



**War Child**

**Anti-Fraud and Anti-Corruption**

**AFAC - POLICY**

**2024**

Policy Document

## Policy Executive Summary

Purpose & objectives	<p>The purpose of this policy is to reaffirm War Child Alliance’s zero tolerance for all forms of fraud and corruption. It outlines the response to mitigate fraud through deterrence, prevention and detection actions.</p> <p>The War Child has zero tolerance against fraud and corruption. War Child has an internal control framework in place to deter, prevent and detect violations.</p> <p>Staff members, volunteers and temporary staff (day workers, consultants) have a duty to report actual or suspected fraud, misconduct, or corruption in accordance with this AFAC policy.</p>
Description & Scope	<p>Implementing partners have a duty to report actual or suspected fraud, misconduct, or corruption to War Child and to have procedures in place to deter, prevent and detect violations. They must comply with this AFAC policy as annexed to the Partner Funding Agreement.</p> <p>Other third parties such as donors, vendors, community based organisations and beneficiaries are made aware of this policy and are stimulated to report suspicions of fraud or corruption involving War Child’s resources, staff or partners by any practical means, as determined locally.</p>
Shared Platform Investigations role	<p>Investigations and AFAC roles will be managed under the Shared platform. Results will be shared with Fundraising members and Country offices as provided for in the Internal Audit Charter and the War Child Alliance (WCA) agreement. Suspected violations will be investigated and if proven, will be followed by appropriate response.</p>
References	<p>References to other policies are made in the text.</p> <p>The Speak Up! Procedure is especially relevant as it contains incident reporting procedures.</p>

## Policy Details

This policy applies to	All members of staff and all external parties that have a contractual relationship with War Child Alliance
Responsible team/ department	Director of Finance, IT & Risk Management
Integrated Core Humanitarian Standard	9 (9.1, 9.2, 9.3, 9.5, 9.6)
Commencement date	1-01-2024

## Approval Signatures

	Global Internal Audit & AFAC lead	Director Finance, IT & Risk Management	Chief Executive Officer
Date	28.12.2023	08.03.2024	06.03.2024
Signature			
Name	Emmanuel Wanyama	Esha Van der Hulst	Rob Williams

# Table of contents

Table of content .....	4
1 Introduction .....	5
1.1 Policy Objectives and Purpose: .....	5
1.2 Zero tolerance.....	5
1.3 Responsibilities .....	5
1.4 Internal Control Framework.....	6
1.3 Incident Reporting.....	6
2 Definitions and Violations .....	7
2.1 Definitions .....	7
2.2 Examples.....	7
3 Deterrence and Prevention.....	11
3.1 Due diligence .....	11
3.2 Risk assessment.....	12
3.2 Communication and Training.....	12
4 Detection .....	13
4.1 Reporting mechanisms .....	13
4.2 Obligations and monitoring of implementing partners. ....	14
4.3 Transaction level monitoring.....	14
4.4 Internal and external audits .....	15
5 Response .....	15
5.1 Investigation.....	15
5.2 Sanctions and loss recovery .....	15
6 Monitoring, Learning and Disclosure .....	17
7 Final Notes .....	18
7.1 Risks.....	18
7.2 Policy Enforcement, Amendments and Review .....	18
7.3 Abbreviations .....	18

# 1 Introduction

## 1.1 ***Policy Objectives and Purpose:***

The purpose of this policy is to reaffirm War Child Alliance's zero tolerance for all forms of fraud and corruption. It outlines the steps to be taken in response to possible fraud.

## 1.2 ***Zero tolerance***

War Child has zero tolerance against fraud and corruption.

“Zero-tolerance” means that War Child will pursue all allegations of fraudulent acts and that appropriate disciplinary measures will be applied if wrongdoing is established. In addition, certain matters may be referred to authorities for prosecution.

Despite its zero tolerance policy, War Child acknowledges that a residual risk of fraud or corruption will always exist, no matter how hard the organisation fights it. The objective of this policy is therefore to reduce fraud and corruption to an absolute minimum through adequate and systematic deterrence, prevention, detection and response actions.

## 1.3 ***Responsibilities***

War Child employees are responsible stewards of funds and assets under War Child's care. Employees and third-parties (volunteers, implementing partners, consultants, vendors, donors and beneficiaries), acting on War Child's behalf or providing goods and services, play a vital role in the deterrence, prevention and detection of fraud, misconduct, corruption, waste and abuse at all levels of the organisation. Staff and external parties have a duty to report actual or suspected fraud or corruption.

