



Whistle-blowing Policy

September 2023

VERSION 5.0

A handwritten signature in black ink, consisting of stylized, cursive letters.

Document review and approval

Revision history

Version	Author	Date	Purpose
1.0	Internal Audit	December, 2012	To establish whistleblowing policy for DCP
2.0	Internal Audit	June, 2015	To reflect the changes in the regulatory requirement and leading practice.
3.0	Internal Audit	March, 2019	To reflect the changes in the regulatory requirement and leading practice.
4.0	Internal Audit	April 2021	To reflect the changes in the regulatory requirement and leading practice.
5.0	Internal Audit	September 2023	To reflect general update in the policy

This document has been reviewed by

S/N	Reviewer	Name	Signature	Date Reviewed
1	Group Chief Internal Auditor	Mr. Jonathan Ogiku		21 Sept, 2023

This document has been approved by

S/N	Designation	Name	Signature	Date reviewed
1	Group MD/CEO, DCP	Mr. Arvind Pathak		29/9/23
2	BARCC Chairman, DCP	Mr. Ernest Ebi		09/11/23
3	Chairman, Board of Directors, DCP	Alhaji Aliko Dangote		14/11/23

Table of Contents

1	Introduction	5
1.1	Policy Statement.....	5
1.2	Objective.....	5
1.3	Applicability	5
1.4	Review	5
1.5	Related Policies.....	5
2	Scope.....	5
2.1	Definition of Terms.....	6
2.2	Importance of Whistle-blowing	8
2.3	Confidentiality	8
2.4	Outsourced Whistle-blowing Platform Managed by Deloitte.....	8
2.5	Whistle- blower Identity Options.....	9
2.6	Subsequent Action.....	9
2.7	Feedback to Whistle-blower.....	10
2.8	Reporting a Whistle-blowing Concern	10
2.8.1	Obligations of the Whistle-Blower	10
2.8.2	Information Required from the Whistle-blower.....	11
2.9	Procedures for Receiving and Investigating Reports	12
3	Protection of Whistle-blowers	12
4	Documentation and Record Keeping	13
5	Responsibility for this Policy.....	13
5.1	The Board	13
5.2	The Anti-Fraud Committee	13
5.3	Group Chief Internal Auditor	13
5.4	Heads of Departments.....	14
5.5	Group Managing Director.....	14
6	Compliance Confirmation.....	15
	APPENDIX I	16
	APPENDIX II	17
	APPENDIX III	18



Glossary of terms

Abbreviation	Meaning
ACFE	Association of Certified Fraud Examiners
AFC	Anti-Fraud Committee
BARCC	Board Audit Risk and Compliance Committee
Board/ BOD	Board of Directors
Chairman	Chairman, BOD
DCP	Dangote Cement PLC
GCFO	Group Chief Financial Officer
GCIA	Group Chief Internal Auditor
GCLCS	Group Chief Legal Counsel and Cooperate Services
GCRO	Group Chief Risk Officer
GMD/CEO	Group Managing Director/ Chief Executive Officer
HOD	Heads of Department
HRD	Human Resources Department
this Policy	Whistle-blowing policy



1 Introduction

1.1 Policy Statement

The Board and Management of Dangote Cement PLC (“DCP”) believe strongly in proactively preventing fraud as well as implementing effective controls to detect and respond to fraudulent activities and misconduct. To this extent, Board and Management have adopted a whistle-blowing policy (“this Policy”).

This Policy is established with the aim of providing acceptable channels to stakeholders to raise concerns about suspected or actual breaches of DCP’s policies and values, without fear of being victimized and with the reassurance that whistle-blower complaints will be treated with utmost confidentiality.

1.2 Objective

This Policy aims to:

1. Create a work environment conducive for employees and other stakeholders to confidentially and anonymously report suspected or actual breaches of DCP’s policies to designated recipients for investigation and other appropriate actions, as soon as possible.
2. Reassure whistle-blowers that:
 - a. They can report any concerns without fear of reprisals, even if their concerns turn out to be erroneous.
 - b. Reported concerns will be taken seriously, investigated, and appropriate action will be taken.
 - c. They will be protected from victimisation for disclosing concerns in accordance with the procedures defined herein, and in other relevant policies.
 - d. Any instance of victimisation will be taken seriously and addressed accordingly.
3. Facilitate a culture of openness, accountability and integrity in DCP.
4. To provide whistle-blowers with guidance on the reporting channels available to them.

