Nation Media Group
Media of Africa for Africa

NATION MEDIA GROUP PLC

WHISTLEBLOWING POLICY AND PROCEDURES

March 2021

Version 1.0

Contents

1. Preamble

The Code of Corporate Governance Practices for Issuers of Securities to the Public (2015) issued by the Capital Markets Authority of Kenya, requires every listed company to establish a whistleblower policy for employees, directors and such other stakeholders to report genuine concerns in such manner as may be prescribed in that policy.

In addition to that requirement, the Board of Directors of Nation Media Group PLC (hereinafter 'the company') wishes to maintain the highest standards of business conduct and ethical behaviour.

The company has embedded the opportunity to file a complaint in its Code of Ethics and Business Conduct, but wishes to buttress this with a formal method by which employees, directors and stakeholders are encouraged to report any breach (as defined hereunder) without being worried of any retaliation, punishment or unfair treatment.

This document explains the company's Whistleblower Policy and Procedure to support its employees, directors and third parties in expressing their concerns about suspected serious misbehavior at, or related to, the activities of company and its subsidiaries (hereinafter the "policy").

This policy should be read together with all the applicable laws as stated in appendix 1 to this policy and or any others as may be enacted or changed from time to time.

2. Definitions

The definitions of some of the key terms used in this policy are given below:

"Authorised Receiver" – means the external body, organisation or company to whom whistleblowers shall make reports of a breach under this policy and shall provide liaison and communication with anonymous whistleblowers.

"Audit Risk and Compliance Committee" – means the committee of the Board constituted under section 769(1) of the Companies Act 2015.

"Board" – means the Board of Directors of the company.

"Breach" or "**Improper Conduct**" -- is a violation or the suspicion of a violation on reasonable grounds of any legislation and/or the company's Code of Ethics and Business Conduct by any company director, employee, contractor, agent or distributor operating on behalf of the company or commissioned by the company.

"Directors" – all persons holding the position of Director in the company, whether independent, non-independent, or executive.

"Employees" -- means all persons engaged by the company on a contract of service irrespective of the duration of that engagement.

"Ethics Committee" -- means the committee formed to evaluate, consider and investigate the protected disclosures received from a whistleblower under this policy.

''Interested Party''-- A party with an interest in the matter and who is not unbiased or connected so as to remain unaffected, regardless of the outcome.

"Protected Disclosure" -- means a written or oral communication, whether by letter/ email/ or over telephone relating to any breach or improper conduct, unethical practice or behaviour or violation of the Code of Ethics and business conduct by directors, employees or contractors made in good faith by the whistleblower.

"Removed" -- means that the personal data are completely deleted or adapted in such a way that identification of the person involved is no longer possible.

"Report" -- means a complaint by a whistleblower of a breach under this policy.

"Subject" -- means a person or group of persons against or in relation to whom a protected disclosure is made or evidence gathered during the course of an investigation.

"Whistleblower" -- means the person or persons making the disclosure under this policy whether a director, employee or third party.

3. Policy objectives

This policy describes what a person should do when he/she suspects or observes a breach. Third parties also can report under this procedure, using the provided links on the company's corporate website www.nationmedia.com or the external receivers designated as such in this policy.

The Board of Directors ("the Board") of the company is committed to achieving and maintaining the highest standard of work ethics in the conduct of business in line with the code of conduct & ethics and good corporate governance practices.

This policy is to provide an avenue for all employees of the company and the public to disclose any breach in accordance with the procedures as provided for under this policy and to provide protection for employees and members of the public who report such allegations.

The policy is designed to support the following:

i. Show the commitment to the company's business ethics of honesty, integrity and transparency;

ii. To provide a transparent and confidential process for all parties to give information on non-compliances to the Code of Ethics and Conduct, or any misconduct regardless of the offender's position, to an independent party to investigate the allegations and take the appropriate actions; and

iii. To uphold the moral duty as a responsible company by protecting the interests of all its stakeholders.

Specifically, the objectives of this policy are to:

a) Provide for a culture of zero tolerance towards fraud, corruption, bribery and any malpractice or wrongdoing.

b) Explain what qualifies as a whistle-blow and provide guidelines on how to report a concern.

c) Encourage stakeholders to bring out information helpful in enforcing good corporate governance practices.

d) Provide a platform to disclose concerns of malpractices within the organisation.

e) Mitigate against any fraud, operational or regulatory risk that could lead to potential financial loss or damage to the company's reputation.

f) Reassure and protect those who raise concerns in the public interest, and not maliciously or for personal gain, that they can do so without fear of reprisals or victimisation or disciplinary action, for making such a report.