The Chief Executive Officer of the War Child Alliance has overall responsibility for the establishment of internal controls. The design and implementation of appropriate frameworks of internal controls is delegated to the Director Finance, IT & Risk management. Responsibility over the management of financial resources is also delegated to Country Directors and project managers. This delegation highlights senior management's responsibility to set the “tone at the top”: by behaving ethically, by creating a positive work environment, by hiring and promoting employees who are competent and have the right work ethic, by implementing the Code of Conduct; by ensuring that fraud controls are implemented; and by taking disciplinary actions when necessary within the parameters established by policies.

Through their delegated authority, Country Directors, Fundraising Member Directors and Shared Platform Directors with their management teams are responsible and accountable for ensuring that all measures aimed at preventing, detecting, and responding to fraud, misconduct and corruption

are in place and that an appropriate and robust internal control environment is maintained. This includes:

- ✓ Ensuring that all AFAC measures are in place and are monitored;
- ✓ Leading and reporting on periodic risk assessments;
- ✓ Raising awareness of risks and ensuring that all staff are more vigilant;
- ✓ Encouraging staff to report any suspected fraud or misconduct without fear of retaliation;
- ✓ Assisting in the recovery of loss related to proven fraud;
- ✓ Reporting breaches of this policy.

The Internal Auditor has responsibility for conducting internal audits and for conducting or coordinating investigations in the organization, consistent with the WCA internal audit charter.

Specific to the AFAC Policy, the Audit & Risk Committee of the Supervisory Board (“Audit & Risk Committee”) will review the prevention, detection and response mechanisms, as well as fraud and corruption incidents and internal audit reports. The Audit & Risk Committee promotes the effectiveness of the audit and investigations function and provides a forum to discuss internal control, fraud and corruption.

#### **1.4 Internal Control Framework**

This Anti-Fraud and Anti-Corruption Policy is a cornerstone of the organization’s internal control framework, which is further set out in the Finance and Accounting Policy. This Policy should also be read in conjunction with the associated Speak Up! procedure, the Global Safeguarding Policy and the Code of Conduct.

The ultimate objective and principle of the Internal Control Framework is to nurture a culture of ethics, integrity, transparency and accountability and thereby to enhance the trust in War Child, both internally and externally.

#### **1.3 Incident Reporting**

Everybody must speak up if and when they suspect or witness fraudulent activities or corruption within War Child, its partner organisation or another party affecting War Child. No matter who is involved, senior or junior staff, and no matter the materiality or the context.

Incidents will be reported through the avenues provided for under the Speak up! Procedure, which includes anonymous or direct channels, on email or through the online link, all of which will be managed in a confidential and serious manner.

## 2 Definitions and Violations

This chapter gives a definition of fraud, corruption and misconduct. There are many definitions and one must take a broad and sensible interpretation of the definitions given. This chapter also provides a list of examples of violations of this policy. Again, this list is non-exhaustive and violations include, but are not limited to the examples given herein. It is also important to note that violations include attempted violations, so-called “near misses”, even if unsuccessful.

### 2.1 Definitions

Fraud is the wrongful or criminal deception by an individual with the intention of obtaining a personal gain, either direct or indirect and either immediate or delayed. It means the actual or attempted use of deceit, falsehood, or dishonest means to secure a personal benefit, and includes fraudulent conduct, corrupt conduct, collusive conduct, coercive conduct, and obstructionist conduct (as defined below).

Corruption encompasses any act or omission that misuses official authority or that seeks to influence the misuse of official authority in order to obtain an undue benefit for oneself or a third party.

Misconduct encompasses any act or omission whereby an individual or entity carries out unacceptable or improper behavior, wrongdoing, mismanagement, neglect of duties or violation of laws, regulations, rules, policies or procedures.

For the purpose of this AFAC Policy, the term “**Fraud**” is intended to include fraud and corruption.