1.3 Applicability

This Policy applies to all employees, directors, customers, distributors, service providers, transporters, creditors, debtors, drivers, contractors, masons, builders, shareholders and other stakeholders of DCP. The Policy is effective from the date it is signed by the Chairman, Board of Directors of DCP.

1.4 Review

This Policy will be reviewed every three (3) years and/or as soon as there are changes in regulatory requirements, trends or leading practice. This is to ensure that the provisions of this Policy continue to fulfil its objectives, DCP’s legal obligations and to reflect leading practice.

1.5 Related Policies

This Policy should be read in conjunction with other policies of DCP, particularly the Employee Handbook. Other whistle-blowing related issues not specifically addressed in this Policy will be dealt with, according to the principles and intents of this Policy.

2 Scope

DCP is committed to high standards of ethical, moral and legal business conduct. Consequently, we have developed this Policy in line with the SEC Code of Corporate Governance Section 32, which

provides that companies should have a whistle-blowing policy that is transparent to all stakeholders, as well as principle 19 of the Nigerian Code of Corporate Governance 2018, which provides that organisations should develop an effective whistle-blowing framework for reporting any illegal or unethical behaviour which minimises the Company's exposure and prevents recurrence.

This Policy serves as a useful guideline in identifying reportable activities and misconduct such as fraud, assets misappropriation, fraudulent financial statements, harassment and bullying, which can have debilitating effects on corporate performance, reputation and wellbeing of employees.

If an employee is uncertain as to whether a particular conduct is within the scope of this Policy, he/she should approach any member of Internal Audit.

2.1 Definition of Terms

Asset Misappropriation: Asset Misappropriation refers to the misuse of DCP assets. Some examples of asset misappropriation include the following:

- Skimming (theft of cash that has not yet been recorded in the accounting system) and cash larceny (theft of money that has been recorded in the accounting system).
- False invoicing via shell companies, false invoicing via non-accomplice vendors and personal purchases made with DCP funds.
- Falsification of amount of sales made by a salesperson in order to earn more commission.
- Theft or wilful destruction or loss of assets e.g. inventory (by employees or transporters).
- Purchase of goods at inflated prices.
- Theft or misuse of non-cash assets, including supplies, fixed assets, etc.
- Disclosing confidential and/or proprietary information to third party without authorisation.
- Insider trading.
- Override of controls.
- Purchase of inferior goods.

Breach: A breach is an act of breaking or failing to observe a law, agreement, or code of conduct with regards to DCP.

Corruption: It is the wrongful use of influence to obtain a benefit for oneself or another person, contrary to the duty or rights of others. It consists of, but is not limited to the following:

- Inappropriate relationships with third parties thereby causing conflict of interest.
- Bribery, where someone is influenced by payment or benefit in kind to unreasonably provide advantage to another through his or her position.
- Facilitation payments.
- Giving or receiving kickbacks from vendors, transporters, customers, distributors, other service providers, among others.
- Abuse of office on the part of any member of staff or director.
- Illegal gratuities.

Deloitte TOA: Deloitte Tip-Offs Anonymous

Fraud: According to the Association of Certified Fraud Examiners ("ACFE"), Fraud refers to any intentional act committed to secure unlawful or unfair gain. It can occur internally or externally i.e. by employees or third parties and can be perpetrated by an individual or through collusion with others. An act will be categorized as fraud if the act has the following characteristics:



- Intent;
- Direct or indirect benefit;
- Loss suffered by the victim;
- Attempt to conceal the act.

Occupational fraud refers to the intentional use of one's role in DCP to directly or indirectly gain an unlawful advantage. According to Association of Certified Fraud Examiners (ACFE), occupational fraud is classified as follows:

- Corruption
- Asset Misappropriation
- Financial Statements Misstatement
- Misconduct

Financial Statements Misstatement: It is the deliberate misrepresentation of the financial condition of DCP through the intentional misstatement, inclusion or omission of information, in order to mislead users of the financial statements. The following are examples of financial statement misstatements:

- Intentional misstatement or omission of material information in DCP'S financial reports.
- Recording fictitious revenues.
- Timing differences fraud e.g. channel stuffing to record higher sales or meet targets.
- Concealing liabilities and expenses.
- Improper assets valuation.
- Improper disclosures.

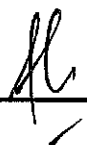
Good Faith: This is evident when a report or concern is made without malice or consideration of personal benefit and the employee has a reasonable basis to believe that the report is true; provided, however, a report does not have to be proven to be true to be made in good faith. Good faith is lacking when the disclosure is known to be malicious or false.