4. Scope of policy

i. This policy shall apply to all subsidiaries of the company in whichever countries they operate from subject to the necessary changes as may be dictated by local legislation. Subsidiaries should adapt this policy in line with local legislation and organisation structures.

ii. This policy shall be read in tandem with the legislation specified in appendix 1 together with the policies mentioned in the said appendix.

iii. All directors, employees, distributors, contractors and agents of the company are covered under this policy with regard to events which have taken place or are suspected to have taken place in the company or in the course of undertaking duties for the company.

5. Reportable breaches

A breach or improper conduct that may be reported under this policy shall not be limited to fraud, theft, corruption, discrimination or harassment, but can be in regard to disobedience to any other company policy or other unethical or behavioral complaints as well.

The following are examples of breaches or improper conduct which should be reported under this policy:

TYPE	**DESCRIPTION**
Fraud	Any intention to deprive another person or the company of money by deception or unfair means.

Bribery	The illegal practice of offering something like money or anything of value to another person for the purpose of gaining an unfair advantage.
Corruption	Dishonest or unethical conduct by a person entrusted with a position of authority so as to acquire personal benefit.
Theft	The unauthorized taking of money, supplies or other property without the permission of the owner.
Financial misstatement	Statements or actions that encourage or result in false or intentionally misleading entries into accounting or financial records.
Discrimination	Statements or actions of favouritism or disadvantage to another person based on age, race, nationality, ethnicity, gender, disability or faith as the basis for employment, or retention in employment or other favour.
Harassment & bullying	Conduct, words or actions, which are habitual, uninvited, degrading, or coercive, offensive, humiliating or intimidating and result in a hostile work environment or domination of others.
Retaliation or retribution	Statements or actions that are threatening, harassing or discriminating against a whistleblower in connection with reporting a violation of law or policy, filing a complaint or assisting with an investigation or proceeding.
Environmental health & safety	Conduct, actions, policies or practices that either violate any laws on environment, health and safety legislation or which may cause or result in potentially hazardous conditions that impact the environment or the health and safety of employees, customers or third parties.
Data privacy breach	The loss of data or unauthorised sharing of the company's confidential information.
Insider trading	Using information that is still confidential within the company to trade in the shares of the company at the expense of the other shareholders or potential investors of the company.

Sexual harassment	The subjection by one person of another person to unwelcome and unwanted sexual advances, requests for sexual favours, and other verbal or physical contact of a sexual nature that creates a hostile or offensive environment.
Abuse of power or authority	Improper use of the authority and privileges that arise from the entitlements of a person's job for personal benefits or to the detriment of the company or any worker or stakeholder

6. Reporting breaches

i. Any person who shall have witnessed or experienced a breach or improper conduct on the part of a director or employee of the company, may make the report or disclosure of the breach in any of the following ways:

   a. In writing, duly addressed to either the line manager of the offender by a letter in a sealed envelope specifically marked as "Disclosure under Whistleblower Policy"; or

   b. By telephone, email or web portal to the authorised receiver at the address that will be provided by the authorised receiver.

ii. The whistleblower may be required to provide suitable proof of his/her identity, contact number, address so that additional information, if any, can be obtained.

iii. In case identity cannot be ascertained, the complaint will be treated as anonymous/ pseudonymous but will nevertheless be investigated to the extent possible unless it is completely impossible to ascertain the key details of the complaint, in which case such an anonymous or pseudonymous complaint may not attract further action.

iv. Disclosure can also be made to the authorised receiver or the line manager as the case may be, by telephone, email or through the web portal.

v. The whistleblower shall be required to provide verifiable information such as the background, history and reasons for his/her concern, together with names, dates, places and as much other relevant information as possible. It is not necessary that a whistleblower proves all facts leading to a breach, but he/she should be able to provide sufficient evidence to substantiate the assumption of a breach. Individuals are encouraged to report breaches at the earliest possible stage, in order for timely action to be taken.

vi. Although it will be preferable to make a report in English, the company will support persons reporting a breach in Kiswahili or any other language in which a report or complaint shall have been made.

vii. Additional information, as deemed necessary, will be sought by the authorised receiver or the Ethics committee.

