WHISTLEBLOWING POLICY

Aligned to the Laws of Kenya and ISO 37002:2021

Policy Document

Version 1.0

Effective Date: 20th December 2025

Approved by: Board of Directors, Impact Gateway Africa

DOCUMENT CONTROL

Policy Title	Whistleblowing Policy
Policy Owner	Compliance Officer, reporting functionally to the Board Audit and Risk Committee
Approval Authority	Board of Directors, Impact Gateway Africa
Version	1.0
Date of Issue	20th December 2025
Effective Date	20th December 2025
Review Cycle	Every 2 years, or sooner upon material legal or operational change
Applies To	All Board members, employees, interns, volunteers, secondees, consultants, suppliers, investee ventures, grant recipients, donors and any other person having dealings with Impact Gateway Africa
Related Policies	Anti Corruption and Conflict of Interest Policy; AML CFT Policy; Risk Management Policy; Human Resources Manual; Data Protection Policy; Procurement Policy; Safeguarding Policy

FOREWORD

Impact Gateway Africa ("IGA") is a venture support studio that channels principal capital, expertise and market access into early stage enterprises across the continent. The trust placed in IGA by its donors, partners, investees and the public is the foundation on which that work stands.

This Whistleblowing Policy exists to keep that trust. It provides every person connected to IGA with a safe, confidential and credible way to raise a concern when something appears to have gone wrong. IGA treats the willingness of people to speak up as a strength. The purpose of this Policy is to make speaking up as easy, as safe and as consequential as possible.

IGA commits to this Policy at Board level, and the Compliance Officer is accountable for making it real in everyday operations.

1. PURPOSE

The purpose of this Policy is to:

- provide every person connected to IGA with clear, trusted channels through which to raise concerns about wrongdoing;
- assure reporters acting in good faith of confidentiality, fair process and protection from retaliation;
- ensure every concern is taken seriously, assessed fairly and investigated proportionately;
- detect and deter bribery, corruption, fraud, money laundering, sanctions breaches and other harm to IGA, its stakeholders and the communities it serves;
- give effect to the obligations arising from Kenyan law, donor expectations, and IGA's own values and policies.

2. SCOPE

This Policy applies to all persons who come into contact with IGA. It covers concerns about the conduct of any person working for IGA, acting on its behalf, or benefiting from its activities, regardless of seniority, location or contractual relationship.

Persons covered by this Policy include, without limitation:

- Board members, members of Board committees and Trustees;
- employees, whether permanent, temporary, part time, on probation or on internship;
- volunteers, secondees and interns;
- consultants, advisors, agents and representatives;
- suppliers, contractors and sub contractors;

- investee ventures and their directors, officers and employees;
- grant recipients and beneficiaries;
- donors, partners and members of the public.

3. LEGAL AND REGULATORY BASIS

This Policy is grounded in the Laws of Kenya and is to be read consistently with them. The principal instruments include:

- The Constitution of Kenya, 2010, in particular Chapter Six on Leadership and Integrity and Article 33 on the freedom of expression;
- The Bribery Act, No. 47 of 2016, which requires entities to put in place procedures to prevent bribery, including accessible reporting channels;
- The Anti Corruption and Economic Crimes Act, No. 3 of 2003, which criminalises corruption, abuse of office and related economic crimes;
- The Ethics and Anti Corruption Commission Act, No. 22 of 2011, which provides for the reporting of corruption to the Ethics and Anti Corruption Commission;
- The Witness Protection Act, No. 16 of 2006, which provides mechanisms to protect persons who give evidence of corruption or other serious offences;
- The Proceeds of Crime and Anti Money Laundering Act, No. 9 of 2009, which requires reporting of suspicious transactions to the Financial Reporting Centre;
- The Prevention of Terrorism Act, No. 30 of 2012, which governs counter financing of terrorism obligations;
- The Employment Act, No. 11 of 2007, which governs the employment relationship and provides protection against unfair termination;
- The Data Protection Act, No. 24 of 2019, which governs the handling of personal data collected during reporting and investigations;
- The Public Officer Ethics Act, No. 4 of 2003, where dealings with public officers arise.

Internationally, this Policy is informed by ISO 37002:2021 on whistleblowing management systems, ISO 37001:2016 on anti bribery management systems, and the United Nations Convention against Corruption, 2003.