Misconduct: Misconduct refers to any unethical or unlawful conduct in violation of DCP's policies, procedures, code of conduct or values. The following are examples of misconduct:

- Breach of any of DCP's internal policies and procedures.
- Forgery (use of fake certificates, false declaration of age, etc.).
- Conduct that is likely to damage DCP's reputation.
- Sexual or physical abuse/harassment.
- The deliberate concealment of any malpractice.
- Miscarriage of Justice.

Stakeholder: A stakeholder is a party that has an interest in a company and can either affect or be affected by the business. Stakeholders include:

- Employees
- Representatives/Agents
- Managers
- Directors
- Consultants
- Vendors
- Regulators
- Investors



- Customers
- Suppliers

Whistle-blowing: Whistle-blowing is the disclosure of any information which, in the reasonable belief of the person making the disclosure, relates to suspected fraud, misconduct and unethical or illegal behaviour.

Whistle-blower: A whistle-blower is any person or entity making a confidential report about suspected or actual fraud, misconduct and unethical or illegal behaviour. A whistle-blower includes DCP's stakeholders such as employees, directors, customers, distributors, service providers, transporters, creditors, debtors, drivers, contractors, masons, builders, shareholders etc.

2.2 Importance of Whistle-blowing

According to the 2020 Report to the Nations, published by the ACFE, a typical organisation loses 5% of its revenue each year to fraud. Tips (whistle-blowing) accounted for 43% of frauds detected in organisations, compared to 15% detected by Internal Audit and 12% by management review.

The report also revealed that organisations with effective whistle-blowing platforms:

- Are much more likely to detect fraud by a tip.
- Experienced frauds that were 50% less costly.
- Detected frauds 50% more quickly.

Therefore, DCP encourages all employees and other stakeholders to report any cases of suspected or actual fraud and misconduct, by making use of the available whistle-blowing mechanisms.

2.3 Confidentiality

Every effort will be made to treat the whistle-blower's identity with appropriate regard for confidentiality. When a complaint is made through the DCP WB Dedicated Line (which would be managed by an independent party, Deloitte), the complaint is given a reference number which is a unique identifier for the complaint and will need to be quoted to make a follow up or when seeking feedback on a reported case. Deloitte will send an incident report of the complaint to the appropriate management level personnel of DCP within 24 hours or as soon as possible.

All concerns/complaints reported via the Deloitte TOA reporting channels (phone calls, emails, web-portal, Mobile App) will be sent confidentially and anonymously to appropriate recipients within DCP. These recipients will be independent of the allegation and will have powers in their personal capacity to ensure the concerns are addressed. Deloitte TOA will always send concerns/complaints reported to at least two (2) recipients. Please note that the identity of the whistle-blower will not be disclosed to DCP, except the Whistle-blower chooses the confidential disclosure option of anonymity.

2.4 Outsourced Whistle-blowing Platform Managed by Deloitte

To assure all DCP stakeholders of the confidentiality and anonymity of reported concerns, DCP maintains an outsourced whistle-blowing service managed by an independent party, Deloitte. This platform is provided by Deloitte for raising concerns, and it is branded as Deloitte Tip-Offs Anonymous

(TOA). All whistle-blowing reports should be made using any of the Deloitte TOA reporting channels (see Appendix I).

Before making a tip-off (report of alleged misconduct), it is important to obtain as much relevant information as possible, as the whistle-blower would be requested to provide relevant information (see Appendix I).

2.5 Whistle- blower Identity Options

There are three (3) options to choose from in protecting your identity as a whistle-blower. This comprises: Completely Anonymous, Partially Anonymous and Full/Confidential Disclosure. Deloitte encourages whistle-blowers to select either options of 'partially anonymous' or 'full/ confidential disclosure', in order to afford DCP sufficient information to better handle your concern. All whistle-blower reports are handled confidentially.

- **Completely Anonymous**

A whistle-blower who selects the completely anonymous option, will not be required to supply his/her name or any information that might reveal the whistle-blower's identity. Consequently, the details of the whistle-blower is unknown to either Deloitte or DCP. However, Deloitte TOA will be unable to contact the whistle-blower for more information on behalf of DCP, if further information about the whistle-blower's reported concern is required.

- **Partially Anonymous**

A whistle-blower who selects the partially anonymous option, will be required to disclose his/her personal details to Deloitte only. Deloitte Tip-offs Anonymous contact centre manages this reporting facility. The whistle-blower's personal details would not be divulged to DCP. If further information about the whistle-blower reported concern is required, the Deloitte Tip-offs Anonymous contact centre will contact the whistle-blower.