### 2.2 Examples

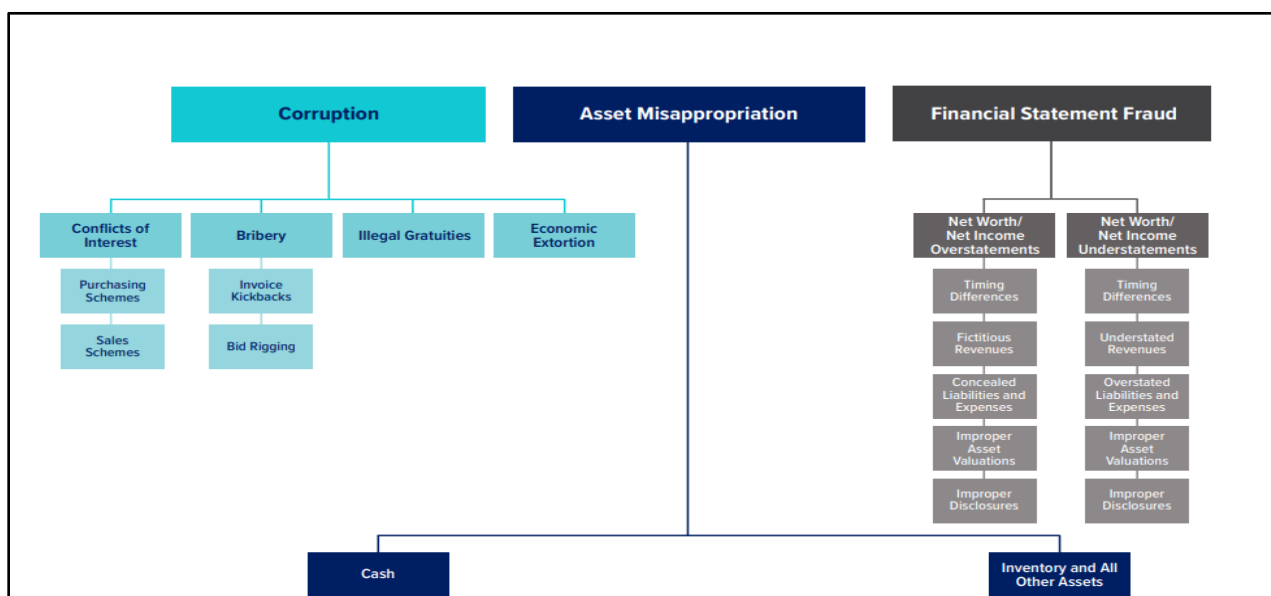
Violations of this policy include the use or the theft of resources belonging to War Child for personal gain of oneself or that of a personal relation (a relative or friend). It also includes abusing ones position by making decisions that are not (fully) in the interest of War Child, due to a conflict of interest. Employees are obliged to disclose to War Child any situation that may appear as a conflict of interest, including when he/she or his/her close relatives or friends has/have an interest or economic ties of any kind with a supplier, a job candidate or an implementing partner of War Child.

Staff members carrying out functions with high fraud risk (such as in procurement, distribution, awarding of grants to partners, or senior management) may be subject to greater scrutiny. It is of overriding importance that actions of such staff members could not be reasonably be perceived as favourable treatment to an individual or entity. In order to preserve staff members' independence

and impartiality, War Child's rules prohibit the solicitation or acceptance of any kind of honours, decorations, favours, gifts or remuneration from any source. In this regard, provisions relevant for all employees have also been included in the Code of Conduct.

A list of examples is given below, but this list is not exhaustive and does not replace the need to exercise prudent judgement in all situations that may arise. In cases of doubt, advice can be sought with the line manager, with the Global Internal Audit & AFAC Lead or with the Director of Finance, IT & Risk Management. In case of suspicion or proof of a breach report in line with the Speak Up! Procedure.

Generic Types of Fraud are shown Below;



The scope of detailed fraud schemes includes but is not limited to:

- Altering results: Increasing or decreasing the (financial) results of the organisation.
- Asset misappropriation: Unlawful appropriation of assets. Forms of asset misappropriation are theft; forgery; embezzlement; skimming; payroll fraud and deception.
- Bribery: Offering or implying money, gifts, preferment or privileges, or undertaking any other unlawful action that alters the behaviour of the recipient, e.g. payoffs and kickbacks.
- Collusion: Agreement with customers or suppliers to charge lower prices; to raise spurious credit notes and to accept under-delivery of, or delivering of inferior goods or services.
- Computer fraud: The use of a computer to take or alter data, or to gain unlawful use or access of computers, applications or services, e.g. hacking; unauthorised access to a bank account.
- Contracts awarded improperly: Awarding contracts to third parties based on interests other than organisational interests.
- Corruption: Paying, promising, authorizing, offering to give or receive anything of value directly

or indirectly to any government official, political party, party official or political candidate to influence the passage of law, regulations, the placement of government contracts, the formulation of policy or other discretionary government functions that accrues to the benefit of the ultimate recipient or promotes his or her interest.