7. Reporting levels and procedures of making reports

7.1 General

i. There shall be three (3) levels of handling disclosures under this policy:

a) Level 1: Where a report is made to the line management;

b) Level 2: Where a report is made to the authorised receiver;

c) Level 3: Where a report is made to either the chairperson of the Board or chairperson of the Audit, Risk and Compliance committee.

ii. Every recipient of a reported breach shall ensure that it is handled carefully, confidentially and promptly, irrespective of the level of the report.

iii. If a breach is not reported at the appropriate level, the person receiving the report will forward it to the appropriate level and inform the whistleblower accordingly, where the identity of the whistleblower can be ascertained.

Level 1: Reporting to line management

(a) As a general rule, employees who wish to report a breach should make the report to their immediate supervisor.

(b) In case the handling of the report by the immediate supervisor (line management) is unsatisfactory or the decision taken is in itself considered a breach, the whistleblower can make a report as a new case to the authorised receiver under Level 2 below.

Level 2: Reporting directly to the authorised receiver

If reporting to line management is not possible, because it would be inappropriate or unfeasible, or is handled in a manner that itself constitutes a breach or is otherwise improper, the whistleblower shall then be entitled to make the report to the authorised receiver by any of the methods specified in section 6.1(i) (b) of this policy.

Level 3: Reporting to either the chairperson of the Board or chairperson of the Audit, Risk and Compliance committee

(a) If the subject of a report of a breach is either a member of the Ethics committee or an executive director of the company, the authorised receiver shall forward the report directly to the chairperson of the Board or;

(b) If the subject of a report of a breach is a non-executive director other than the chairperson of the Board, then the authorised receiver shall submit the report directly to the chairperson of the Board.

(c) If the subject of a report of a breach is the chairperson of the Board, then the authorised receiver shall submit the report directly to the chairperson of the Audit, Risk and Compliance committee.

(d) Reports under the categories 7.3(i), 7.3(ii) and 7.3(iii) below shall be deemed to be Level 3 reports in this policy.

7.2 Procedure for handling reports

Upon receipt of the report under either Level 1 or Level 2 or Level 3, the line manager or the authorised receiver as the case may be, will take the following actions:

i. Confirm receipt of the report to the whistleblower.

ii. If relevant, arrange an interview with or request additional information from the whistleblower to get more details of the complaint.

iii. Inform the Ethics committee as soon as possible after receipt of a report of a breach.

7.3 Procedure on report of breach by a Board director or Ethics committee member

i. If the subject of a report of a breach is either a member of the Ethics committee or an executive director, the authorised receiver shall forward the report directly to the chairperson of the Board.

ii. If the subject of a report of a breach is a non-executive director but not the chairperson of the Board, then the authorised receiver shall submit the report to the chairperson of the Board.

iii. If the subject of a report of a breach is the chairperson of the Board, then the authorised receiver shall submit the report directly to the chairperson of the Audit, Risk and Compliance committee.

iv. Upon receipt of a report under section 7.3(i), the chairperson of the Board shall review the report and may discuss it with any other non-executive director and make a determination within ten (10) days on whether the report is admissible under the criteria listed in section 9.3 of this policy.

v. Upon receipt of a report under section 7.3(ii), the chairperson of the Board shall review the report and may discuss it with any other non-executive director who is not the subject of the report and make a determination within ten (10) days on whether the report is admissible under the criteria listed in section 9.3 of this policy.

vi. Upon receipt of a report under section 7.3(iii), the chairperson of the Audit, Risk and Compliance committee shall review the report and may discuss it with any other non-executive director and make a determination within ten (10) days on whether the report is admissible under the criteria listed in section 9.3 of this policy.

vii. Upon making a determination that a report made under section 7.3(i) is admissible, the chairperson of the Board shall constitute an ad-hoc committee of the Board comprising at least two other non-executive directors to investigate the report.

viii. Upon making a determination that a report made under section 7.3(ii) is admissible, the chairperson of the Board shall constitute an ad-hoc committee of the Board comprising at least two other non-executive directors to investigate the report.

ix. Upon making a determination that a report made under section 7.3(iii) is admissible, the chairperson of the Audit, Risk and Compliance committee shall constitute an ad-hoc committee of the Board comprising at least two other non-executive directors to investigate the report.

x. The chairperson of the Board or the chairperson of the Audit, Risk and Compliance committee may involve the Ethics committee, the Group Chief Executive Officer and other company employees or directors, as well as external advisers or institutions in the investigation as required and as far as they are not the subject of the report themselves.