- **Confidential Disclosure**

A whistle-blower who selects the confidential disclosure option, will be required to disclose his/her personal details to Deloitte and DCP. The whistle-blower's name and contact details would be known to the Deloitte Tip-offs Anonymous contact centre, DCP and the investigators that will conduct the investigation.

2.6 Subsequent Action

Upon receipt of a report via any of the TOA reporting channels, Deloitte transmits the report to the designated recipient within DCP (see Appendix III) for investigation to be conducted. Deloitte will send each TOA report to designated recipients usually within 24 hours of receiving an incident reported by a stakeholder.

Public holidays, weekends and events/circumstances beyond the control of Deloitte (such as strikes, riots and other force majeure) are excluded from the 24 hours timeline within which reports are required to be submitted to DCP.



2.7 Feedback to Whistle-blower

Feedback will be provided by DCP to Deloitte TOA after investigation and subsequently transmitted to the whistle-blower through the initial channel of submission, upon the request of the Whistle-blower (see Appendix II).

Deloitte would immediately acknowledge receipt of any reported concern by a whistle-blower. However, feedback on the outcome of any reported concern would be dependent on DCP's time to completion of its internal investigations.

2.8 Reporting a Whistle-blowing Concern

Employees and other stakeholders are enjoined to report incidents of suspected or actual fraud and misconduct to DCP in a confidential and anonymous manner through the internal reporting channels and Deloitte Tip-Offs Anonymous (TOA). The earlier a concern is reported, the more efficient it is to investigate and take prompt action. Delay may cause substantial loss and reputational damage to DCP. Therefore, as soon as a whistle-blower becomes aware of suspected or actual fraud or misconduct the whistle-blower should report through the reporting channels mentioned below.

Reported concerns may be difficult to investigate if the whistle-blowers do not provide sufficient information, we therefore encourage all whistle-blowers to provide detailed information that will facilitate efficient and effective investigation. Such information should include, but are not limited to the following:

- Background and nature of the incident
- Parties involved.
- Date(s) of incident.
- Place of occurrence.
- How the incident occurred.
- Any other useful information.

However, lack of complete information about an incident should not discourage potential whistle-blowers from "blowing the whistle".

2.8.1 Obligations of the Whistle-Blower

In making whistle-blowing reports, the whistle-blower is obligated to ensure that:

- the report is made in good faith;
- he or she has reasonable ground to believe that the report is true. The whistle-blower is encouraged to report even if he or she does not have all the relevant information;
- he or she is not making the report for personal gain;
- reports should be made timely;
- although the whistle-blower shall not be expected to prove the truth of an allegation, he/she shall need to demonstrate that there are sufficient grounds for the concern;
- any employee or director who makes a report in bad faith is subject to discipline, including termination of board appointment or employee status, or other legal means to protect the reputation and brand of DCP and members of its Board and employee; and
- disciplinary/legal action will be taken against anyone deliberately raising false and malicious allegations against DCP.

It shall be the policy of DCP to protect whistle-blowers who disclose concerns, provided the disclosure is made;

- in the reasonable belief that that it is intended to show malpractice or impropriety;
- to an appropriate person or authority; and
- in good faith without malice or mischief.

DCP shall consider the following in dealing with anonymous disclosure:

- seriousness of the issues being reported;
- the significance and credibility of the concern; and
- the possibility of confirming the allegation.

Directors, executive management and/or employees who acted in good faith by reporting violation of DCP Employee Handbook and/or other policies, processes and procedures shall not suffer any form of harassment, retaliation or adverse employment consequence. Anyone who retaliates against the whistle-blower (who reported an event in good faith) will be subject to discipline, including termination of board appointment or employee status.

The whistle-blower shall receive no retaliation or reprisal for a report that was provided in good faith even if the report turns out to be wrong i.e. that was not done primarily with malice to damage another or the Corporation.

Employees of DCP are prohibited from supplying any information regarding internal impropriety to the media, outside the procedure set out in this policy.

2.8.2 Information Required from the Whistle-blower

A whistle-blower is encouraged to provide as much information as possible regarding the matter in a clear and concise manner to facilitate adequate investigation, resolution and closure. Whistle-blowers shall be asked to identify themselves as the need may arise for further contact, clarification or information. However, whistle-blowers have the right to refuse such request.

