Document number: POL_COM_004V3

POLICY: PROTECTION OF PERSONAL INFORMATION

1. PURPOSE

The purpose of this policy is to explain the manner in which Enterprises University of Pretoria (Pty) Ltd ('the Company') deals with personal information of Data subjects, and in addition, the purpose for which this information is used.

This policy also serves to protect the Company from compliance risks associated with the protection of personal information which includes:

- Breaches of confidentiality
- Failing to offer choice to Data subjects to choose how and for what purpose their information is used
- Reputational damage.

The policy also demonstrates the Company's commitment to protecting the privacy rights of Data subjects.

2. SCOPE

This document applies to the Company's Board of Directors, all employees, contractors, suppliers, clients, persons acting on behalf of the company and all potential and existing Data subjects.

3. INTRODUCTION

The Protection of Personal Information Act, 4 of 2013 ('POPIA') requires the Company to inform Data subjects as to how their personal information is used, disclosed and destroyed.

The Company is committed to compliance with POPIA and other applicable legislation, protecting the privacy of Data subjects and ensuring that their personal information is used appropriately, transparently and securely.

This policy is made available on the Company's website www.enterprises.up.ac.za and should be read in conjunction with the Company's Website Privacy Notice, Employee Privacy notice, Delegate Privacy Notice and Job Applicant Privacy Notice.

4. DEFINITIONS

4.1. Personal Information

Personal information means information relating to an identifiable, living, natural person, and where it is applicable, an existing, identifiable juristic person and may include but is not limited to:

- 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;
- information relating to the education or the medical, financial, criminal or employment history of the person;
- any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

- the biometric information of the person;
- the personal opinions, views or preferences of the person;
- correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- information regarded as confidential business information;
- the views or opinions of another individual about the person; and
- 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.

4.2. Data subject

This refers to the natural or juristic person to whom personal information relates, such as employees, clients, delegates, sub-contractors or a company that supplies the Company with goods or services.

4.3. Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

4.4. Processing

The act or processing information includes any activity or set of operations concerning personal information and includes:

- the collection, receipt, capturing, collation, storage, updating, retrieval, alteration or use;
- dissemination by means of transmission, distribution or making available in any other form; or
- merging, linking, erasure or destruction of information.

5. RIGHTS OF DATA SUBJECTS

The Company will ensure that it makes Data subjects aware of their rights as appropriate and specifically with regards to the following:

5.1. The right to access personal information

Data subjects have the right to establish whether the Company holds personal information related to them, including the right to request access to that personal information.

5.2. The right to have personal information corrected or deleted

Data subjects also have the right to ask the Company to update, correct or delete their personal information on reasonable grounds.

5.3. The right to object to the processing of personal information

Data subjects have the right on reasonable grounds, to object to the processing of their personal information.

The Company will consider such requests and the requirements of POPIA and may cease to process such personal information and may, subject to statutory and contractual record keeping requirements, also destroy the personal information.

5.4. The right to object to direct marketing

Data subjects have the right to object to their personal information being used for the purposes of direct marketing by means of unsolicited electronic communications.

5.5. The right to complain to the Information Regulator

Data subjects have the right to submit a complaint to the Information Regulator regarding infringements of any of their rights protected under POPIA and to institute civil proceedings against alleged non-compliance with the protection of their personal information.

5.6. The right to be informed

Data subjects have the right to be informed that their personal information is being collected by the Company and should also be notified in any situation where the Company reasonably believe that the personal information of data subjects has been accessed by unauthorised person/s.

6. GENERAL GUIDING PRINCIPLES

All employees and persons acting on behalf of the Company will be subject to the following guiding principles:

6.1. Accountability

Compliance failure could damage the reputation of the company and its shareholder, the University of Pretoria. The Company could also be exposed to a civil claim for damages. The protection of personal information is therefore everybody's responsibility.

The Company will take appropriate steps including disciplinary action against individuals who through intentional or negligent actions and/or omissions fail to comply with this policy.

6.2. Processing limitation

The Company collects personal information directly from Data subjects only as pertains to business requirements. The type of information will depend on the need for which it is collected and will be processed for that purpose only. We will inform Data subjects as to what information is mandatory or deemed optional, as far as possible.