4. POLICY STATEMENT

IGA welcomes, values and protects the reporting of concerns. IGA commits to the following standards in every case:

- Every report made in good faith will be taken seriously, assessed fairly and investigated proportionately.
- Every reporter acting in good faith will be protected from retaliation of any kind.
- Confidentiality will be preserved to the fullest extent consistent with a fair investigation.
- Anonymous reports are accepted and will be acted on where they contain sufficient information to enable a meaningful response.
- The fact that a report turns out, after investigation, to be unsubstantiated will not of itself expose the reporter to any adverse consequence.
- Knowingly false, malicious or vexatious reports are not tolerated and may themselves be investigated.
- This Policy does not replace any statutory right to report directly to a regulator or law enforcement agency.

5. WHAT CAN BE REPORTED

Concerns may be reported under this Policy whenever a reporter reasonably believes, on the facts available to them, that wrongdoing has occurred, is occurring, or is likely to occur. The following categories are illustrative and not exhaustive.

Category	Examples
Bribery and corruption	Offering, giving, receiving or soliciting bribes, kickbacks, facilitation payments or any other improper advantage, contrary to the Bribery Act, 2016 and the Anti Corruption and Economic Crimes Act, 2003
Fraud and financial impropriety	Theft, embezzlement, falsification of records, false expense claims, forged signatures, duplicate invoicing, diversion of donor or investee funds
Money laundering and terrorism financing	Any suspicion that funds handled by IGA are the proceeds of crime, or that IGA, an investee, a counterparty or a beneficial owner has links to terrorism financing, contrary to the Proceeds of Crime and Anti Money Laundering Act, 2009 and the Prevention of Terrorism Act, 2012

Category	Examples
Sanctions breaches	Actual or suspected engagement with sanctioned persons or entities; circumvention of IGA's sanctions screening controls
Conflict of interest	Undeclared personal, family or financial interests that influence, or could influence, decisions made on behalf of IGA
Procurement irregularities	Bid rigging, collusion, favouritism in tender evaluation, or any breach of the IGA Procurement Policy and the Public Procurement and Asset Disposal Act, 2015 where applicable
Data protection and confidentiality	Unlawful processing, disclosure or loss of personal data contrary to the Data Protection Act, 2019; unauthorised disclosure of confidential information
Safeguarding, harassment and discrimination	Sexual harassment, exploitation or abuse; bullying; discrimination on grounds protected by the Constitution and the Employment Act, 2007; harm to any beneficiary touched by IGA programmes
Health, safety and environment	Conduct that endangers the health, safety or life of any person, or that causes serious environmental damage
Abuse of power or mismanagement	Misuse of authority, waste of resources, maladministration, or the deliberate suppression or destruction of information
Retaliation	Any act of reprisal, dismissal, demotion, harassment or other detriment taken against a person because they have made, or intend to make, a report under this Policy
Any other breach of law or IGA policy	Any other act or omission that is, or could be, a breach of Kenyan law, donor rules, or any IGA policy, procedure or code of conduct

6. WHO CAN REPORT

This Policy is open to anyone who has information about a concern falling within its scope. A reporter does not need to be certain that a wrong has occurred. It is sufficient that the reporter has a reasonable basis to believe so. A reporter does not need to have evidence in hand. It is enough that the reporter shares what they know.

Reports from persons external to IGA, including beneficiaries, members of the community, members of the public and donors, are welcomed through the channels set out in Section 7.

7. REPORTING CHANNELS

A reporter may choose whichever channel feels safest. IGA maintains multiple channels so that no single channel is a barrier to speaking up. A reporter is not required to raise a concern with their line manager first.

Channel	How to use it	Best for
Line manager	Speak to your immediate supervisor in person or by email	Everyday concerns that can be resolved locally and do not involve the line manager or a senior leader
Compliance Officer	Email: whistleblowing@impactgatewayafrica.africa to via website form that goes directly to the Board Chair and CEO.	Most concerns, including bribery, fraud, AML or CFT suspicions, sanctions issues and conflicts of interest
Chair of the Audit and Risk Committee	Sealed envelope marked "Strictly Confidential and To Be Opened By Addressee Only" sent to the registered office of IGA	Concerns implicating the Compliance Officer, the CEO, the CFO or a member of the Executive Committee
Chair of the Board	Sealed envelope as above, addressed to the Chair of the Board or via email that goes directly to the board chair whistleblowing@impactgatewayafrica.africa	Concerns implicating the Chair of the Audit and Risk Committee or the Board as a whole
Independent Whistleblowing Hotline	Operated by an independent third party on behalf of IGA. Contact details: [the lawyers office]	Reporters who prefer a wholly independent channel, including fully anonymous reports
Ethics and Anti Corruption Commission	Toll free: 1551 Email: report@integrity.go.ke SMS: 22180 Website: www.eacc.go.ke	Where the reporter considers internal channels inappropriate, or where the matter constitutes a criminal offence of corruption, bribery or economic crime
Financial Reporting Centre	Website: www.frc.go.ke Email: info@frc.go.ke	Suspicious transactions involving money laundering or terrorism financing
Office of the Data Protection Commissioner	Website: www.odpc.go.ke Email: info@odpc.go.ke	Serious breaches of the Data Protection Act, 2019

