actionaid

Final and Approved

Global Staff Safety & Security Policy (2019)

Author:	Javeria Ayaz Malik
Owner:	GS Staff Security Advisor
Version:	FINAL & APPROVED
Approved by:	General Assembly June 2019

Table of Contents

Terminologies and Abbreviations

- **AAI:** ActionAid International
- **Acceptance:** A strategy often adopted by humanitarian organisations that aim to reduce security risks by gaining acceptance for their presence and work by upholding strong ethics, value and needs-based programming.
- **Concern:** Any occasion where staff have reason to believe that a contextual situation or event may possibly impact the safety, security, health or well-being of themselves, their colleagues, partners or communities.
- **Consultant:** Any individual hired from a Limited Company (i.e. not freelance consultants who are deemed as Staff) that have been contracted by ActionAid to undertake services or activities on its behalf.
- **Deterrence:** A strategy only used by humanitarian organisation in extreme circumstances that aim to reduce security risks by issuing counter-threats (e.g. threatening to stop programming).
- **Dependant (s):** For the purpose of this Policy, the term means accompanying Partner, Spouse and/or dependent children of a relocated or deployed staff member.
- **Diverse profiles:** The personal identity characteristics of an individual, for example, their age, biological sex, gender, ethnicity, sexuality, religion, etc.
- **Duty of Care:** A legal, moral and contractual obligation that requires an employer to minimise any risks to staff and third parties as far as reasonably practicable in pursuit of its mission (i.e. standard of reasonable care)[1]
- **Evacuation:** The physical movement of staff over an international border in response to a significant deterioration in the security environment or any situations where associated safety and security risks are no longer manageable.
- **GS:** ActionAid's Global Secretariat
- **Hibernation:** The temporary suspension of programmatic activities or the restriction of staff's physical movements in response to any incident, situation or event that present elevated safety and security risks.
- **HR:** Human Resources
- **ILT:** International Leadership Team (Global Secretariat) comprising of AAI Secretary General and International Directors
- **Incident:** Any situation or occasion where the safety, security, health or well-being of staff, partner or communities are compromised or put at any undue risk.
- **Member:** Associate and Affiliate Members of the Federation
- **Near-Miss:** Any situation that has narrowly avoided becoming an incident through either luck or adherence to policies or procedures.
- **Programme:** ActionAid's programme refers to all aspects of our work including but not limited to projects, campaigns, child sponsorship, fundraising, administration, and other official duties.
- **Protection:** A strategy used in higher risk environments that aims to reduce security risks by placing physical or procedural barriers between staff and the 'thing or being' that may harm them.

[1] ActionAid's liability as an employer is provided by the applicable laws in each country where ActionAid acts in this capacity.

- **Relocation:** The physical movement of staff over within the same country in response to a significant deterioration in the security environment or any situations where associated safety and security risks are no longer manageable.
- **Safety:** Freedom from risk resulting from unintentional acts where there is no motive to inflict damage or harm (e.g. Road Traffic Accident due to mechanical fault)
- **Security:** Freedom from risk resulting from violence or intentional acts where there is a motive to inflict damage or harm (e.g. compound robbery, carjacking, kidnap)
- **SHEA & Safeguarding:** Sexual Harassment, Exploitation and Abuse, Child Abuse, and Adult at Risk Abuse
- **Staff:** Any individual, including employees, volunteers, short-term workers, Trustees/Board members, accompanied legal dependants (relocated staff), and freelance consultants working for ActionAid under a contract of employment or under ActionAid's instruction.

1. Policy Statement

For its *Strategy 2028* to be realised and successfully implemented, ActionAid must accept and manage risk, rather than adversely avoiding it.

Fighting global injustice, challenging gender inequality, eradicating poverty and working in locations where there are disasters and protracted crises does not come without an inherent and foreseeable exposure to safety and security risks. It is not reasonable, or even possible, for ActionAid to completely eliminate these risks. For it to remain purposeful and impactful in driving social change, ActionAid acknowledges that its staff, consultants and others working on its behalf will face situations where their health, safety, security, and well-being may be jeopardised in some way. However, it is ActionAid's duty to ensure that these situations are rare and exceptional, and that it is well prepared to deal with them when, or if, they occur, in line with this Policy, our Health & Safety Policies, Code of Conduct, as well as our Sexual Harassment Exploitation and Abuse (SHEA) and Safeguarding approach.

This *Duty of Care* to its staff is not just influenced by ActionAid's need to comply with applicable laws, legislations or donor requirements, but is equally driven by its desire to keep staff, consultants and others safe, secure and healthy when working on its behalf or under its instruction, because morally, it is the right thing to do.

2. Scope and Application

This *Global Staff Safety & Security Policy* aims to outline how safety and security risks that ActionAid staff [2] and others working under its instruction are exposed to during the delivery of its work are to be consistently managed to within acceptable limits across the entire ActionAid Federation.

The Policy acts as the foundation for any subsequent procedures, plans, tools or initiatives that ActionAid or any of its Members develop and implement to mitigate safety and security risks that staff and others working on ActionAid's behalf or under its instruction are exposed to.

All ActionAid staff are expected to read and understand this Policy in full. To support this, familiarisation with this Policy will be included in HR induction for all new starters or upon the Policy's revision. **Any deliberate breach of this Policy is considered to be serious misconduct and will result in disciplinary measures being applied.**

This Policy must be shared with and effectively rolled out to all staff, legal dependants, official visitors, consultants and others to whom this Policy applies, as well as with allies and partners for their information.