Personal information will only be used for the purpose for which it was collected, intended and as agreed. This may include:

- Registering delegates on training courses;
- Issuing certificates to delegates upon successful completion of training courses;
- Processing claims received from subcontractors;
- Issuing tax certificates to subcontractors;
- Recruitment activities;
- Recordkeeping and payment of employees;
- Administration of employment benefits;
- Recording and payment of suppliers;
- Confirming, verifying and updating client information;
- For registration purposes with statutory bodies (CIPC, SARS) and institutions (banks);
- Contractual obligations;
- In connection with legal proceedings;
- In connection with and to comply with legal and regulatory requirements or when allowed by law;
- For audit and reporting purposes; and
- Marketing activities.

According to Section 10 of POPIA, personal information may only be processed if the purpose for which it is processed, is adequate, relevant and not excessive. Certain

conditions must be met for the Company to process personal information as in Section 11 of POPIA. These are listed below:

- Data subjects consent to the processing – consent is obtained during early stages of the relationship.
- Processing is necessary – personal information is required to facilitate the provision of services to the Data subject or for the conclusion of a contract to which the Data subject is a party.
- The Company is under obligation by law.
- The legitimate interest of the Data subject is protected – it is in their best interest to provide the personal information.
- Processing is in the best interest of the Company – in order to provide our services to the Data subject.

6.3. Further processing limitation

Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose. Where the secondary purpose is not compatible with the original purpose, the Company will first obtain additional consent from the Data subject.

6.4. Information quality

The Company will take reasonable steps to ensure that all personal information is complete, accurate and not misleading. Where personal information is collected from third parties, the Company will take reasonable steps to ensure that the information is correct by verifying the accuracy of the information directly with the Data subject or by way of independent sources.

6.5. Security safeguards

Section 19 of POPIA requires the adequate protection of personal information that is held by the Company. The Company will continuously review security controls and processes to prevent unauthorised access and use of personal information.

The following procedures are in place to ensure that personal information are secure:

- This policy is available from the Company's website and Intranet;
- Employees will be trained on this policy and POPIA;
- All product marketing activities using email addresses derived from leads capturing or enrolment data, unsolicited proposals and letter campaigns must be distributed through the ClickDimensions marketing platform to ensure subscription consent compliance. Marketing mail mergers from personal individual inboxes are not allowed.
- Reputable service providers must be used for the purchase or acquisition of databases for marketing purposes. In addition, databases may only be acquired if the provider can provide certification of assurances that they have obtained permission from prospects/customers to on-sell their information and that they accept legal liability for any misrepresentation thereof.
- Redundant hardcopies of personal information are stored in locked bins until it is securely destroyed by our service provider;
- Archived personal information are destroyed according to legislative retention periods;
- The Company's internal server hard drives are protected by firewalls; and
- The backup of electronic files and data are managed and regulated through a service level agreement entered into with a reputable service provider.

7. SPECIFIC DUTIES AND RESPONSIBILITIES

7.1. Board of Directors

The Company's Board of Directors is ultimately accountable for ensuring that the Company meets its obligations under POPIA. The Board of Directors may however delegate some of its responsibilities to management or other capable individuals.

7.2. Chief Executive Officer

The Chief Executive Officer is by virtue of the position, appointed automatically as Information Officer in terms of the Promotion of Access to Information Act and POPIA and may authorise any person in the Company to act as the Information Officer of the Company. The CEO however retains the responsibility and accountability for any powers or the functions authorised to that person and has the right to amend and/or withdraw any of these powers, duties and responsibilities.

7.3. The Company's Information Officer is responsible for the following:

- Taking steps to ensure the Company's reasonable compliance to POPIA;
- Reviewing the Company's information protection procedures and policies;
- Ensuring that the Company makes it convenient for Data subjects to communicate with the Company regarding their personal information;
- Encourage compliance with the lawful processing of personal information;
- Ensure that employees and persons acting on behalf of the Company are aware of the risks associated with the processing of personal information;
- Ensure that employees are trained in the processing of personal information;
- Address employees' POPIA related questions;
- Address POPIA related requests and complaints made by the Company's Data subjects; and
- Act as contact point for the Information Regulator on issues pertaining to the processing of personal information.