- Covering up: Altering, adding, falsifying or deleting records to cover up unlawful or unethical actions, such as misappropriation.
- Deception: Act of deceiving such as false expense claims, unauthorised expenditures, and purchases from fictitious vendors.
- Embezzlement: Dishonestly withholding assets, goods or financial donations.
- Extortion : The use of authority to secure unlawful financial gain or advantage.
- Facilitating Payments: Offering or making a small payment to a low-level public official, which is not officially required, to enable or speed up a process which is the official's job to arrange.
- Financial statement fraud: Manipulation of financial statements.
- Forgery :The action of forging a document or a signature, such as an invoice or banknote.
- Manipulation of contracts: Using unlawful or unethical means to exercise pressure on the process of drafting a contract with a third party.
- Misappropriation of service or goods: Unlawful or unethical use of services or goods for personal ends or for the benefit of relatives, intended for and/or paid for by the organisation.
- Money Laundering: The process of taking the proceeds of criminal activity and making them appear legal.
- Nepotism: The unfair use of power in order to get jobs or other benefits to family or friends; patronage or favoritism on the basis of family relationship.
- Payoffs and kickbacks: Situations in which cash or other benefits are accepted in exchange for contracts, assignments, purchases. Payoffs are paid or received before the deal is made, whereas kickbacks are paid or received during or afterwards.
- Payment fraud: The unauthorised altering of creditor, payroll or benefits systems in order for an (existing or non-existing) employee or supplier to receive funds which are not due.
- Revenue and expenditure recognition: Involves recording receipts in incorrect periods, holding bills or the improper coding of bills to profit from financial mechanisms such as currency fluctuation or budget revisions.
- Sharing of confidential information: Sharing of confidential information with third parties without proper authorization or underlying documentation, or without valid reason.



- Skimming: Taking money from receipts and failing to record the revenues in the books.
- Theft: Direct theft of cash, stock or assets, as well as theft of intellectual property, customer lists, contracts, (confidential) information.
- Unfavorable transaction: Undisclosed financial interests in a transaction taken on at unfavorable terms.
- Unlawfully influencing decision making: Using unlawful means to influence decision making within the organisation.
- Unpaid purchases: Ordering goods on credit with no intention of paying.

### 3 Deterrence and Prevention

War Child's anti-fraud and anti-corruption framework includes preventive measures encompassing:

- ✓ a system of internal control (such as segregation of duties, standards for supporting documents, the authorization matrix and system hard controls) laid down in the Global Finance manual,
- ✓ standards of conduct laid down in the Code of Conduct,
- ✓ procurement procedures (such as a transparent bid process with multi-functional selection committees) as laid down in the Logistics Policy,
- ✓ implementing partner monitoring procedures of activities and expenses and contractual obligations to refrain from fraud and corruption as laid down in the Partnership Policy,
- ✓ audit protocols laid down in the Internal Audit Protocol,
- ✓ tools and procedures laid down in process-specific anti-fraud controls,
- ✓ whistleblowing and incident reporting mechanisms and the signing of a statement by all employees, as laid down in the Speak Up! Procedure,
- ✓ due diligence before entering into a business relation (see below)
- ✓ risk assessment (see below),
- ✓ communication, training and awareness raising (see below).

#### 3.1 *Due diligence*

Anti-fraud due diligence measures comprise various activities aimed at subjecting a person or third party (e.g. consultants, vendors, donors, implementing partners, staff, etc.) to systematic scrutiny of any indications of past or present fraudulent activity or otherwise unwanted behavior prior to engaging in a business relationship with them. This includes:

- ✓ Background and reference checks of recruits as laid down in the Human Resources Policy,
- ✓ Third party screening laid down in the Counter Terrorism and Anti Money Laundering Policy,
- ✓ Supplier vetting laid down in the Logistics Policy,
- ✓ Checking implementing partner's past performance, previous engagements, funding structure and references as laid down in the Partnership Policy,
- ✓ Verification of Civil Society Organisations, e.g. that the entity is established/registered as a non-profit organisation and that its mandate is in line with War Child principles,
- ✓ Searching the internet to review comments, feedback, reviews, social media activity, annual reports, financial statements and news articles that may indicate red flags related to any of the above parties,
- ✓ The Responsible Fundraising Policy covers additional areas that are relevant for diligence for donors.