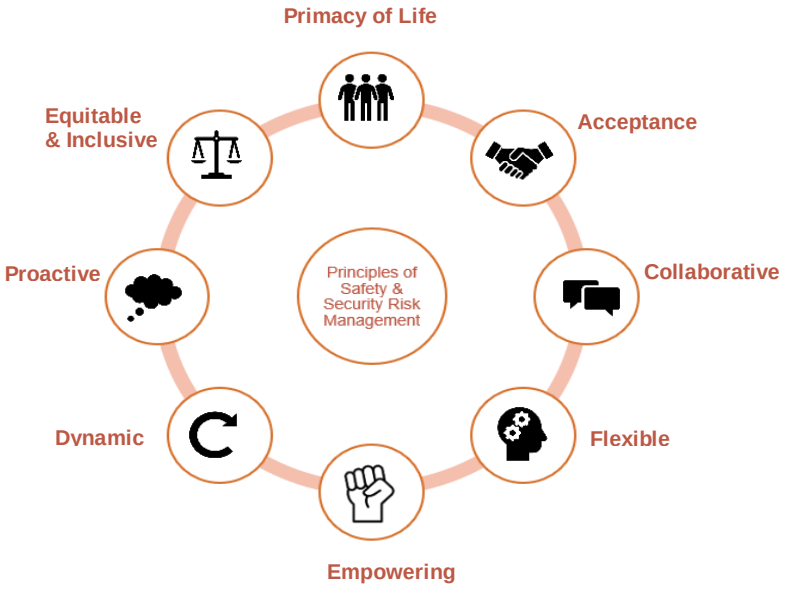
This Policy does not intend to replace any national or local laws that apply in contexts where ActionAid operates. For circumstances where applicable national or local laws do not align with or contradict this Policy, it is these national or local laws that supersede any instructions, directives or statements issued by ActionAid under this Policy.

[2] Any individual, including employees, volunteers, short-term workers, Trustees, legal dependants and freelance consultants working for ActionAid under a contract of employment or under ActionAid's instruction.

3. Principles

ActionAid's approach to managing safety and security risks is underpinned by the following **eight** guiding principles which have all been designed to engender a strong 'risk management culture' across the ActionAid Federation. When applied consistently and correctly, the principles will enable the safe delivery of its *Strategy 2028*, rather than unnecessarily inhibiting it.

Only in extreme circumstances e.g. when there is a direct threat to the life of staff, accompanied legal dependants, consultants or others working under ActionAid's instruction, and with explicit written authority from the Secretary General (for GS and CPs) or Country/Executive Director (for Affiliate /Associate Members) can these principles be deviated from or overridden.



a. Primacy of Life

Without exception, unless explicitly mentioned in this Policy, ActionAid will prioritise to protect the safety, security, health and well-being of all staff, consultants or others working on its behalf or under its instruction above anything else; this includes preserving finances, assets, reputation or external relationships. Furthermore, no staff or consultants are expected to place themselves in excessive danger [3] or undue risk in order to deliver ActionAid's activities or programmes.

b. Acceptance

In keeping with its organisational values, ActionAid will seek to gain acceptance for its presence and work as a primary strategy for reducing safety and security risks during the delivery of activities, programmes and campaigns.

[3] See Section 5 on Risk Appetite

In practice, this means nurturing and maintaining strong working relationships with relevant local actors through active communication, respectful personal conduct and values-driven programming.

However, given that its *Strategy 2028* advocates ActionAid to be bolder and more courageous in fighting global injustice, gender inequality and poverty, it is recognised and acknowledged that it may not be able to gain acceptance from everyone. In such circumstances, ActionAid may consider adopting harder protective or deterrence measures in conjunction with its acceptance strategy to reduce harm to staff; however, these measures should not stray into being the 'norm' (as this would be a strong indication that associated safety and security risks exceed what ActionAid is willing to accept – see Section 5 - 'Risk Appetite')

In order to support its default strategy of acceptance, ActionAid must be very strict on staff involvement with arms and cautious about its engagement with armed actors. Staff members must never be in possession of or handle weapons, explosives or ammunition when representing ActionAid, and no armed personnel will be allowed into any ActionAid premises or vehicles.

The use of armed protection (e.g. armed guards or escorts) can only be approved by the **International Director of Federation Development** in situations where it is assessed that not taking these measures will present a clear and immediate threat to life. Where ActionAid needs to interact with armed actors (e.g. in a conflict zone or post-disaster situation), all efforts must be made to ensure ActionAid remains independent and separate from these parties.

c. Collaborative

ActionAid believes that managing safety and security risks to within acceptable limits is best achieved collectively, rather than in isolation. Not only does this mean that internal roles and responsibilities for safety and security risk management must be shared across all levels of the organisation, but that ActionAid must actively collaborate with partners, social movements or other external stakeholders to pool expertise, knowledge and resources to ensure that safety and security risks are being managed effectively and sustainably.