7.4. The Company's Executive Manager in charge of Information Technology is responsible for:

- Ensuring that the Company's IT infrastructure and any other devices used for processing personal information meet acceptable security standards;
- Ensuring that servers containing personal information are sited in a secure location;
- Ensuring that all electronically stored information is backed-up and tested on a regular basis;
- Ensuring that all back-ups are protected from unauthorised access, accidental deletion and malicious hacking attempts;
- Ensuring that information being transferred electronically is encrypted;
- Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software;
- Performing regular IT audits to ensure that the security of the Company's hardware and software systems are functioning properly;
- Performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by unauthorised persons; and
- Performing a proper due diligence review prior to contracting with third party providers to process personal information on the Company's behalf.

7.5. The Company's Executive Manager: Stakeholder Relations is responsible for:

- Approving and maintaining the protection of personal information statements and disclaimers that are displayed on the Company's website, including those attached to communications such as emails and electronic newsletters;
- Ensuring that the Company complies with section 69 of POPIA;
- Addressing any personal information protection queries from media; and
- Work with persons acting on behalf of the company to ensure that any outsourced marketing initiatives comply with POPIA.

7.6. The Company's Executive Manager: Human Resources is responsible for:

- Ensuring that the human resource and payroll system is POPIA compliant;
- Providing assurance of good privacy practices applied in the division; and
- Authorising access rights to the human resource and payroll systems.

7.7. Employees and other persons acting on behalf of the Company are responsible for:

- Keeping all personal information that they come into contact with secure by taking precautions and complying with this policy;
- Ensuring that personal information is kept in as few places as is necessary;
- Ensuring that personal information is encrypted prior to sharing the information electronically;
- Ensuring that all devices such as computers, flash drives, etc. are password protected and never left unattended (refer to the Company's Electronic Communications policy);
- Ensure that computer screens and other devices are switched off when not in use;
- Ensure that removable storage devices such as external drives that contain personal information are locked away securely when not being used;
- Ensure that where personal information is stored on paper, that such hard copies are kept in a secure place where unauthorised persons are not able to access it;
- Ensure that where personal information has been printed out, that the printouts are not left unattended where unauthorised individuals could see them;
- Take reasonable steps to ensure that personal information is stored only for as long as it is needed or required;
- Undergo POPIA awareness training from time to time.

Employees and other persons acting on behalf of the company will under no circumstances:

- Process personal information where it is not a requirement to perform their work-related duties;
- Save copies of personal information directly to their own private computers or mobile devices; and
- Share personal information informally.

8. DATA BREACH PROCEDURE

8.1. Reporting a possible breach

Any employee who becomes aware of a possible breach of Personal Information must immediately inform their line manager and the Information Officer and/or the Deputy Information Officers.

The employee must ensure to retain any evidence they have in relation to the breach and provide a written statement setting out any relevant information relating to the suspected data breach using the Data Breach Report form (Annexure A).

Employees may not attempt to investigate the suspected breach themselves and must not notify the affected data subjects. The data breach team will investigate and assess the suspected breach and will determine who will be notified and how.

8.2. Response plan

The Company's CEO together with the Information Officer will assemble a team to investigate, manage and respond to the data breach.

The breach team will then:

4.2.1. Make an urgent preliminary assessment of what data have been lost, why and how.
4.2.2. Take immediate steps to contain the breach and recover any lost data.
4.2.3. Undertake a full and detailed assessment of the breach.
4.2.4. Record the breach in the company's data breach register.
4.2.5. Notify the Information Regulator, if necessary.
4.2.6. Notify affected data subjects, if necessary.
4.2.7. Put in place any measures to address it and to mitigate its possible adverse effects and to prevent further breaches.

9. DATA BREACH REGISTER

The company will maintain a register of all personal data breaches regardless of whether or not it is notifiable to the Information Regulator. The register will include a record of:

9.1. The facts relating to the breach including the cause, what happened and what personal data were effected;
9.2. the effects of the breach; and
9.3. the remedial actions we have taken.

10. NOTIFICATION TO THE INFORMATION REGULATOR

Not all personal data breaches have to be notified to the Information Regulator. The breach will only have to be notified if it is likely to result in a risk to the rights and freedoms of data subjects and this will be assessed by the company on a case-by-case basis.

