| Process Owner | Doc. Author | | | | Revision Data | |
|---|---|---|---|---|---|---|
| Group Financial Director | Jeandie Leonie | | | | Effective Date | 21/06/2021 |
| | | | | | Revision Date | - |
| Document Title | Policy and Standard Operating Procedure for Personal Information Access, Data Breach and POPIA Non-Compliance Reporting and Investigation | | | | | |
| Document No | WHL-POL-POPI 2/2021 | Controlled | Y | | Revision Number | 01 |

**Amendment History**

| Issue | Date | Amendment Details | Requested By |
|---|---|---|---|
| 01 | 21/06/2021 | New Document | Jeandie Leonie |

## 1. BACKGROUND

1.1. Workforce Holdings Limited ("the group") understands the importance of protecting the personal information it collects and processes as envisioned in the Protection of Personal Information Act 4 of 2013 ("POPIA"). As such, it has identified the procedures set out herein for:

1.1.1. The reporting and investigation of data breaches and/or any other non-compliance incidents relating to POPIA, and

1.1.2. Data Subject participation as required by POPIA.

## 2. PURPOSE OF THIS STANDARD OPERATING PROCEDURE

2.1. With the onset of technological advancements and the rapid development of digital business practices, it has become necessary to regulate the use of data in our business which falls within the ambit of the definition of personal information. This ensures that personal information of employees, clients, suppliers and other third parties are used and processed with circumspection and care. It is also necessary to give effect to Data Subject rights set out in POPIA.

2.2. The aim of this policy and procedure is to regulate the process for reporting, investigating, and resolving non-compliance with POPIA within the Workforce Holdings Limited group of companies, and to provide Data Subjects with information relating to the access of their information.

## 3. APPLICATION OF THIS STANDARD OPERATING PROCEDURE

3.1. This policy and procedure applies to all employees within the Workforce Holdings Limited group of companies, including temporary employees, independent contractors, brokers and contracted service providers. This procedure shall further apply to any Data Subject or third party whose Personal Information is processed by the Group, or who may become aware of a Data Breach or other Non-Compliance Incident which may affect the Group and/or any of its subsidiaries and operating divisions.

## 4. DEFINITIONS

4.1. "POPIA" means the Protection of Personal Information Act 4 of 2013.

4.2. "Personal Information" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

4.2.1. 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;

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

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

4.2.4. the biometric information of the person;

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

4.2.6. 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;

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

4.2.8. 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.

4.3. "Information Officer" means the Information Officer duly appointed by the Chief Executive Officer for purposes of POPIA implementation, monitoring and compliance, and registered as such with the Information Regulator.

4.4. "Deputy Information Officer" means the Deputy Information officers duly appointed by the Information Officer for purposes of POPIA implementation, monitoring and compliance within their specified business units/entities, and registered as such with the Information Regulator.

4.5. "Data subject" means the person or entity in respect of whom Personal Information is processed by the Group.

4.6. "Group" means collectively all subsidiaries and operating divisions under the Workforce Holdings Limited group of companies.

4.7. "Data breach" means the intentional or unintentional access, theft, release or compromise of Personal Information, in any form whatsoever, to or by an unauthorized person or entity, and also includes any suspected or contemplated access, theft, release or compromise.

4.8. "Non-Compliance Incident" means any act or omission which constitutes non-compliance with POPIA, other than a Data Breach as defined, and shall include a suspected or contemplated act or omission in this regard.

4.9. "Company" means a specific subsidiary or operating division of the Group.

## 5. ACCESS TO PERSONAL INFORMATION

5.1. The Group is committed to processing Personal Information in accordance with the provisions of POPIA and is bound by its Privacy Policy, which can be found on the website of Workforce Holdings Ltd and the websites of its subsidiaries and operating divisions.

5.2. Notwithstanding its compliance with its Privacy Policy, the Group recognizes that, unless refusal is legally mandated, a Data Subject has the right to:

5.2.1. request the Company to confirm, free of charge, whether or not it holds Personal Information about the Data Subject;

5.2.2. request from the Company the record or a description of the Personal Information about the Data Subject held by the Company, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information—

a. within a reasonable time;
b. at a reasonable fee;
c. in a reasonable manner and format; and
d. in a form that is generally understandable.