d. Flexible

The locations where ActionAid operates in and the circumstances surrounding its work vary so greatly from programme-to-programme that it cannot simply apply a single, fixed approach to managing safety and security risks. As such, ActionAid will never assume that what may have provided effective risk management in one context will work in another. Whilst ActionAid wants to encourage consistency and standardisation in how safety and security risks are managed across the entire Federation, this must not endanger its ability to remain flexible and nimble to the varying types of safety and security threats, incidents or situations that ActionAid faces across its operating locations.

e. Empowering

In addition to the above, any subsequent safety and security procedures, plans, tools or initiatives that ActionAid or any of its Members develop and implement must not encourage a formulaic or 'box-ticking' approach to safety

and security risk management. Rather, they should empower staff, managers and senior leaders to think and adapt to the diverse range of factors that influence their exposure to safety and security risks, and that encourage creativity and innovation.

f. Dynamic

Considering that the nature and severity of any safety and security risks that our staff face will alter over time and locations (due to a variety of influencing factors), safety and security risk management is not something that can be switched 'on and off; As such, ActionAid commits to ensure that its approach to managing safety and security risks is constantly reviewed against the prevailing environments where its work, the circumstances surrounding our activities, sector best-practice and any changes to applicable laws or legislation. Furthermore, staff, managers and Board members must ensure that safety and security risk management, including cyber security risks, are openly and regularly discussed, and that it forms an integral part of programme design.

g. Proactive

ActionAid's approach to managing safety and security risk predominantly seeks to prevent incidents from occurring, rather than just relying on strong response mechanisms should an incident occur. In practice, this means that ActionAid will place a strong emphasis on being able to identify, assess and mitigate safety and security risks prior to undertaking any of its activities, programmes or campaigns.

Additionally, by adopting the principles of being '*Collaborative*' and '*Dynamic',* ActionAid will always have appropriate contextual knowledge, platforms and resources that enable it to anticipate changes in risk exposure, any impending threats that indicate a deterioration in the environments where its works and ensure that it is well placed to react to these changes.

h. Equitable & Inclusive

ActionAid recognises that its staff may face, or perceive to face, varying degrees of safety and security risk due to their gender, perceived gender, ethnicity, religion, HIV / AIDS status, race, sexual orientation, physical and mental ability or any other protected characteristics. As such, and in line with our intersectional feminist approach, ActionAid will manage safety and security risks with sensitivity and inclusivity to these individual factors, and it will aim to apply measures that offer equal and fair protection to staff regardless of their profile.

Only in exceptional circumstances where it is has been determined through inclusive risk analysis that the gender, perceived gender, ethnicity, religion, HIV / AIDS status, race, sexual orientation, physical and mental ability or any other protected characteristics of an individual increases their risk exposure (or that of others) beyond limits which ActionAid or the concerned staff are willing to accept, will additional measures or restrictions be placed on individuals or groups. Such action will only be driven by our Duty of Care obligation and will not be applied with discrimination of any kind.

4. Roles & Responsibilities

ActionAid strongly advocates that effective safety and security risk management can only be achieved where roles and responsibilities are shared across **Strategic, Operational and Individual** layers. Failure to address these at any one of these layers will see safety and security ultimately diminish.

Below shows roles and responsibilities that are assumed at each one of these layers:

Strategic	
At the **Global Secretariat**, the following groups or individuals are responsible for:	
Governance Bodies (National / International Board and General Assembly)	• Ownership of risk and carrying the highest responsibility and accountability for ensuring ActionAid's Duty of Care towards staff and third parties (International Board is accountable for implementation of this Policy at the GS and Country Programmes, while National Boards are accountable for their respective Members). • Ensuring that staff security is prioritised and a strong 'risk management' culture is promoted and role-modelled by the Trustees and Senior Management. • Overseeing that ActionAid's *Minimum Safety & Security Requirements* are consistently applied and supported in terms of human and financial resources across the Federation.
International Leadership Team (Delegated authority from the International Board)	• Defining the level of safety and security risks ActionAid is willing to accept in pursuit of its mission and vision, ensuring that this is well communicated across the entire Federation and is incorporated into all subsequent policies, procedures, tools and resources used by ActionAid to control or regulate safety and security risks. • Ensuring that a *Global Staff Safety & Security Policy* is developed that outlines a common approach to safety and security risk management across the entire Federation, and that its relevance and effectiveness is reviewed at least once every 03 years or whenever there is a significant change in external or internal operating context. • Specifying *Minimum Safety & Security Requirements* to be adopted and consistently applied across the Federation during the delivery of programmes, official travel, the reporting of incidents and dealing with critical incidents or major crises. • Establishing mechanisms and resources that ensure ActionAid is resilient and well-prepared to respond to any safety or security incident (including online/cyber threat) that may cause harm or disruption to programmes, regardless of its magnitude. • Reporting to the International Board cases where Country Programmes, Associates or Affiliates are routinely in breach of ActionAid's *Minimum Safety & Security Requirements* • Championing a strong 'risk management culture' across the Federation.