The whistle-blowing process may be initiated based on suspicion, and whistle-blowers are not expected to prove the truth of an allegation. However, individuals making reports must prove that there are sufficient grounds for concern. Consequently, whistle-blowers will be required to provide a description of the matter, information about those involved, supporting evidence and information about witnesses, where applicable.

Examples of information that may be required include but are not limited to:

- Details pertaining to the known or suspected wrongdoing;
- Details about when, where and how it occurred;
- Names of those suspected of being involved (within DCP or external);
- Names of persons who may have relevant information;
- Details of how the whistle-blower came to know about the suspected activities;
- Estimated value of the loss to DCP or other parties (if known);
- The breaches of internal controls, policy, procedure or other requirements that are believed to have taken place;
- Any recommendations for actions; and
- Names of persons the whistle-blower had previously discussed or reported this incident to (where applicable).

In a case where a whistle-blower requests complete anonymity, such shall be respected by DCP. However, it is important for the reporting party to note that it may be difficult to investigate the issues disclosed under the completely anonymous option. There may be cases where follow-up calls/reports are required, and such may not be possible to obtain from the whistle-blower.

Whistle-blowers who reveal their identity in the course of disclosure are assured of the strictest confidentiality of such information. Individuals making reports should also endeavour to disclose their involvement in any raised concern from the outset.

If a whistle-blower is involved in any wrongdoing and has elected to make such disclosure via any of the whistle-blowing channels, such disclosure shall not preclude the whistle-blower from being investigated.

2.9 Procedures for Receiving and Investigating Reports

Once a concern has been reported through the Deloitte TOA, the GCIA will arrange to have a preliminary investigation to determine whether the claim is credible and/or warrants further investigation. The GMD/BARCC Chairman will oversee the preliminary investigations of complaints against the GCIA.

In the event that a preliminary investigation determines that the services of an external investigator is required, DCP may appoint an external investigator. The investigator may proffer recommendations to minimise the risk of the re-occurrence of the investigated incidents.

Where a report is not made anonymously, DCP will inform the whistle-blower of the outcome of its preliminary investigation, and the whistle-blower may be required to provide further information. In the event of an anonymous report, the whistle-blower will be provided an update when he/she requests for feedback.

The GCIA will be charged with reviewing all reported cases through the established whistle-blowing channels and initiating appropriate action except reports against him/her which should be sent to the GMD/CEO and the BARCC Chairman.

If any crime has been committed against any person or property, DCP reserves the right to report these to the appropriate law enforcement authority without delay.

Where an allegation or report against a director or employee of DCP is substantiated, such person will be subject to disciplinary action. Such disciplinary action may include summary dismissal or other legal means necessary to protect the reputation of DCP, members of the Board, employees and shareholders of DCP. (Please refer to DCP's Employee Handbook).

3 Protection of Whistle-blowers

It is understandable that whistle-blowers are sometimes worried about possible repercussions of whistle-blowing. To this end, DCP aims to encourage openness and will support members of staff who report concerns under this Policy, even if they turn out to be erroneous.

Whistle-blowers will not suffer any detrimental treatment as a result of reporting a concern. Detrimental treatment includes dismissal, disciplinary action, threats, denial of promotions, pay rise, trainings, secondment, or other unfavourable treatment connected with reporting a concern.

Any individual who suffers any retaliation as a result of whistle-blowing, should report formally to the Board, GMD, GCIA and the DCP WB Dedicated Line.



Members of staff must not threaten or retaliate against whistle-blowers in any way. In the event that such whistle-blower feels or is victimised, DCP shall be obligated to employ appropriate tools to offer redress to the whistle-blower concerned, following the necessary investigation of such victimisation. Anyone involved in such conduct will be subject to disciplinary action which may lead to their summary dismissal.

4 Documentation and Record Keeping

The GCIA will maintain a strictly confidential register containing all whistle-blowing reports that are brought to DCP's attention and submit a summary whistle-blowing report to the Board on a quarterly basis. The report will contain the following:

- Summary of the reported cases.
- Investigation status.
- Procedures performed in investigating cases.
- Recommended process improvements.
- Actions taken as a result of the investigations.

5 Responsibility for this Policy

5.1 The Board

The Board has overall responsibility for this Policy, and for reviewing the effectiveness of actions taken in response to concerns reported under this Policy. The Board is also to ensure that this Policy is implemented, enforced and updated as required, and that the appropriate mechanisms for reporting suspected or actual breaches of DCP's policies are established.