11. NOTIFICATION TO DATA SUBJECTS

The data breach team will consider several factors in determining the notifications to individuals affected by the data breach including but not limited to:

11.1 Contractual obligations;
11.2 Risk of identity theft or fraud because of the type of information lost such as contact details, bank information or identity numbers;
11.3 Risk of physical harm;
11.4 Risk of hurt, humiliation or damage to reputation if the information includes medical or disciplinary records; and
11.5 Number of data subjects affected.

Affected individuals must be notified without unreasonable delay, unless such notification will impair a criminal investigation. Notices must be in plain language and include basic information such as what happened, type of information involved, steps being taken, steps individuals should take and contact information.

12. DISCIPLINARY ACTION

The Company may recommend appropriate legal or disciplinary action to be taken against any employee found to be implicated in any non-compliant activity outlined within this policy.

Any gross negligence or intentional mismanagement of personal information will be considered a serious form of misconduct under the Company's Disciplinary code and may lead to dismissal.

Examples of actions that may be taken subsequent to an investigation include:

- A recommendation to commence with disciplinary action
- A referral to law enforcement agencies for criminal investigation
- Recovery of funds in order to limit any damages caused.

Document data

Document number	POL_COM_004V3
Policy owner	CEO
Approval date	20/08/2021
Effective from	20/08/2021

Annexure A

DATA BREACH REPORT FORM *To be completed by the person that became aware of actual or suspected data breaches*	
Part A – Employee details	
Full name:	
Position title:	
Division:	
Phone number:	
Email:	
Part B – Incident details	
Estimated date and time of the data breach:	
Date of discovery of the data breach:	
Location of the data breach:	
Breach of personal information suspected:	
Full description of the data breach:	
How was the breach detected:	
Is the breach ongoing/current status of the breach:	
What is believed to be the cause of the breach:	
How many individuals does the data breach effect:	
What system (e.g. devices, email accounts, databases, etc.) have been affected by the breach:	
Attach any evidence of the breach (e.g. screenshots, relevant emails, etc.)	
Response actions performed:	
Report submitted to:	
Signature:	Date:
Once this form is completed it must be provided to your line manager	

Annexure B

DATA BREACH INCIDENT RESPONSE FORM *To be completed by the investigator of the incident or the Information Officer*			
INVESTIGATOR DETAILS:			
NAME		POSITION	
DATE		EMAIL	
INCIDENT INFORMATION:			
DATE/TIME OR PERIOD OF BREACH:			
DESCRIPTION AND NATURE OF BREACH:			
TYPE OF BREACH:			
CATEGORIES OF DATA SUBJECT AFFECTED:			
CATEGORIES OF PERSONAL DATA RECORDS CONCERNED:			
NUMBER OF DATA SUBJECTS AFFECTED:		NUMBER OF RECORDS INVOLVED:	
IMMEDIATE ACTION TAKEN TO CONTAIN/MITIGATE BREACH:			
STAFF INVOLVED IN BREACH:			
PROCEDURES INVOLVED IN BREACH:			
THIRD PARTIES INVOLVED IN BREACH:			
BREACH NOTIFICATIONS:			
WAS THE INFORMATION REGULATOR NOTIFIED?	YES	NO	
IF YES, WAS THIS WITHIN 72 HOURS?	YES	NO	

If no to the above, provide reason(s) for the delay		
IF APPLICABLE, WAS THE BELOW INFORMATION PROVIDED?		
A description of the nature of the person data breach	YES	NO
The categories and approximate number of data subjects affected	YES	NO
The categories and approximate number of personal data records concerned	YES	NO
The name and contact details of the Information Officer and/or any other relevant point of contact	YES	NO
A description of the likely consequences of the personal data breach	YES	NO
A description of the measures taken or proposed to be taken to address the personal data breach	YES	NO
WAS NOTIFICATION PROVIDED TO DATA SUBJECTS?	YES	NO
INVESTIGATION OUTCOME ACTIONS		
DETAILS OF ACTIONS TAKEN		
PROCEDURE/S REVISED DUE TO BREACH:		
STAFF TRAINING PROVIDED		
WILL THE MITIGATING ACTIONS PREVENT SUCH BREACH FROM HAPPENING AGAIN?		
IS APPROPRIATE TECHNICAL PROTECTION MEASURES IN PLACE? *describe measures*		
Information Officer name and signature	Date	
CEO signature	Date	