GS Staff Security Advisor	• Developing, disseminating and maintaining the *Global Staff Safety & Security Policy* and subsequent staff safety and security procedures, guidelines, tools and templates that are applicable across the Federation. • Evaluating ActionAid's *Minimum Safety & Security Requirements to* ensure that they provide effective governance, regulation and management of safety and security risks, and that these can be feasibly fulfilled in practice. • Reviewing the Federation's compliance with this Policy and reporting incidents of non-compliance to the ILT. • Providing technical advice and guidance to Security Focal Persons and senior leaders, including Country / Executive Directors across the Federation to successfully meet ActionAid's *Minimum Safety & Security Requirements.*
For **Country Programmes**, **Affiliate or Associate** members of ActionAid, the following groups or individuals are responsible for:	
Senior Leadership Team (Delegated authority from the International and National Boards)	• Providing reasonably practicable human and financial resources to ensure ActionAid's *Minimum Safety & Security Requirements* are being fully met on paper and in practice. • Defining mechanisms to ensure staff, consultants and others working on ActionAid's behalf or under its instruction can report safety and security incidents that occur during the course of official work or travel. • Periodically assessing the safety and security of staff and consultants as a corporate risk and reporting to the relevant Governance Bodies as well as to the GS Staff Security Advisor if this has significantly increased or negatively changed. • Providing reasonably practicable travel and personal accident insurance to staff or consultants working under ActionAid's instruction, and ensuring access to medical and psychosocial assistance when needed.
Operational	
At an Operational level, the following groups or individuals are responsible for:	
Director of Federation Development and Heads of Country Support	• Monitoring that the GS, CPs and Members are complying with this Policy and ActionAid's *Minimum Safety & Security Requirements.* • Ensuring that ActionAid programmes including projects, campaigns and other activities are designed and implemented with the safety and security of staff in mind (e.g. ensuring that any decision to start programming in a new location is informed by an assessment that ActionAid can competently manage associated safety and security risks to within acceptable limits).
Country / Executive Director	• Championing a strong 'risk management culture' and leading by example. • Ensuring that programmes and activities that come under their remit are being delivered with full adherence to ActionAid's *Minimum Safety & Security Requirements.*

	• Ensuring that all programmes and activities are being thoroughly and comprehensively risk assessed before they are approved, including those that are already being implemented. • Ensuring rules, regulations and plans are in place that describe mandatory measures that staff, consultants and third parties (as applicable) must follow to prevent safety and security incidents from occurring, and that ensure ActionAid is able to anticipate and react to incidents and emergencies if they occur. • Acting as the alternative point-of-contact (in the absence of a trained Security Focal Person) for staff, consultants and third parties to report any safety and security incidents, near-misses or concerns that may occur in any locations under their remit. • Ensuring that any visiting or newly recruited or deployed staff, consultants or accompanied legal dependants have been informed of the contextual safety and security risks they are exposed to when working in or visiting the country (including that they understand the measures, mechanisms and provisions ActionAid has, and does not have, to minimise these risks). • Appointing a suitable member of staff to act as a Security Focal Person who is able to commit at least 20% of their time to safety and security functions[4]. • For locations that have a **HIGH** or **EXTREME** Security Threat Level: Approving any field movements and emplacing mechanisms to monitor the whereabouts of staff during field movements. • Ensuring that adequate finances that support the implementation of ActionAid's *Minimum Safety & Security Requirements* are appropriately budgeted for.
Security Focal Persons (This includes all part-time and full-time SFPs, as well as those externally employed or retained)	• Supporting Country Directors or the GS Office Management to fulfil ActionAid's *Minimum Safety & Security Requirements* by leading on the production and review of country-level Risk Assessments, Safety and Security Rules / Regulations and Contingency Plans. • Delivering or emplacing mechanisms to deliver contextual safety and security briefings to incoming visitors or newly recruited / deployed staff, consultants, accompanied legal dependants and, where necessary, partners and third parties. Ensure that briefings are carried out in line with ActionAid's values and SHEA and Safeguarding approach • Acting as a primary point of contact for staff and other working under ActionAid's instruction to report any safety and security incidents, near-misses or concerns that occur in areas under their responsibility

[4] In some high-risk environments, a full time Security Focal Person may be appointed, while smaller teams operating in low-threat environments may reduce the time allocation. An informed decision must be taken by the Senior Management Team who will be responsible to review the environment and adjust accordingly. The role can also be outsourced to an external advisor/consultant if deemed reasonable and effective by the relevant management.

	• Ensuring that safety and security risks within facilities or premises that are owned, leased or routinely used by ActionAid are being appropriately risk assessed and mitigated. • For locations that have a **HIGH** or **EXTREME** Security Threat Level: Providing support to the Country / Executive Director to inform any decision to approve or decline field movements and emplacing mechanisms to monitor the whereabouts of staff during field movements.
Human Resources Managers	• Ensuring that familiarisation with this Policy is included in HR induction with new starters and hired consultants. • Supporting initiatives that promote staff health, safety, welfare and well-being. • Ensuring that staff have independent and confidential access to professional, survivor-centred psychosocial support services following a traumatic safety or security incident, including SHEA or any other emotional trauma that is experienced when representing ActionAid.
Line Managers	• Ensuring that all staff and consultants under their direct management have received a copy of this Policy and have been inducted on it by HR. • Approving any official travel undertaken by staff or consultants under their direct management on **(1)** that travel is considered to be necessary, **(2)** that they and those who are travelling are comfortable with the level of safety and security risk they are exposed to and **(3)** that all reasonable measures to reduce safety and security risks have been applied. • Ensuring that appropriate time and resources have been made available for staff and consultants under their direct management to attend necessary security training that is required of them. • Championing a strong 'risk management culture' in their teams/lines of management
Individual	
All **staff and consultants** working on ActionAid's behalf or under its instruction are expected to:	
All Staff	• Not act in a manner that contradicts or contravenes ActionAid's mission, vision or values as outlined in ActionAid's Code of Conduct. • Strictly adhere to this Policy and any other safety or security rules, regulations, instructions or directives that are issued by ActionAid. • Comply with any national or local laws or customs that exist in locations where staff and consultants are working in, travelling to or transiting through. • Treat ActionAid resources, information, equipment and money responsibly, and report any cases of their misuse. • Not abuse any of ActionAid's IT and communications equipment for illicit or inappropriate reasons.

