities and other agencies in circumstances where the Consent of the Data Subject has not been obtained or required.

17.2. In the circumstances set out in paragraph 17.1 above, the Organisation may be obliged to disclose the requested Personal Data, but will first ensure that the request is legitimate and will seek assistance beforehand from its legal advisers and/or other experts. Only the Information Officer will be authorised to furnish the requested Personal Data to the enquiring party after consultation with the Privacy Committee.

18. DATA BREACHES

18.1. Any Employee, Operator, supplier, or service provider shall immediately notify the Information Officer of any suspected or actual data breach or compromise of Personal or Confidential Information, as soon as they become aware of or ought reasonably to have become aware of such suspected or actual breach, in a manner prescribed by the Breach Notification Form annexed to the Organisation's Data Breach and Incident Management Protocol.

19. EMPLOYEE'S CODE OF CONDUCT

19.1. To the extent that this Policy sets out workplace rules governing Employees in the course of their work and services to the Organisation, it shall form part of and is hereby incorporated into the Organisation's Disciplinary Code and Procedure.

19.2. A breach of any rule in relation to the protection of Personal Information/Data set out in this Policy shall form the basis of disciplinary action and, in appropriate circumstances, may lead to dismissal.

19.3. The imposition of any disciplinary sanction or dismissal shall not preclude the Organisation from instituting civil proceedings against an Employee or Operator who acted in breach of this Policy, negligently or otherwise, and where such breach has resulted in liability, loss, reputational damage and/or other damages to the Organisation.

19.4. Every Employee must familiarise him/herself with the content of this Policy, and must remain up to date as and when it is notified of any changes to this Policy in writing (including email correspondence and/or website notification).

20. RESPONSIBLE PARTY FOR PERSONAL AND OTHER CONFIDENTIAL DATA BREACHES

20.1. The Information Officer is responsible for managing Personal Data and other Confidential data security breaches in conjunction with the Privacy Committee and Board of the Organisation.

In disaster situations, the Disaster Recovery Team shall take over responsibility and manage personal data security breaches in conjunction with the Information Officer.

ANNEXURE A

DATA REGISTER TEMPLATE

[see attached Excel document]