8. CONFIDENTIAL AND ANONYMOUS REPORTING

8.1 Confidential reporting

A confidential report is one in which the reporter identifies themselves to the Compliance Officer (or the recipient of the report) but asks that their identity be protected. The recipient will keep the reporter's identity known only to those who strictly need to know in order to carry out the investigation. Disclosure to any other party, internal or external, requires the written consent of the reporter, except where IGA is compelled to disclose by court order, subpoena or an overriding statutory obligation.

8.2 Anonymous reporting

An anonymous report is one in which the reporter's identity is not known to IGA. Anonymous reports are accepted and acted upon. However, because investigators may not be able to seek clarification from an anonymous reporter, anonymous reports should contain as much detail as possible, including specific dates, names, places, amounts and any supporting documents.

8.3 Reference number and follow up

Where the independent Whistleblowing Hotline is used, the reporter receives a unique reference number and personal identification number (PIN). Using these credentials, the reporter can return to the hotline at any time to provide further information, answer investigator questions or check the status of the case, without disclosing identity.

8.4 Choice of channel

The choice between confidential and anonymous reporting, and the choice of channel, belongs to the reporter. IGA encourages confidential reporting because it allows for more effective investigation, but will not pressure any reporter to identify themselves.

9. PROTECTION FROM RETALIATION

IGA commits to the following rules, which apply to every report made in good faith regardless of its ultimate outcome.

1. No person will be dismissed, demoted, disciplined, harassed, transferred, subjected to loss of benefits, threatened or otherwise placed at a disadvantage because they have made, or are believed to have made, or are considering making, a report under this Policy.
2. No person will be subjected to retaliation because they have cooperated with an investigation, given evidence, provided information, or otherwise assisted the Compliance Officer or the Audit and Risk Committee.
3. Retaliation against a Family Member, close personal associate, colleague or representative of a reporter is treated as retaliation against the reporter.

4. Retaliation is a material breach of this Policy. Where substantiated, it will be treated as gross misconduct under the Employment Act, 2007 and the IGA HR Manual, and will attract disciplinary action up to and including summary dismissal.
5. Where retaliation is suspected, the Compliance Officer may, with the approval of the affected person, implement temporary protective measures such as reassignment, remote working or leave on full pay pending investigation.
6. Where the retaliator is a third party (for example a supplier or an investee), IGA will pursue the remedies set out in the relevant contract, including termination and debarment, and may refer the matter to law enforcement.

Risk to the reporter	IGA's response
Dismissal or disciplinary action	Any proposed disciplinary action against a reporter is reviewed by the Compliance Officer and the Head of HR. Action is only taken where it is demonstrably unrelated to the report and otherwise justified on the merits
Harassment, bullying or hostility	Treated as a fresh breach of this Policy and of the HR Manual. Subject to immediate investigation and disciplinary action, up to and including summary dismissal for gross misconduct
Loss of professional opportunity	Decisions on promotion, training, assignment and remuneration involving the reporter are reviewed for one year after the report to ensure they are made on the merits
Practical safety risk	Where a credible safety risk exists, the Compliance Officer may recommend temporary reassignment, remote working or, in serious cases, a referral to the Witness Protection Agency under the Witness Protection Act, 2006
Legal exposure for the reporter	IGA will, where appropriate, fund independent legal advice for a reporter acting in good faith under this Policy, subject to CEO and Chair of the Audit and Risk Committee approval
Third party retaliation (supplier or investee)	Treated as a material breach of contract. Remedies include termination of contract, debarment, damages and referral to law enforcement

10. RESPONSIBILITIES OF THE REPORTER

A reporter is expected to:

- report in good faith, with a reasonable basis for their concern;
- provide as much relevant information as possible, including dates, names, places, amounts and supporting documents;
- cooperate with reasonable follow up requests from the investigator, including clarification where the reporter has not chosen to remain anonymous;
- keep the fact and content of the report confidential, including by not discussing it with colleagues or on social media, so as to protect the integrity of the investigation;
- refrain from conducting any personal investigation, confronting the person concerned, or gathering evidence by unlawful means;
- report any perceived retaliation promptly to the Compliance Officer or the Chair of the Audit and Risk Committee.