Due diligence measures do not stop at the point of engagement but continued screening is extended at regular intervals on existing relationships. In addition, anti-fraud clauses are included in agreements and contracts as applicable.

### **3.2 Risk assessment**

The shared platform will prepare a risk register of key strategic risks for the War Child Alliance, the fundraising members and Country offices will perform annual risk assessments as part of their annual planning, including fraud and corruption risks. This helps management to understand risks, to identify weaknesses in controls and to develop practical plans to mitigate those risks. The fraud risk assessment includes:

- ✓ identifying fraud risk factors and potential fraud schemes;
- ✓ assessing the likelihood and impact of the risks;
- ✓ mapping the suitability of existing fraud controls;
- ✓ documenting key findings and conclusions in the country or departmental annual plan;
- ✓ reporting on the risks and mitigating measures in the periodic reporting cycle.

The Shared platform directors, Country Directors and fundraising member Directors are responsible for conducting the risk assessment.

The Internal Audit function supports the risk management function to facilitate the process by reviewing the overall risk assessments and by ensuring that assessments are an ongoing effort, results are properly communicated and that mitigation efforts are implemented in a timely manner.

### **3.2 Communication and Training**

Communication and training are important in the development and nurturing of an anti-fraud culture. The internal auditor is responsible for the global communication and training. Periodic communications are distributed regarding anti-fraud efforts and results. The internal auditor develops or selects training material for mandatory fraud-awareness trainings, which are conducted in-person or online. These trainings convey to staff and other stakeholders the importance of preventing and reporting fraud, and deter potential violators as they become aware of the risks associated with fraudulent conduct.

War Child's reporting procedures should be displayed physically, in the language that is generally used in the geographical area, at all programme sites and at War Child and the implementing partner's offices during the period of active implementation of a programme on behalf of War Child.

## 4 Detection

Preventive measures may serve as detection measures and vice versa. For example, monitoring transactions is a detection mechanism, but staff being aware that diligent monitoring is being performed also has an important preventive value. War Child's fraud detection methods are laid out in the following paragraphs.

### 4.1 Reporting mechanisms

Employees and third parties have the duty to report any (suspected) breach of this Policy as laid out in the Speak Up! Procedure. Reporting suspicions and actual breaches of this Anti-Fraud and Anti-Corruption policy is a joint responsibility of everyone. Everybody must speak up if and when they suspect or witness fraudulent activities or corruption within War Child, its partner organisation or another party affecting War Child. No matter who is involved, senior or junior staff, and no matter the materiality or the context.

Whistle blowers (staff and third parties alike) can use the mechanism highlighted in the Speak Up! Procedure without fear of retaliation, reprisals and in the full knowledge that their interests will be protected. There is a procedure for anonymous reporting, which is encouraged for cases where the reporter feels unsafe to make their identity known, because anonymous reporting this may impede effective and efficient investigation due to lack of witnesses and evidence. Anonymous reporting also increases the risk of defamation. Defamation is the communication of a false statement that harms the reputation or otherwise harms an individual. Spoken defamation is also called slander, and defamation in other media such as printed words or images, is called libel. War Child does not tolerate deliberate defamation.

Reports can take any form, including: complaint, allegation, observation or concern, and can originate from any source, including: identified or anonymous, employees, beneficiaries, implementing partners, vendors, stakeholders or the communities where the programmes are implemented. War Child will continue to enhance its reporting mechanisms and consider the cost effectiveness of an independent third-party to manage the reporting where practical to do so. These are currently outlined in the speak up! Procedure.

When reporting on possible breaches, staff members and others are encouraged to provide as much detail as possible, including any supporting documents. However, staff (including managers) or others should not take steps to investigate the alleged misconduct without first consulting with the internal auditor.