	• Report safety and security incidents, near-misses or concerns that have caused, or have the potential to cause harm to themselves, colleagues, partners or communities. • Not use bribes, concessions or extorting others in order to gain access to locations or sensitive information, or to coerce others to undertake work on behalf of ActionAid or to represent ActionAid under duress. • In line with ActionAid's Code of Conduct, report any forms of corruption, abuse or fraud committed by colleagues or partners. This includes SHEA & Safeguarding incidents that must be reported in line with ActionAid's SHEA and Safeguarding policies. • Not behave in a way that exposes colleagues, partners or communities to any unnecessary harm or place them in undue danger.

5. Risk Appetite

Although ActionAid acknowledges that it must take risks in order to fulfil its strategy, vision and mission, yet the level of safety and security risks that it can accept in pursuit of this will be limited by its ability to cope with or tolerate such risks.

As a general principle, ActionAid is not willing to expose staff, consultants and partners to any safety and security risks that it, or its partners, cannot tolerate.

Any decisions that ActionAid makes to determine whether it accepts, avoids or transfers safety and security risks will be made on a discretional basis and informed by a thorough and comprehensive risk assessment.

Furthermore, ActionAid's appetite to accept safety and security risk is not a single, fixed concept. Rather, ActionAid may choose to accept greater safety and security risks in order to fulfil a critical programme or campaign need, as long as commensurate risk control measures have been ensured.

As opposed to defining a single threshold that expresses when any associated safety and security risks have exceeded ActionAid's willingness or capacity to accept them, ActionAid has instead developed a set of scenarios to indicate when risk appetite is close to being exceeded and that requires ILT to be notified for onward decision-making:

ILT <u>must</u> be notified for any situations:

- That place our staff in danger or increased risk because of our presence or any programming activities;
- Where ActionAid's acceptance or perceived acceptance, in a specific locality, requires it to adopt hard protective (e.g. armoured vehicles) or deterrent measures (e.g. armed guards, threatening withdrawal) as a 'norm' or as its preferred security strategy;

- Where a credible threat has been made to ActionAid staff that places their safety, security, health or well-being in immediate danger or undue risk;
- Where any high-impact events (e.g. kidnap / abduction, effects of conflict / war, sexual assault, long-term imprisonment or serious digital or reputational risk) have been assessed as having a high likelihood of occurrence.

5.1. Right to Refuse or Withdraw

Whilst efforts have been made by ActionAid to set its own risk appetite, it recognises that perceptions and attitudes towards safety and security risk can vary from person-to-person, and that its organisational risk appetite may not always be harmonious with what individuals are willing to tolerate. As such, staff, their accompanied legal dependants and consultants have a right to request to be withdrawn from locations or refuse activities that exceed their own personal risk threshold.

In most circumstances, this right will be respected by ActionAid regardless of its assessment of the associated safety and security risks, without this negatively impacting on the person requesting to be withdrawn or refusing to undertake activities. The only exception to this is if the withdrawal of individuals places remaining staff (or third parties) at greater danger or if this request has been repeatedly exercised to the point where this significantly impacts on staff's ability to fulfil their role. Such situations will be resolved by the respective Line Management in accordance with the applicable HR policies.

In line with our mission and Feminist principles, ActionAid will promote a culture in which staff, their accompanied legal dependants and consultants and others are able to raise concerns about their safety or well-being without fear of retribution (e.g. losing out on future job opportunities) or stigmatisation. If staff, their accompanied legal dependants, consultants and others believe that ActionAid's processes are in breach of this right, they can raise concerns to their Senior Management, HR, or via the Whistleblowing Policy.

5.2. No Right to Remain

Conversely, ActionAid will always retain the right to suspend activities, cancel or postpone travel, or to withdraw or relocate staff, consultants or accompanied legal dependants from locations if it feels the associated safety and security risks are beyond its risk appetite. Any directives or instructions issued by ActionAid to suspend, cancel, postpone or withdraw staff, consultants or their accompanied legal dependants must be respected by all. Failure to do so may result in disciplinary measures being taken, including possible termination of contract or association with ActionAid.

The only exception to this is in situations where ActionAid has instructed national staff to withdraw or relocate from a place where they normally reside or have family. In this case, ActionAid cannot force staff to withdraw or relocate under duress, and instead it must consider alternative and practicable 'people-focussed' measures that safeguard the health, safety, security and well-being of remaining staff and their accompanied legal dependants.

5.3. No Ransom or Concessions

If a staff member, their accompanied legal dependants or a consultant is taken hostage by any criminal, terrorist or other party, ActionAid pledges to do everything in its power to seek that individual's safe and unconditional release. However, ActionAid will not concede to any ransom, concessions or any other demands to facilitate their release on the assessment that this will only increase the risk of kidnap to other ActionAid staff.