Reporting in good faith does not guarantee a finding in the reporter's favour. A report that is not substantiated, provided it was made in good faith, will not expose the reporter to any adverse consequence.

11. FALSE, MALICIOUS OR VEXATIOUS REPORTS

While IGA will err on the side of believing reporters, a person who makes a report knowing it to be false, or with intent to mislead, harass or cause harm, is in breach of this Policy. Such conduct will be investigated and may result in disciplinary action, termination of contract, referral to law enforcement, or civil action by IGA.

An investigation that concludes a report is unsubstantiated is not of itself evidence of bad faith. Good faith is presumed unless the contrary is clearly established.

12. INVESTIGATION PROCESS

Every report is handled in accordance with the standard process below. The timelines are targets. The Compliance Officer may extend them with the approval of the Audit and Risk Committee where the complexity of the matter requires, and will keep the reporter informed where contactable.

Step	Stage	What happens	Timeline
1	**Acknowledgement**	The Compliance Officer acknowledges receipt of the report to the reporter (where contactable) and opens a confidential case file with a unique reference number	Within 3 working days
2	**Initial assessment**	The Compliance Officer evaluates whether the concern falls within this Policy, whether there is a reasonable basis to proceed, and whether any immediate protective action is required	Within 10 working days
3	**Triage and assignment**	The concern is classified, an investigator is appointed, and a proportionate investigation plan is prepared. Conflicted persons are excluded. External investigators may be engaged for serious matters	Within 15 working days
4	**Investigation**	Evidence is gathered, relevant persons are interviewed, and any person implicated is given a fair opportunity to respond in line with the rules of natural justice. Confidentiality is preserved throughout	Target 60 days; extended only with written approval of the Audit and Risk Committee
5	**Report of findings**	A written investigation report is prepared setting out the facts established, findings, root causes and recommendations. The report is shared with the CEO and, for material matters, with the Audit and Risk Committee	Within 15 working days of closing the investigation
6	**Decision and action**	Appropriate disciplinary, contractual, civil or criminal action is taken. Recommendations are added to the IGA Risk Register and tracked to	Within 30 working days of the report

Step	Stage	What happens	Timeline
		completion. External referrals are made where required by law	
7	**Feedback**	The reporter is given feedback on the outcome to the extent permitted by law, confidentiality and the rights of any person investigated	At closure
8	**Closure and records**	The case file is closed, archived securely and retained for not less than seven (7) years. Lessons learned are shared across IGA on an anonymised basis	At closure

13. CONFIDENTIALITY AND DATA PROTECTION

13.1 Case file handling

Every whistleblowing report is recorded in a secure case management system accessible only to the Compliance Officer and authorised investigators. Case files are not stored in the ordinary HR or operational systems.

13.2 Legal basis and lawful processing

Personal data processed in the course of a whistleblowing investigation is processed on the legal basis of IGA's legitimate interest in preventing and detecting wrongdoing, and in compliance with the Data Protection Act, 2019. Data subjects have the rights afforded to them by that Act, subject to any lawful restriction necessary for the integrity of an ongoing investigation.

13.3 Retention

Case files are retained for a minimum of seven (7) years after closure, or longer where required by law, donor rules or anticipated litigation. Anonymised lessons learned may be retained indefinitely for training and improvement.

13.4 Disclosure to third parties

The identity of a reporter who has chosen confidential reporting will not be disclosed to any third party without the reporter's written consent, save where disclosure is compelled by a court order or by an overriding statutory obligation, in which case the Compliance Officer will, where lawful, inform the reporter in advance.

14. SPECIAL CATEGORIES OF CONCERN

14.1 Safeguarding

Concerns involving the safety, welfare or dignity of a child, a vulnerable adult or any beneficiary of an IGA programme are treated with the highest urgency and are referred to the Safeguarding Focal Point in parallel with any other investigation.

14.2 Criminal conduct

Concerns that disclose, or appear to disclose, a criminal offence are referred to the Ethics and Anti Corruption Commission, the Directorate of Criminal Investigations, or the Office of the Director of Public Prosecutions as appropriate. Referral does not relieve IGA of its own investigative duties.

14.3 AML, CFT and sanctions

Suspicions of money laundering or terrorism financing are handled in accordance with the IGA AML CFT Policy. Where a Suspicious Transaction Report or Suspicious Activity Report is required, it is filed with the Financial Reporting Centre by the Compliance Officer.