Employees and others may not be retaliated against for complying with the duty to report possible misconduct. No action may be taken against staff or others as a reprisal for reporting and disclosing information on possible fraud or corruption, or otherwise co-operating with investigation and audit activities. Individuals who believe they have been subjected to retaliation or a threat of retaliation should report this in accordance with the Speak Up! Procedure.

#### **4.2 *Obligations and monitoring of implementing partners.***

War Child expects its implementing partners to adhere to the highest standards of moral and ethical conduct, to respect local laws and not to engage in any form of fraudulent or corrupt practices. As part of contractual terms, War Child requires implementing partners to use resources efficiently and for the intended purpose, refrain from acts of fraud and corruption, and to have procedures in place to address incidents of fraud or corruption.

Funds entrusted with partners are subject to regular monitoring activities, verifications and audits by War Child's finance and programmes staff, by the internal auditor and/or by external auditors. This includes regular programme visits, scheduled audits, voucher checks and reviewing financial reports against partner activities. It also includes training, capacity building, recommendations, resolutions and remediation when issues and risks are identified.

Appropriate provisions are included in all agreements with implementing partners to put into place strengthened measures for prevention and detection; to report allegations of fraud and corruption to War Child; and to cooperate in any investigation undertaken by War Child to detect possible fraud or corruption. Failure by implementing partners to take effective measures to prevent misconduct, failure to investigate allegations of misconduct, or failure to take disciplinary and corrective actions when misconduct is found to have occurred constitutes grounds for the termination of the Partner Funding Agreement and for other follow-up actions by War Child.

#### **4.3 *Transaction level monitoring***

Shared Platform, Fundraising Member and Country Office finance and logistics officers play an important role in detecting fraud and corruption when doing their periodic and systematic checks of the financial statements on a high level as well as on transaction level. They specifically check if procurement processes were followed and if there are any inconsistencies in supporting documentation.

War Child will follow developments in the area of systems that perform automated analytics technology in order to scan financial data to detect abnormalities and identify suspicious transactions that require further follow-up.

#### **4.4 Internal and external audits**

Proactive fraud detection procedures by War Child's Internal Audit function include continuous auditing techniques specifically designed to detect fraudulent activities as part of internal audit and external audit reviews. These are normally established as part of the audit plans on an annual basis, as proposed by the internal auditor based on a risk assessment and as approved by the Audit & Risk Committee.

## **5 Response**

Staff members and external parties who violate, willfully or with gross negligence, the principles of this AFAC Policy or who directly or indirectly take part in any of the specific violations described herein, either through their own action or by not implementing mandatory control mechanisms, are subject to sanctions and may be required to reimburse War Child for losses incurred to the organization as a result of their actions.

### **5.1 Investigation**

For each reported suspicion or breach, an internal or external investigation is conducted. Employees and third parties have the duty to cooperate with audits and investigations. The purpose of fraud investigations is to collect evidence relating to specific allegations in order to determine the facts relating to a case. Investigations are conducted in a timely manner and case results are reported to management using established protocols.

The investigations examine the allegations of corrupt or fraudulent practices and allegations of misconduct involving staff, consultants, implementing partners, and institutional contractors. The type and scope of the investigation will be reasonable compared with the (suspected) severity of the breach. The investigation includes research of documents and conduction of interviews, taking note of confidentiality. If possible and if not dangerous or harmful to (relations of) War Child, the person who is the subject of the investigation is confronted with the suspicions or the findings.

The Internal Auditor has responsibility for conducting internal audits and for conducting or coordinating investigations in the organization, consistent with its internal audit charter.

The applicable law and all relevant circumstances are considered in the investigation and when deciding on the sanction.

### **5.2 Sanctions and loss recovery**

War Child holds people accountable for fraud and misconduct through administrative or disciplinary measures and contractual remedies. Once fraud or misconduct has been detected management takes appropriate action to remedy the harm caused (e.g. initiates legal proceedings where

necessary to recover monies or other property lost) and administers discipline to those involved in the inappropriate actions (e.g. dismissal of the staff member(s) involved; cessation of relationships with third parties involved; blocking guilty parties from working with the Organization in the future; reporting of the incidents to the authorities where appropriate), as well as those in management positions who failed to prevent or detect such events in accordance with the relevant policies in place.