xi. The decision whether a breach has occurred or not shall be taken and communicated to the whistleblower and the interested party within two (2) months after the chairperson of the Board or the chairperson of the Audit, Risk and Compliance committee have arrived at a determination or such other appropriate period as may be necessary.

xii. In case of a finding that there has been a breach, the chairperson of the Board or the chairperson of the Audit, Risk and Compliance committee, as the case may be, shall ask the ad-hoc committee to make a recommendation to the Board for its consideration and determination based on the findings of the Investigations.

xiii. Once a determination on a report has been made the chairperson of the Board, the chairperson of the Audit, Risk and Compliance committee or the chairperson of the Ethics committee, as the case may be, shall inform the whistleblower in writing about the decision taken on the whistleblower's report.

Notwithstanding the foregoing, no adverse decision shall be made against any subject of a report under this policy before the subject is given details of the complaint and allowed to make a response to it in writing or any other reasonable manner as the subject shall request.

7.4 Information to subject of a report

i. The Ethics committee may, through the Head of Human Resources or the Group Chief Executive Officer in the case of an employee, inform the subject of a report under this policy of such report having been made.

ii. If the subject of a report is a director of the Board, then the Board chairperson or the chairperson of the Audit, Risk and Compliance committee shall inform the subject of a report under this policy of such report having been made.

iii. In cases where there is a substantial risk that such notification would jeopardise the ability to effectively investigate the reported facts or to gather the necessary evidence, notification to the person about whom a report is filed can be withheld as long as such risks exist.

iv. The information given to the subject of the report will contain the facts of the breach as reported.

v. The subject of a report of breach under this policy will be given the opportunity to provide an explanation, without the name of the person who reported the breach being disclosed to him/her.

vi. The subject of the report shall be entitled to and may request access to his/her personal data held by the company through the chairperson of the Ethics committee in the case of an employee or the board chairperson or the chairperson of the Audit, Risk and Compliance committee, as the case may be.

vii. As soon as the investigation has been concluded, the subject of the report will be informed of any action to be taken as a result of the report. If the person about whom a report was filed is informed that no action will be taken, any suspension or temporary measure that had been imposed on him/her will automatically terminate and cease to be of effect.

viii. The subject shall have the right to have incorrect, incomplete and outdated data corrected or removed in accordance with the rights available under the Constitution, The Data Protection Act and the Fair Administrative Action Act respectively.

8. Protection of the whistleblower

8.1 Non-retaliation

i. Any whistleblower who reports a situation or occurrence which he/she reasonably believes is a breach under this policy shall be protected from blame, harassment or undue questioning.

ii. Retaliation against a whistleblower for reporting in accordance with this policy is a serious violation of the policy itself. If this occurs, the violator will be subject to appropriate disciplinary sanctions.

iii. Any such retaliation shall be reported to the authorised receiver, the chairperson of the Board or the chairperson of the Audit, Risk and Compliance committee at once as a breach in itself.

iv. The company, the authorised receiver and/or the Ethics committee as appropriate shall assure the whistleblower that he/she will not be expected to get involved in the investigations after providing the disclosure information.

8.2 Confidentiality

i. The company would prefer to avoid anonymous reports, as it can make investigating allegations very difficult. However, if a person feels there is no other way than filing an anonymous report and applicable local law allows for it, the company will take appropriate protective action.

ii. In recognition that a whistleblower may require anonymity, all whistleblower reports shall be handled confidentially and whistleblowers shall also be expected to observe absolute confidentiality.

iii. Under circumstances, when maintaining someone's privacy hinders finding the truth, the company may not be able to guarantee full confidentiality for the whistleblower such as where the breach may require to be reported to the police for further action.

8.3 Abuse of the policy

i. The company encourages persons to report breaches in good faith. If after an investigation a breach cannot be confirmed or cannot be substantiated, no action shall be taken against the whistleblower.

ii. Appropriate action will, however, be taken against a person who it is established made a report in full knowledge or could have known that a reported alleged breach was false at the time it was made.

iii. Where it is established that an employee has made a malicious report without any factual foundation, disciplinary action will be taken against the malicious whistleblower.