14.4 Conflicts of interest in the investigation

If any person involved in receiving, assessing or investigating a report has an actual, potential or perceived conflict of interest, they must recuse themselves immediately. Where the Compliance Officer is conflicted, the matter is escalated to the Chair of the Audit and Risk Committee. Where the Chair of the Audit and Risk Committee is conflicted, the matter is escalated to the Chair of the Board.

15. ROLES AND RESPONSIBILITIES

Role	Key responsibilities
Board of Directors	Sets the "tone from the top"; approves this Policy; holds management accountable for its effective operation; receives reports on material whistleblowing matters; approves dispositions implicating senior management
Audit and Risk Committee	Provides oversight of the whistleblowing programme; reviews trends and lessons learned; receives quarterly reports on the case log; commissions independent investigations where required
CEO	Owns implementation of this Policy; ensures adequate resources are available; takes timely action on investigation findings; ensures retaliation is not tolerated
Compliance Officer	Day to day custodian of this Policy; receives and triages concerns; maintains the case log; conducts or commissions investigations; reports to the Audit and Risk Committee

Role	Key responsibilities
Head of HR and Administration	Supports investigations that involve employment matters; applies the disciplinary process fairly; protects the reporter from retaliation
Heads of Function	Promote the Policy in their teams; escalate concerns promptly; cooperate fully with investigations; do not retaliate
All Covered Persons	Report concerns in good faith using the channels described; cooperate with investigations; maintain confidentiality; refrain from retaliation

16. COMMUNICATION AND TRAINING

The Compliance Officer is responsible for:

- publishing this Policy on IGA's intranet and external website;
- including the Policy in the induction pack for every new joiner;
- delivering annual speak up training to all staff and Board members, as provided for in the IGA Training Policy;
- briefing investees, suppliers and grant recipients on the availability of the Policy as part of onboarding;
- displaying whistleblowing channel details prominently in IGA premises.

17. REPORTING AND OVERSIGHT

The Compliance Officer reports to the Audit and Risk Committee at each committee meeting on the following metrics, on an anonymised basis where appropriate:

- number of reports received, by channel and category;
- number of investigations opened, ongoing and closed;
- average time from receipt to closure;
- substantiation rate;
- disciplinary or contractual actions taken;
- themes and lessons learned.

The Audit and Risk Committee reports to the Board annually, or sooner for any material matter, on the effectiveness of the whistleblowing programme.

18. REVIEW AND CONTINUOUS IMPROVEMENT

This Policy is reviewed at least annually by the Compliance Officer. Revisions are approved by the Board. The effectiveness of the Policy is measured through the reporting metrics above, periodic staff surveys on trust in the Speak Up process, and external benchmarking against ISO 37002 and comparable peer organisations.

APPENDIX A WHISTLEBLOWING REPORT FORM

Complete as much of this form as you are able to. You may remain anonymous. If you provide contact details, we will use them only to follow up on this report.

Date of report	
Reporter name (optional, may be left blank)	
Relationship to IGA (employee, consultant, supplier, investee, donor, other)	
Preferred contact method (email, phone, anonymous hotline reference)	

Details of the concern

1. Nature of the concern (select or describe all that apply): bribery or corruption; fraud or financial impropriety; money laundering or terrorism financing; sanctions breach; conflict of interest; procurement irregularity; data protection; safeguarding, harassment or discrimination; health, safety or environment; abuse of power or mismanagement; retaliation; other.

2. Person or persons involved (names, positions, organisations if known):

3. What happened? Please describe what, when, where, how and how often:

4. Who else knows about this, or may have information? (Names, roles if known):

5. Supporting documents or evidence (please attach copies where possible and list here):

6. Have you raised this concern elsewhere (internally or externally)? If yes, where and when?

7. Is there any reason you fear retaliation? If so, please explain so that IGA can take protective measures:

For office use only

Case reference number	

Received by	
Date received	
Initial classification	
Assigned investigator	
Date closed	

APPENDIX B WHISTLEBLOWING CASE LOG (TEMPLATE)

Maintained by the Compliance Officer. Reviewed at each meeting of the Audit and Risk Committee. Retained for not less than seven (7) years after case closure.

Case No.	Date received	Channel	Category	Status	Outcome	Closed date

APPENDIX C INVESTIGATION PLAN (TEMPLATE)

Case reference	
Investigator(s) assigned	
Conflict of interest screening completed by	
Scope of the investigation	
Key allegations to be tested	
Evidence sources to be reviewed	
Witnesses to be interviewed	
Confidentiality and data protection safeguards	
Immediate protective measures (if any)	
Proposed timeline	
Approval by Compliance Officer	
Approval by Audit and Risk Committee (if extended)	