5.2.3. request the Company to correct or delete Personal Information about the Data Subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or

5.2.4. destroy or delete a record of Personal Information about the Data Subject that the responsible party is no longer authorised to retain.

5.3. The requests referred to in paragraph 5.2.1 and 5.2.2 above may be made in writing to the Information Officer of the Group, or the Deputy Information Officer of the Company concerned, by utilising the email addresses set out in **"Schedule 1"** hereof.

5.4. The requests referred to in paragraph 5.2.3 and 5.2.4 may be made in writing to the Information Officer of the Group, or the Deputy Information Officer of the Company concerned, by using the prescribed format in **"Schedule 2"** hereof and submitting the request to the relevant email address set out in **"Schedule 1".**

5.5. The provisions relating to the access of information contained in this policy and procedure should be read with the Group's Promotion of Access to Information Act ("PAIA") Manual, available on the website of Workforce Holdings Limited and the websites of its subsidiaries and operating divisions.

## 6. REPORTING OF DATA BREACHES AND OTHER NON-COMPLIANCE

6.1. Data Subjects and other third parties are encouraged report any Data Breach or Non-Compliance Incident immediately upon becoming aware thereof. Employees, including temporary employees, employed under any entity forming part of the Workforce Holdings group of companies, shall have a duty to do so by virtue of their contractual and common-law duty to act in the best interest of the Group.

6.2. Any uncertainty as to whether an act/omission/incident warrants reporting as contemplated in this policy, must be referred to the appointed Information Officer of the Group, and/or the Deputy Information Officer of the business entity concerned, for clarification.

6.3. The following reporting procedure will apply:

6.3.1. Data Breaches and Non-Compliance Incidents will be reported in writing to the Information Officer. The Complainant may also copy the Deputy Information Officer appointed for the Company in respect of which the complaint is lodged. The contact details of the Information Officer and Deputy Information Officers are set out in "Schedule 1" to this policy and procedure.

6.3.2. The Information Officer, in consultation with the relevant Deputy Information Officer, shall assess the complaint to determine its validity against legislative guidelines, the Data Subjects affected, the risk or potential risk of the alleged Data Breach or Non-Compliance Incident on the Company or the Group as a whole, and the best course of action in resolving the complaint.

6.3.3. Should the Information Officer and/or the Deputy Information Officer determine that the complaint carries merit and is of such a nature that widespread damage (whether financial, reputational, or otherwise) has been or may be caused, the Information Officer shall immediately refer the complaint to:

- The Group Risk and Audit Manager;
- The Chief Information Officer;
- The Managing Executive/CEO of the cluster of companies implicated/affected; and

- The Managing Director of the entity/ies implicated/affected.

6.3.4. The parties referred to in clause 6.3.3 above shall conduct a detailed investigation into the complaint lodged and shall determine the steps necessary to resolve the complaint. In this regard, the parties may determine the necessity of acquiring independent expert advisory services (such as service providers with legal or information technology expertise) and shall recommend such appointment/s to the Board of Directors.

6.3.5. Where the parties referred to in clause 6.3.3 above determine that the complaint may or has caused considerable reputational damage, the complaint shall also be referred to the Group Board of Directors and Group Marketing Manager to determine the necessity of internal and external public relations interventions, and the most suitable strategy to mitigate and minimize potential or actual reputational damage.

6.3.6. The Information Officer shall, unless specifically delegated to a Deputy Information Officer on a case-by-case basis, be responsible for following legislative reporting procedures and shall be the primary liaison with the Information Regulator where applicable.

## 7. DELEGATION OF AUTHORITY

7.1. For purposes of this policy, any designation referred to herein may delegate their duties or responsibilities to a senior director or employee in their Company or department in writing.