6. Commitments to Different Stakeholders

Whilst ActionAid has a strong legal, moral and contractual obligation to provide adequate Duty of Care to anyone working on its behalf or under its instruction, the extent to which this duty can be achieved will differ from person-to-person.

The following outlines our commitments to **staff, consultants, accompanying legal dependants of deployed/relocated staff** and **social justice / programme partners:**

Staff (including short-term workers, volunteers, freelance consultants and EFAST members)
For all staff, ActionAid commits to providing: • Regulatory policies and processes that ensure they will not be undertaking activities under ActionAid's instruction that exceed its capacity and capability to manage associated safety and security risks. • Access to contextual safety and security information and a thorough induction on safety and security policies and procedures to ensure that decisions made by them to consent to safety and security risks are informed not only by understanding the nature and severity of any contextual risks, but also taking into account the measures, mechanisms and systems ActionAid has, and does not have, to mitigate these risks. • Safety and security training that is commensurate with the risks that exist in locations where they are recruited in, deployed to or visiting. Additionally, any staff that assume safety and security risk management duties or functions (i.e. Security Focal Person) will be provided with Safety & Security Risk Management training. • Safety and security-assessed accommodation for relocated/deployed staff and their accompanied legal dependants that factor in gender-specific requirements and considerations. • Means to be able to confidentially report safety and security incidents, near-misses or concerns directly to ActionAid or any affiliated third-party responders (e.g. insurers) at any time. • Access to medical, security, psychosocial and any other support and assistance immediately after reporting an incident, near-miss or concern, in line with our duty of care and SHEA and Safeguarding approach. • Dedicated and specialised crisis management support focussed on resolving or stabilising serious incidents. • Kit or equipment that is determined to be critical for their health, safety, security and well-being e.g. specialist communications equipment (e.g. satellite phones), first aid kits, Post Exposure Prophylaxis (PEP) kits, mosquito nets, any specific field clothing as applicable etc. • Access to external technical / professional security advisory services that are able to provide information, guidance and recommendations to address vulnerabilities, concerns or issues they may have, with assurance that these external services are in line with ActionAid's values.

Consultants (hired from a Limited Company)[5]

Consultants contracted to undertake activities or deliver services on ActionAid's behalf will be provided with:

- Travel / personal accident insurance[6] where it has been determined that their own insurances do not provide equivalent coverage to that provided for staff.
- Access to contextual safety and security information and pre-travel briefings.
- Extended crisis management support when the incident in question has involved ActionAid staff members as well as the consultant, or where it is found that the consultant's employer does not possess the ability to sufficiently manage, resolve or stabilise a serious, time-critical incident.

Accompanied Legal Dependants of Relocated / Deployed Staff

Accompanied legal dependants of relocated /deployed staff members will be provided with:

- Access to contextual safety and security information and pre-deployment briefings.
- Medical or personal accident insurance that enables access to emergency medical care and psychosocial support should an incident occur
- An option or possibility to be evacuated across an international border or relocated in-country (as applicable) if there is a rapid or gradual deterioration in the security environment where they are based.
- Extended crisis management support if they are involved in serious or critical incident that requires immediate support or treatment.

Partners & Communities

Partners that we routinely work alongside will be provided with:

- Technical expertise and guidance on what provisions they should have in place to govern and regulate safety and security risks they may face because of the environment they work in, what they represent and what they do.
- Where possible, an opportunity to attend ActionAid's in-house safety and security risk management trainings.
- Policies, templates and guidelines with the aim to support partners to develop their own safety and security structures and systems, while at the same time creating opportunities to recognise and learn from their experience and knowledge vis-à-vis safety and security risk management.
- For Communities: Staff must follow ActionAid's Policy on the Security of Communities in Emergencies, AA's Code of Conduct and other applicable Policies.

[5] Consultants hired independently may be treated as staff or short-term workers

[6] Consultants must provide other insurances (e.g. public liability and professional indemnity) independently

7. Minimum Safety & Security Standards

The *Minimum Safety & Security Requirements or Standards* have been developed so that safety and security risks can be consistently managed across all ActionAid programmes. **They are non-negotiable** and compliance will be measured on a yearly basis by the GS Staff Security Advisor.

For Satellite and Digital/Virtual Country Models, these standards will need to be ensured by the Centre of Excellence supporting these structures.

Country Programmes, Affiliates or Associates that are found to be in regular breach of the *Minimum Safety & Security Standards* will be reported to the International Board and General Assembly.

The standards have been designed to be applicable consistently across the Federation and cover the following main areas:

- When ActionAid is **implementing programmes, campaigns or projects in a country** (this includes Country Programmes, Associates and Affiliates and other forms of presence i.e. Country Models)
- When ActionAid staff and consultants are **travelling locally or over an international border on official ActionAid business**
- When staff and consultants are **reporting a safety or security incident, near-miss or concern**
- When ActionAid is **dealing with the impact and aftermath of a critical safety/security incident, major crisis or an external trigger event** i.e. hazard/disaster, conflict, political event.