In addition, the Board is required to continually reaffirm its support for and commitment to the Whistleblowing mechanisms.

5.2 The Anti-Fraud Committee

The members of the Anti-Fraud Committee ("AFC") are as follows:

- 1) GMD/CEO (Chairman)
- 2) GCIA (Secretary)
- 3) GCFO
- 4) GCLCS
- 5) GCHRO
- 6) GCRO

The AFC is responsible for the following:

- Implementing this Policy.
- Decisions on disciplinary actions to be taken based on the outcome of investigations.
- Provision of regular updates to the BARCC on all whistleblowing activities including status of ongoing investigations, outcome of closed investigations, and remedial actions taken.
- The review of this Policy.

5.3 Group Chief Internal Auditor

The GCIA is responsible for ensuring the following:



- The investigation of all reported incidents of suspected or actual fraud or misconduct. Certain investigations will be outsourced to a professional service firm if a potential conflict of interest exists in conducting the investigations internally or if the individuals involved in the allegations/whistlesblown occupy sensitive positions.
- Recommending remedial actions in line with DCP's Employee Handbook.
- Providing the Board with a summary of reported investigated cases, the process of investigation and the result of the investigation, on a quarterly basis.
- Conducting awareness sessions.

5.4 Heads of Departments

All HOD's are required to communicate the existence and contents of this Policy to all employees of their department. This policy is available on DCP's website as a "Read Only" document for all employees and other stakeholders to access.

HOD's dealing with parties who are not employees of DCP, such as contractors, vendors, etc., should ensure that the relevant contents of this Policy are communicated to the parties.

5.5 Group Managing Director

The GMD is responsible for ensuring that all new employees of DCP are made aware of the provisions of this Policy, and a statement in this regard should be periodically submitted to the GCLCS.



6 Compliance Confirmation

This is to confirm that I, have received, read and understood my copy of the DCP Whistle-blowing Policy document on this day.....

I hereby also confirm my compliance with the provisions of the policy.

Staff No:

Company Location:

Signature:

Date:

Please return this page to Human Resources Department.



APPENDIX I

Procedure for using Deloitte Tip-Offs Anonymous

How it Works:

Whistle-blowing reports should be made using any of the Deloitte TOA reporting channels listed below.

- Toll free hotline: 0800-TIP-OFFS (0800-847-6337).
- Web Portal: <https://tip-offs.deloittemanagedsolutions.com.ng/>
- E-mail: tip-offs@deloitte.com.ng
- Mobile App: Download Deloitte Tip-offs Anonymous App on Android or iOS devices.

Step 1:

Whistle-blower contacts Deloitte Tip-offs Anonymous contact centre via the toll-free hotline (Calls are toll free to all networks). Dial the hotline from any telephone of your choice. You may call anonymously – even if you disclose your name, your identity will remain confidential and will not be disclosed to DCP except with your consent.

Step 2:

Our contact centre agent provides options of anonymity, prompts questions and provides a unique reference number to the whistle-blower. The contact centre agent interviews the whistle-blower to obtain as much relevant information as possible. Ensure you provide all the available details:

- a. Nature of the incident
- b. People involved
- c. Dates of incident
- d. Place of occurrence
- e. How the incident occurred
- f. Any other useful information

Step 3:

Report analyst sanitizes report to remove any details that might identify the whistle-blower.

You will be assigned a unique reference code (PIN) – keep this confidential as you will need this number if you make a follow up. You may call back for feedback on your report or to provide additional information

Step 4:

The information received is captured into a TOA report format, the report is reviewed by the contact centre manager and transmitted to designated persons within DCP for further action.

Step 5:

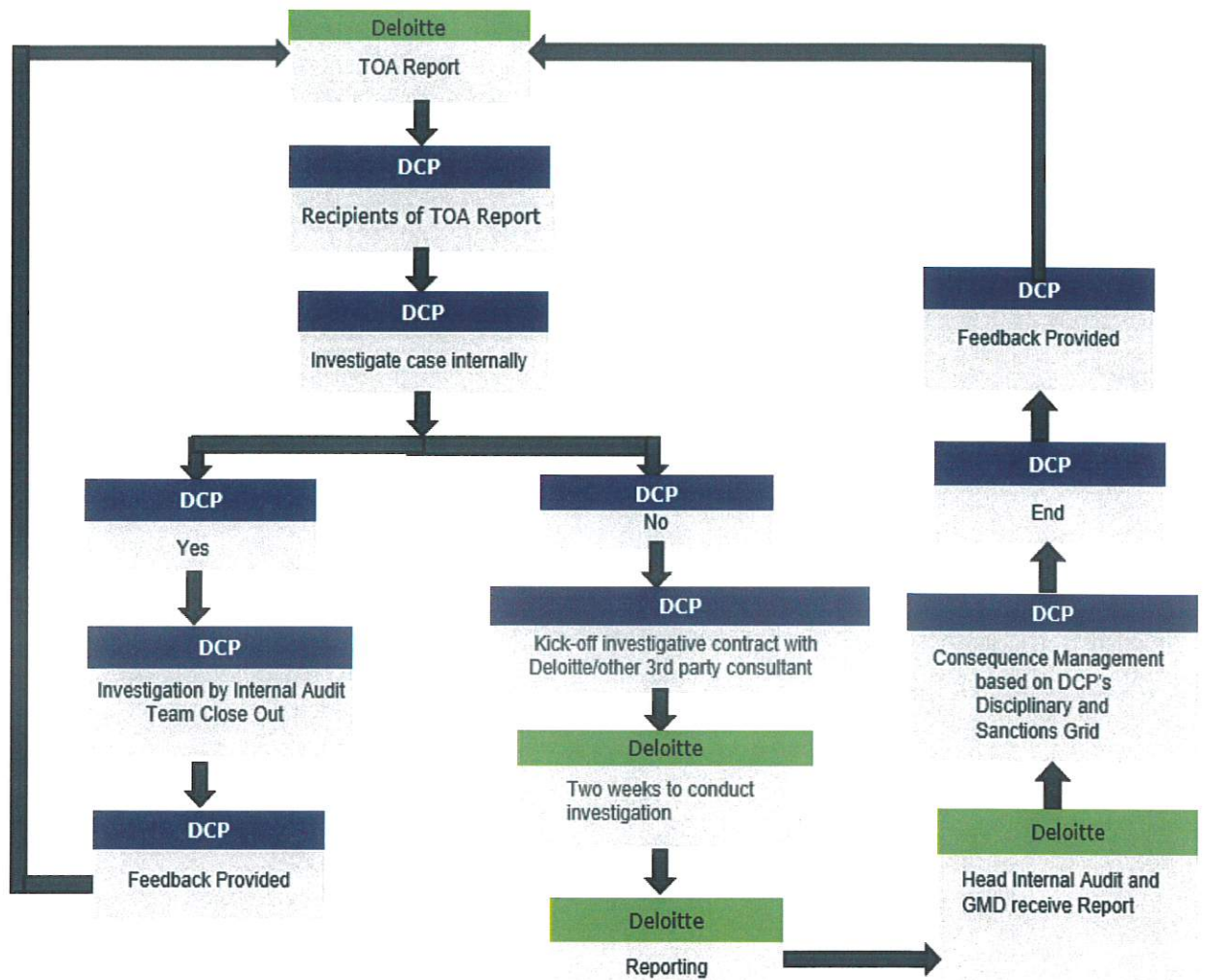
Investigation is conducted and feedback provided by DCP to Deloitte.

Step 6:

The Whistle-blower may subsequently call back to provide additional information or request for feedback.