War Child's policy is to recover any fraud and corruption losses incurred by the organisation. War Child reserves the right to sanction employees that violate the AFAC policy. Even in case of suspicion only, War Child reserves the right to take all measures necessary to protect its reputation.

Sanctions, disciplinary measures and actions by War Child may include, but are not limited to:

- ✓ Suspension until full investigation is complete, with or without pay,
- ✓ Verbal reprimand,
- ✓ Written censure,
- ✓ Written warning letter,
- ✓ Demotion or loss of one or more steps-in-grade of staff member,
- ✓ Recovery of losses by deduction of salary or by other means,
- ✓ Legal proceedings to recover or claw back losses,
- ✓ Separation or dismissal of staff with or without notice or compensation,
- ✓ Black listing individuals or organisations,
- ✓ Cessation of relationships with third parties involved,

Apart from the above mentioned sanctions, War Child may report the case to the relevant authorities, such as but not limited to the police or the prosecutor, where the misconduct may be considered a criminal act.

When monies are due to War Child, the organization will make use of all means available to recover misappropriated funds, including by making deductions from salaries, wages, pension and other emoluments, and by taking judicial action before the relevant national authorities.

The internal auditor is tasked with facilitating oversight over fraud loss recoveries and overseeing response to fraud cases. The Audit & Risk Committee is responsible for assessing the effectiveness thereof.

## 6 Monitoring, Learning and Disclosure

All incidents are registered in the Case management system and will be updated in a global Fraud and Corruption Incident Register by the Internal Audit function. Documents related to the incident report, investigation and justification of sanctions are filed with the register. The internal auditor and the Audit & Risk Committee will examine the incidents to determine the root causes of the relevant control breakdowns, ensuring that risk is mitigated and that controls are strengthened.

The incident register is reviewed by management for monitoring and learning purposes and it is shared with the statutory auditor at its request. Incidents are reported to the Audit & Risk Committee of the Supervisory Board immediately or in its next meeting, depending on the severity and materiality of the loss. The Audit & Risk Committee will review War Child's strategy and its prevention, detection and response mechanisms to fraud and corruption. The Audit & Risk Committee provides a forum to discuss internal control, fraud and corruption issues.

Actual examples of fraud and corruption are used internally for awareness raising and learning purposes. Cases are adjusted and anonymized for confidentiality reasons.

When a fraud affects resources trusted to War Child by a donor, and the grant agreement specifies that War Child should report the case to the donor, such cases are reported to the donor as per through the donor account manager via the Fundraising members account manager or Shared Platform Fundraising Team.

War Child believes the humanitarian sector can benefit from more openness about fraud and corruption cases. War Child reports externally about breaches in its organisation in accordance with local legislation and regulation, but it may also do so voluntarily in its annual report or on its website. War Child will reasonably respect confidentiality and privacy of parties involved.



## 7 Final Notes

### 7.1 Risks

Not complying with the AFAC Policy could lead to the following main -interrelated- risks:

- ✓ Financial risk. War Child carries the financial consequences of mismanagement and loss of resources due to fraud and corruption. It also risks financial fines by authorities and the financial expenses of investigations and legal procedures. Even in case of fraud by partners or other related parties, War Child is ultimately responsible for all sub-awarded funds and remains fully responsible and accountable to the donor. Non-compliance might result in ineligible costs and audit qualifications.
- ✓ Reputational risk. War Child's good reputation with donors, partners, beneficiaries and the general public may be harmed. War Child's good reputation is of utmost value. Damage to it may affect risk ratings by donors and ultimately may result in withdrawal of funding.
- ✓ Human resources risk: A culture of non-compliance to AFAC standards is hurtful and demotivating to honest and loyal staff, who may decide to exit the organisation.

### 7.2 Policy Enforcement, Amendments and Review

Proposals for improvements can be made to the Policy Owner who will decide upon immediate need for an amendment process or to keep the input for future review process. Implementation of the policy is the responsibility of all employees, while the Internal Auditor monitors the implementation and facilitates as needed.

A formal evaluation and review process will take place three years after start of the policy implementation or earlier as decided upon by the IMT.

### 7.3 Abbreviations

<b>Abbreviation</b>	<b>Clarification</b>
AFAC	Anti-Fraud and Anti-Corruption
IMT	International Management Team
CMT	Country Management Team
WCA	War Child Alliance Foundation