Minimum Safety & Security Standards for Programme Delivery	
A1	All countries or locations where ActionAid is delivering programmes, projects or campaigns must be issued with a **Security Threat Level** using a credible external threat rating service**.**
A2	All Country Programmes, Members and GS offices must complete a **Security Risk Assessment** of all programme activities. This Security Risk Assessment must detail what specific risks ActionAid staff, assets and programmes are exposed to (as derived from contextual research), what context-specific measures are to be implemented to mitigate these risks and provide a quantitative score against the level of risk that remains after these mitigation measures have been applied. Risk Assessments must consider diversity in risk profiles, including both external and internal threats. All Security Risk Assessments must be reviewed once every six months, or more often in case of any event or situation that is likely to alter the environment ActionAid works in, and / or following a major incident or crisis.

<table>
<tr><td>A3</td><td>All Country Programmes, Members and GS offices must develop and effectively disseminate rules, regulations and standard operating procedures (SOP's) that ActionAid staff must mandatorily follow at all times. Rules, regulations or SOP's must be reviewed in line with Security Risk Assessment and written into a Security Plan that is disseminated to all staff who are bound by them. Security Plans must include considerations for a diverse range of personal profiles.</td></tr>
<tr><td>A4</td><td>All Country Programmes, Members and GS offices must nominate a Security Focal Person (SFP) who will act as the single-point-of-contact for staff or consultants to report safety and security incidents, near-misses or concerns, as well as manage other matters related to safety and security (Security Focal Persons can be fulltime, or part-time staff designated to perform security responsibilities, or the role could be outsourced to a retained consultant or security company depending upon the context, available resources and workload).

In the absence of a nominated and trained Security Focal Person, the Country/Executive Director (or Office Manager in case of GS offices) must act as the SFP.

The SFP must be available and on-call 24/7 for emergencies and have a nominated deputy during periods of absence.</td></tr>
<tr><td>A5</td><td>All Country Programmes, Members and GS offices must have an Emergency Contingency Plan that prescribes measures that must be taken following any incident, situation or event that results in staff requiring medical, security or psychosocial assistance, or that requires them to hibernate, relocate or be evacuated, or programmes to be suspended or closed. In line with our commitment to staff welfare and well-being, support and response options should be carried out in line with ActionAid's Feminist Principles and SHEA and Safeguarding approach.

All Emergency Contingency Plans should be developed in accordance with ActionAid's Security Phases. These may be applied across a country or specific location and ensure that clear directives and instructions can be given to staff, consultants or visitors where there is either a rapid or gradual deterioration in the environment.

<table>
<tr><th>Security Phase 01
'Normal'</th><th>Security Phase 02
'Possible Deterioration'</th><th>Security Phase 03
'Crisis'</th></tr>
<tr><td>Situation is in line with what is determined as normal. Application of SOP's and basic precautions offer sufficient mitigation.</td><td>Situation indicates that the environment is gradually deteriorating. Some extraordinary measures may need to be applied, including the partial withdrawal of non-essential staff, visitors or accompanied legal dependants, hibernation or suspension/scale down of programmes.</td><td>Situation has deteriorated to a point that presents or is likely to present immediate and serious risks to staff, consultants or visitors, or that might prohibit continuation of programmes.</td></tr>
</table>
</td></tr>
<tr><td>A6</td><td>All premises that are owned, leased or frequently used by ActionAid for accommodation, meetings, events, office or storage purposes must be approved following the completion of a Site Security</td></tr>
</table>

	Assessment. All premises must have clearly marked firefighting equipment (e.g. fire extinguishers, smoke alarms) that are checked regularly as per local laws, clearly defined evacuation procedures and a first aid kit.
A7	All locations where staff, consultants or visitors are expected to undertake activities or services must have a reliable communication infrastructure so that incidents or emergencies can be reported at any time. Where reliable communications cannot be provided by mobile telephones, Country Programmes, Members and GS offices must ensure that secondary forms of communications have been set up (e.g. radio network, satellite phones). **As far as reasonably practicable, at no point should staff or consultants be unable to report incidents or emergencies because of poor communications coverage or lack of a secondary back-up**
A8	All Country Programmes, Members and GS Offices must allocate a reasonable percentage of their budget to staff safety and security risk management depending on their local context and as informed by their local Security Risk Assessment.
A9	All users have a responsibility to observe technical and organisational policies designed to protect against unauthorised or unlawful processing of personal data and against accidental loss, disclosure, destruction or damage to personal data. Staff members are responsible for ensuring that any device they use to log in to the AA network, including remote logins, have the appropriate antivirus and threat protection installed. Performance of illegal activities through the ActionAid network by any user (Authorized or otherwise) is prohibited. Any suspected breach of security must be reported immediately. For further information, please refer to ActionAid's Acceptable Use Policy for IT Systems Here
Minimum Safety & Security Standards for Travel	
B1	All travel on official ActionAid business must be approved by a line manager under the following conditions: **(1)** it is necessary, **(2)** there is an acknowledgement and acceptance from the line manager and traveller that any associated safety and security risks are within both ActionAid's and the traveller's risk appetite and **(3)** that all other *Minimum Safety & Security Standards* defined in this Policy have been adhered to.
B2	All staff or consultants travelling internationally or locally, or those who are deployed or relocated to another country/region must provide details of their legal Next-of-Kin or an alternative emergency contact in case an incident or crisis occurs during the trip. All staff, their accompanied legal dependants or consultants who are travelling to a location that has a **HIGH** or **EXTREME** Security Threat Level must also complete a Proof of Life Form and submit this to their relevant HR Unit. Information disclosed on this form will only be accessed in the event of an incident or major crisis.
B3	All staff and dependants who are travelling or deploying to a location that has a **HIGH** or **EXTREME** Security Threat Level should complete Hostile Environment Awareness Training (HEAT) prior to