APPENDIX II



APENDIX III

TOA Report Matrix

S/N	Type of Incident	Proposed Recipients for DCP	Name	E-Mail Address	Telephone No.
1	All forms of financial malpractices or impropriety such as fraud, corruption, bribery, and extortion	Group MD/CEO	Mr. Arvind Pathak	Arvind.Pathak@ Dangote.com	0808 594 5547
		Acting Group Chief Legal Officer (GCLO)	Mr. Edward Imoedemhe	Edward.Imoedemhe@ Dangote.com	0815 089 2300
		Group Chief Internal Audit (GCIA)	Mr. Jonathan Ogiku	Jonathan.ogiku@ Dangote.com	0705 350 0780
		Group Chief Risk Officer (GCRO)	Dr. Adenike Fajemirokun	Adenike.fajemirokun@ Dangote.com	0807 049 3841
		Acting Group Chief Financial Officer. (GCFO)	Mr. Gbenga Fapohunda	Gbenga.fapohunda@ Dangote.com	0903 000 5656
2	HR-related matters (e.g., sexual harassment, conflict of interest, other employment, political activities, alcohol & drug abuse, certificate forgery, etc.)	Group MD/CEO	Mr. Arvind Pathak	Arvind.Pathak@ Dangote.com	0808 594 5547
		Group Chief Internal Audit (GCIA)	Mr. Jonathan Ogiku	Jonathan.ogiku@ Dangote.com	0705 350 0780
		Group Chief Human Resources Officer (GCHRO)	Mrs. Gloria Byamugisha	Gloria.byamugisha@ Dangote.com	0812 946 7068
		Acting Group Chief Financial Officer. (GCFO)	Mr. Gbenga Fapohunda	Gbenga.fapohunda@ Dangote.com	0903 000 5656
3	Breach of the Code of Conduct and Business Principles	Group MD/CEO	Mr. Arvind Pathak	Arvind.Pathak@ Dangote.com	0808 594 5547
		Acting Group Chief Legal Officer (GCLO)	Mr. Edward Imoedemhe	Edward.Imoedemhe@ Dangote.com	0815 089 2300
		Group Chief Internal Audit (GCIA)	Mr. Jonathan Ogiku	Jonathan.ogiku@ Dangote.com	0705 350 0780
		Group Chief Risk Officer (GCRO)	Dr. Adenike Fajemirokun	Adenike.fajemirokun@ Dangote.com	0807 049 3841
		Acting Group Chief Financial Officer. (GCFO)	Mr. Gbenga Fapohunda	Gbenga.fapohunda@ Dangote.com	0903 000 5656
4	Theft of company asset, Sabotage or vandalism of the company asset	Group MD/CEO	Mr. Arvind Pathak	Arvind.Pathak@ Dangote.com	0808 594 5547
		Acting Group Chief Legal Officer (GCLO)	Mr. Edward Imoedemhe	Edward.Imoedemhe@ Dangote.com	0815 089 2300
		Group Chief Internal Audit (GCIA)	Mr. Jonathan Ogiku	Jonathan.ogiku@ Dangote.com	0705 350 0780
		Group Chief Human Resources Officer (GCHRO)	Mrs. Gloria Byamugisha	Gloria.byamugisha@ Dangote.com	0812 946 7068
		Group Chief Risk Officer (GCRO)	Dr. Adenike Fajemirokun	Adenike.fajemirokun@ Dangote.com	0807 049 3841
5	Any other type of unethical conduct	Group MD/CEO	Mr. Arvind Pathak	Arvind.Pathak@ Dangote.com	0808 594 5547
		Acting Group Chief Legal Officer (GCLO)	Mr. Edward Imoedemhe	Edward.Imoedemhe@ Dangote.com	0815 089 2300
		Group Chief Internal Audit (GCIA)	Mr. Jonathan Ogiku	Jonathan.ogiku@ Dangote.com	0705 350 0780
		Group Chief Human Resources Officer (GCHRO)	Mrs. Gloria Byamugisha	Gloria.byamugisha@ Dangote.com	0812 946 7068
		Group Chief Risk Officer (GCRO)	Dr. Adenike Fajemirokun	Adenike.fajemirokun@ Dangote.com	0807 049 3841
6	Reports against Directors & Executives (other than the Managing Director) irrespective of the type of incident	Chairman, Board of Directors	Alhaji Aliko Dangote	Aliko.dangote@ Dangote.com	0807 049 0000
		Group MD/CEO	Mr. Arvind Pathak	Arvind.Pathak@ Dangote.com	0808 594 5547
7	Reports against the Managing Director irrespective of the type of incident	Chairman, Board of Directors	Alhaji Aliko Dangote	Aliko.dangote@ Dangote.com	0807 049 0000
		Chairman, BARCC	Mr. Ernest Ebi	Ernest.ebi@ Dangote.com	0803 404 4400
8	Monthly Summary Reports	Group MD/CEO	Mr. Arvind Pathak	Arvind.Pathak@ Dangote.com	0808 594 5547
		Acting Group Chief Legal Officer (GCLO)	Mr. Edward Imoedemhe	Edward.Imoedemhe@ Dangote.com	0815 089 2300
		Group Chief Internal Audit (GCIA)	Mr. Jonathan Ogiku	Jonathan.ogiku@ Dangote.com	0705 350 0780
		Group Chief Human Resources Officer (GCHRO)	Mrs. Gloria Byamugisha	Gloria.byamugisha@ Dangote.com	0812 946 7068
		Group Chief Risk Officer (GCRO)	Dr. Adenike Fajemirokun	Adenike.fajemirokun@ Dangote.com	0807 049 3841
		Acting Group Chief Financial Officer. (GCFO)	Mr. Gbenga Fapohunda	Gbenga.fapohunda@ Dangote.com	0903 000 5656