**"SCHEDULE 1"**

| CLUSTER/ENTITY | DESIGNATION | EMAIL ADDRESS |
|---|---|---|
| Workforce Holdings Ltd | Information Officer | popia@workforce.co.za |
| Debtworx (Pty) Ltd | Deputy Information Officer | popia@baberekiservices.co.za |
| Babereki Employee Support Services | Deputy Information Officer | popia@baberekiservices.co.za |
| Essential Employee Benefits | Deputy Information Officer | popia@baberekiservices.co.za |
| GetSavvi Group of Companies | Deputy Information Officer | popia@baberekiservices.co.za |
| Training Force (Pty) Ltd | Deputy Information Officer | popia@trainingforce.co.za |
| Prisma Training Solutions (Pty) Ltd | Deputy Information Officer | popia@trainingforce.co.za |
| KBC Health & Safety (Pty) Ltd | Deputy Information Officer | popia@trainingforce.co.za |
| The Cyber Academy | Deputy Information Officer | popia@trainingforce.co.za |
| Dyna Group of Companies | Deputy Information Officer | popia@dyna-training.co.za |
| Only the Best (Pty) Ltd | Deputy Information Officer | popia@recruitco.co.za |
| Fempower Personnel (Pty) Ltd | Information Officer | popia@recruitco.co.za |
| Accotech a division of Workforce Staffing (Pty) Ltd | Deputy Information Officer | popia@recruitco.co.za |
| OpenSource Intelligent Solutions | Deputy Information Officer | popia@recruitco.co.za |
| Programmed Process Outsourcing | Information Officer | popia@workforce.co.za |
| Workforce Staffing (Pty) Ltd | Information Officer | popia@workforce.co.za |
| Gcubed a division of Workforce Staffing (Pty) Ltd | Information Officer | popia@workforce.co.za |
| Quyn Group of Companies | Information Officer | popia@workforce.co.za |
| Worldwide Staffing (Pty) Ltd | Information Officer | popia@workforce.co.za |
| Oxyon People Solutions (Pty) Ltd | Information Officer | popia@workforce.co.za |
| Interchange Business Consulting | Information Officer | popia@workforce.co.za |
| Workforce Management Services (shared services) | Deputy Information Officer | popiainfo@workforce.co.za |
| Workforce Healthcare (Pty) Ltd | Deputy Information Officer | popia@workforcehealthcare.co.za |
| Allmed Healthcare Professionals | Deputy Information Officer | popia@allmed.co.za |
| Nursing Emergencies (Pty) Ltd | Deputy Information Officer | popia@allmed.co.za |

**"SCHEDULE 2"**

**REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013) REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018 [Regulation 3]**

*Note:*

1. *Affidavits or other documentary evidence as applicable in support of the request may be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*
3. *Complete as is applicable.*

Mark the appropriate box with an "x".

Request for:

☐ Correction or deletion of the personal information about the data subject which is in possession or under the control of the responsible party.

☐ Destroying or deletion of a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

| A | DETAILS OF THE DATA SUBJECT |
|---|---|
| Name(s) and surname / registered name of data subject: | |
| Unique identifier/ ID number: | |
| Residential, postal or business address: | _____<br>_____<br>_____<br>_____(Code) |
| Contact number(s): | |
| Fax number / email address: | |
| **B** | **DETAILS OF RESPONSIBLE PARTY** |
| Name(s) and surname / registered name of responsible party: | |
| Residential, postal or business address: | _____<br>_____<br>_____<br>_____(Code) |
| Contact number(s): | |
| Fax number / email address: | |

***PLEASE CONTINUE WITH SECTIONS "C" AND "D" ON THE NEXT PAGE***

| C | INFORMATION TO BE CORRECTED/ DELETED/ DESTROYED |
|---|---|
| | |

| D | REASON FOR CORRECTION/ DELETION/DESTRUCTION *(Please provide detailed reasons)* |
|---|---|
| | |

**SIGNED AT _____ON THIS _____DAY OF 20_____**

_____

**DATA SUBJECT**

## 8. REVIEW

This policy will be reviewed annually to ensure it meets the objectives of the relevant legislation and remain effective for the Group and may be changed at any time at the discretion of the Board of Directors.