	departure. If such a training is not available locally, a suitable online training must be completed instead. These trainings must be organised and paid for by the base office (HR/Line Manager)
B4	All staff or consultants travelling internationally or locally on ActionAid business must be provided with a reliable form of communication. For destinations where an international phone with roaming enabled does not offer sufficient communications coverage, staff or consultants must be informed of where to obtain a local SIM or phone or be issued with a satellite phone.
B5	All staff and consultants that are travelling to a location that has a **HIGH** or **EXTREME** Security Threat Level can only stay in accommodations or hotels that have been security-assessed and approved by the relevant Management and Security Focal Person.
B6	All vehicles that are purchased or leased by ActionAid must be regularly serviced in accordance with the manufacturer's guidance, checked frequently, fully insured, legally registered and have basic safety devices such as seatbelts, first aid kits and breakdown equipment. Any local travel undertaken outside of a base location or urban environment that is in a country or region that has a **HIGH** or **EXTREME** Security Threat Level must be approved by the Country Director / Executive Director in advance of departure. In such circumstances, all field movement will be approved on the acknowledgement of the security situation and the condition of roads and routes at the time of intended travel. Additionally, all staff travelling to the field must communicate their arrival and departure from their destination to the SFP or Line Manager (for some contexts, more frequent check-in intervals may be enforced). Any travel that is made by air can only be undertaken with international or domestic airliners that have been approved by the relevant Management or Security Focal Person. All staff travelling by boat must be issued with or have access to a lifejacket in case of emergency.
Minimum Safety & Security Standards for Incident Reporting	
C1	All staff or consultants that are involved in, affected by or that witness a safety and security incident, or near-miss must report this to ActionAid within 24 hours of it occurring or as early as it is safe to do so. This includes SHEA and Safeguarding incidents that must be reported in accordance with ActionAid's SHEA and Safeguarding policies.
C2	All safety & security incidents or near-misses that are reported by staff or consultants must be written into an *Incident Report Form* within 07 days of it being resolved / stabilised and submitted to the concerned Security Focal Person. If the incident occurs during travel, this should be reported to the host office SFP as well as one's base station SFP.
C3	All safety & security incidents and near-misses that are recorded onto an *Incident Report Form* must be reviewed within 7 days of it being received. This review must identify why the incident or near-miss occurred and define any remedial action that must be applied to prevent its future reoccurrence. This

	review must also be used to identify and report any wider issues resulting from the incident, such as safeguarding issues. If there are potential SHEA or safeguarding issues, this must be shared with the SHEA and Safeguarding Focal Point, and/or with the Global SHEA and Safeguarding Team. Any actions that have been defined must be assigned an owner and timeframe for implementation.
C4	All incidents and near-misses reported to ActionAid must be collectively reviewed annually by the relevant SLT/ office management to identify trends, patterns and strategic actions required. This analysis must be shared annually with the GS Staff Security Advisor.
Minimum Safety & Security Standards for Critical Incident/ Crisis Management	
D1	The Global Secretariat must have an International Crisis Management Team (ICMT) that is available and on stand-by at all times to deal with the impact and aftermath of a serious incident or major crisis affecting ActionAid staff, their legal dependants, consultants or the Federation itself.
D2	For CPs and Members, a National Crisis Management Team (NCMT) must be established and remain on stand-by to deal with any serious incident or crisis that occurs in their country or region.
D3	Any CMT that is defined at the Global Secretariat or with a CP/Member must be supplemented with a Crisis Management Plan that prescribes actions and considerations that must be made when activating a [7] CMT, when a crisis is first notified to the CMT, as the crisis is being dealt with and upon its close-down.
D4	As a minimum, the CMT must have the functionality and authority to make decisions that may affect the outcome of the critical incident or crisis, provide emotional and practical support to family members, manage internal and external communication statements, liaise with third party service providers and stakeholders (e.g. insurers, governments, consultants) and record all major decisions and actions. In recognition that dealing with a serious incident or major crisis can be traumatic and may last an indefinite period of time, all individuals assuming roles or duties as part of a defined CMT must do so on a voluntary basis (i.e. with consent) and nominated deputies must be assigned to each function for contingency purposes (e.g. during periods of leave and for rotation during prolonged crises). In line with our commitment to staff welfare and well-being, during a crisis response, all members of the CMT will be offered frequent professional psychosocial support and other support options as needed.
D5	All CMT's must have appropriate training and access to contingency funds readily available for unforeseen situations.
D6	An incident or crisis that requires a CMT to be activated must have an in-depth After-Action Review within 28 days of the CMT being disbanded. The Review must be in writing and circulated to the relevant Board of Trustees as well as the GS Security Advisor.

[7] The Crisis Management Plan is a confidential document that must be accessible to the CMT only and must not be shared wider than this unless under explicit authority from the Global Security Advisor.

8. Policy Review

This Policy will be reviewed by the GS Staff Security Advisor at least once every 03 years and updated in case of a considerable change in the external or internal context where ActionAid operates. The review will be informed by sector best-practices, changes in applicable laws or legislation and an analysis of the Policy's overall effectiveness in achieving its intended purpose.