9. The Ethics committee

9.1 Role of the Ethics committee

i. The Ethics committee shall be the body duly authorised by the Board for the purpose of considering and, evaluating all protected disclosures from whistleblowers, maintaining records thereof and liaising with the Group Chief Executive Officer in the preparation of the reports to the Board under section 10 of this policy.

ii. The Ethics committee shall meet and determine within fourteen (14) days of receipt of a report, whether that report is admissible under section 9.3 of this policy.

iii. The Ethics committee may co-opt or liaise with the security officers in the company in the event that it requires investigation and or other security-related guidance with regard to any matter under its consideration.

9.2 Composition of Ethics committee

i. The Ethics committee shall consist of the following persons, each of whom shall be a full-time employee of the company and is well respected for integrity, independence and fairness:

   a. The Head of Human Resources
   b. The Editorial Director
   c. The Head of Audit, Risk and Compliance
   d. The Head of Legal, and
   e. Any other person as the committee may consider necessary to discharge its functions under this policy;

ii. The Ethics committee shall appoint a chairperson from among its members whose primary function shall be to preside during the conduct of the committee's functions.

iii. A member of the Ethics committee, who is the subject of a whistleblower's report shall not attend or participate in the proceedings of the committee until the report of breach against such member is conclusively resolved.

9.3 Admissibility of reports

A report by the whistleblower shall only be deemed to be admissible if:

i. It clearly specifies and relates to a breach; and

ii. It is sufficiently substantiated.

9.4 Investigation by Ethics committee

i. If the Ethics committee determines that the report is admissible, it shall investigate it by itself or through any other departments of the company or external organs as it may consider necessary.

ii. The Ethics committee shall be entitled to speak to the whistleblower either directly or through the authorised receiver to clarify the information provided or may seek additional information from other persons.

iii. The Ethics committee shall, in conducting its investigations, be entitled to all documents and information from the company, its subsidiaries, employees or directors, including all of the company's departments and organs as it shall consider necessary for that purpose.

iv. Upon conclusion of the investigation, the Ethics committee shall consider the evidence and determine whether a breach has occurred or not.

v. If the Ethics committee determines that a breach has been established to have been committed by an employee, it shall make a recommendation to the Group Chief Executive Officer based on the company's policies and any other applicable laws for execution in accordance with the recommendation.

vi. The Ethics committee shall simultaneously with its recommendation to the Group Chief Executive Officer inform the whistleblower in writing about its recommendation. This information may be direct or through the authorised receiver.

vii. The Ethics committee shall inform the whistleblower accordingly if the investigation of the report takes more than one (1) month and give a written indication of how long it may take to provide a final response.

viii. Providing false information, refusal to give information and, or, withholding relevant information from the Ethics committee will be regarded as gross misconduct on the part of an employee or any other involved party.

ix. The periods mentioned in this policy start on the day following the date on which the report is received at the appropriate reporting level, unless otherwise indicated.

9.5 Confidentiality

i. The authorised receiver, the whistleblower, the Ethics committee and the Board shall keep each report confidential.

ii. Information relating to the report shall only be given to other persons within the company if they need this to execute their tasks under this policy and/or to implement the conclusions of the investigation.

iii. The name of the whistleblower will not be disclosed, unless this is necessary for the investigation and/or judicial procedures and only after informing the whistleblower.

10. Reports

The Ethics committee shall provide a report of cases covered under this policy to the Group Chief Executive Officer and the Board through the Audit, Risk and Compliance committee on a quarterly basis.

11. Data privacy and retention periods

i. Personal data relating to a report judged to be “inadmissible” or “admissible but not valid” shall be removed immediately.

ii. The Ethics committee will take the necessary technical and organisational measures to adequately safeguard personal data against loss or unauthorised access.

iii. Personal data relating to reports that are “admissible and valid” will be kept for two (2) years, unless disciplinary action is taken or court proceedings are filed against a person. In these events, the data will be removed within two (2) years after the disciplinary action or the court proceedings have been finalised.

APPENDIX 1: LIST OF APPLICABLE LAWS

In implementation of this policy, regard and compliance shall be made to the following laws and regulations as amended from time to time:

i. The Companies Act (2015)

ii. The Fair Administrative Action Act (2015)

iii. The Penal Code (Cap. 63)

iv. The Bribery Act (2016)

v. The Data Protection Act (2019)

vi. The Capital Markets Authority Act (Cap.485A) and the Code of Corporate Governance Practices for Issuers of Securities to the Public (2015)

vii. All policies and guidelines issued by the company