GLOBAL POLICY

SAFETY AND SECURITY

Lead	PII Global Safety and Security
Version Number	2.0
Date of Approval by Members' Assembly	20 November 2021
Effective Date	20 November 2021
Next Review Date (5 years from Effective Date)	November 2026

APPLICATION

As a Global Policy, this policy applies to:

a. Plan International, Inc. ("PII"), including its headquarters in the United Kingdom (operating through its UK subsidiary, Plan Limited), and all of its country offices, regional offices, liaison offices, and any other offices, some of which operate as branches and some as subsidiaries;
b. All National Organisations that have signed a Members' Agreement and License Agreement with PII; and
c. All other entities that agree to be bound by the Global Policies.

(together, "Plan International Entities", also referred to as "we" or "us" in this document).

All of the entities that are bound by Global Policies, including PII, shall enact their own procedures, regulations or other regulatory documents that enable compliance by its employees (and/or, when appropriate, contractors and other partners) with this Global Policy.

PURPOSE

The purpose of the Global Policy is to establish and reinforce a positive security culture across all Plan International Entities and ensure Staff feel safe, secure, and supported in their work.

This Global Policy defines our core safety and security principles and outlines our approach to managing security risks and operational safety risks, effectively responding to incidents, and incorporating lessons learned into future operations.

This Global Policy also sets out the specific responsibilities of Staff, in particular managerial Staff, regarding the aforementioned principles and functions.

POLICY STATEMENT

We are committed to fulfilling our duty of care to our Staff, and where applicable to our Associatesand Programme Participants, by providing a safe and secure environment so that we can better fulfil our Purpose of a just world that advances children's rights and equality for girls.

We recognise that our Staff and Associates may work in or travel to difficult and complex environments that present unique safety and security risks. We will be proactive in identifying and mitigating these risks, and we will prepare our staff to better manage their personal safety. In everyinstance, we understand that security risk management should be an enabler rather than a barrier.

We also acknowledge that despite our best efforts, things will sometimes go wrong, and we are committed to having robust incident and Crisis management procedures in place, as well as procedures to report and review incidents and share lessons learned.

APPLICABLE REQUIREMENTS

Our approach to security risk management emphasises increasing capacity in programmes and offices to effectively identify and address their unique risks. Thesafety and security risks to each Plan International Entity will be different, and dependent on a variety of local factors and operational circumstances. Rather than being overly prescriptive, we focus on Entities understanding and addressing the individual, and essential, elements that comprise a holistic security risk management programme and adapting these elements to the local context.

Each Plan International Entity will create and maintain a local safety and security management programme which addresses the following essential elements:

- *Prepare* – Provide relevant and appropriate training and preparedness measures for Staff and Associates. All staff should receive a security induction, including basic security training, and advanced security training for high-risk contexts. Appropriate safety and security equipment and first aid kits must be in place for all offices, vehicles, and fixed work sites (not including home-working arrangements).
- *Assess* – Develop mechanism for conducting security risk assessments prior to undertaking activities. These mechanisms must be intersectional and inclusive in their approach, and acknowledge and address specific risks related to gender, ethnicity, LGBTIQ+ (SOGIESC), and disability. Care should be taken to ensure mitigation measures are in line with risk appetites outlined in the Global Policy on Risk Management. Security risk assessment templates are standard for all PII entities.
- *Act* – Monitor safety and security situations and ensure mitigation measures remain sufficient. Security plans and standard operating procedure documents should incorporate specific mitigation measures identified during the security risk assessments.
- *Respond* - Ensure all staff are aware of incident reporting requirements.Maintain a pool of relevant functional area representatives to serve in Crisis management teams. The Crisis management team representatives should be familiar with the relevant Crisismanagement protocol (standard for all PII Entities) and receive regular refresher training.
- *Learn* – Implement procedures for regular incident review, and mechanisms toincorporate lessons learned. Management teams should solicit input from all staff on improvingsecurity risk management and standing guidelines.

We are committed to building and maintaining a positive security culture that enables us to deliver on our organisational strategy. There are certain values and standards that must be acknowledged and incorporated into each element of every local security programme. To achieve this, each Plan International Entity will adhere to the following core principles:

a. Primacy of Life

No Staff, Associates, or Programme Participants should be placed under unnecessary safety and security risk in the course of our work or to protect our assets, property, or reputation. Moreover, any incident responseor Crisis management decisions will prioritise the preservation of life for Staff, Associates, and Programme Participants.

b. Duty of Care

We recognise that we have a duty of care to our Staff, and that our duty of care responsibilities may differ between Staff, Associates, and Programme Participants. Such responsibilities may be defined and limited bycontract, nature of relationship, situational context, and local law as applicable.

To the extent that any Plan International Entity has a duty of care towards any individual in the course of its work, it shall not transfer it to any other entity. In addition, no Plan International Entity shall assume the duty of care of another organisation towards any individual.

Management Responsibility

Staff travelling to or working in the offices of Plan International Entities, programme locations, or offices of partner organisations will at all times adhere to the security procedures of the receiving office (the "Receiving Entity"). In accordance with the principle of Informed Consent, the Receiving Entity will also ensure all staff travelling to or working in the office have access to any security information that is relevant and appropriate for their work.

The Plan International Entity sending Staff (the "Sending Entity") is required to ensure that such Staff are adequately prepared for travel. This may include certain training and/or equipment. Consistent with duty of care requirements, the Sending Entity shall be informed by the Receiving Entity of any security incidents involving their Staff as soon as is practicable. All reasonable efforts will be made to involve the Sending Entity in decisions affecting its Staff during serious incidents or Crisis management situations. Management of an evacuation or relocation of Staff due to a decision to cease operations is the responsibility of the Receiving Entity.

c. Equality

We recognise that Staff and Associates may face, or be vulnerable to, certain safety and security threats due to their individual profile, which may include, but is not limited to, nationality, ethnicity, gender, religion, sexual orientation, gender identity or expression, sex characteristics., ordisability. While we will always strive for equality in our approach to safety and security, there may be circumstances where we are compelled to place restrictions on individual participation in operations when a specific characteristic or intersectionality would pose an unreasonable and unmitigable risk of harm. When possible, additional support, training and mitigation measures will be identified and providedto maintain equality. Review and approval mechanisms must be in place to ensure personal bias is not a factor in imposing restrictions on the grounds outlined above.

d. Informed Consent

Staff and Associates should undertake activities with full knowledge of the threat landscape and the measures we take to mitigate risk. When and where possible, line management or a representative of the Receiving Entity will provide Staff with all relevant information related to safety and security in a location where related factors may affect them or their work. If it is not possible to provide this information, either due to operational barriers or in exceptional circumstances where disclosure could reduce the effectiveness of risk mitigation measures, line management will inform Staff this is the case and ensure reasonable measures are taken to address Staff concerns.

e. Right to Refuse

Staff and Associates have the right to withdraw from a location or refuse to take up work for a Plan International Entity due to concerns about their security or safety if they believe that the identified risks are not sufficiently mitigated.

f. No Right to Remain

Each Plan International Entity retains the right to suspend activities and withdraw or relocate Staff and Associates from operating environments where safety and security risks cannot be adequately managed or mitigated. Under no circumstances will Staff have a right to remain operational in any location where the relevant Plan International Entity has decided to withdraw or relocate. Non-adherence to this principle may result in disciplinary procedures, including termination of employment contract or association with any Plan International Entity, as well as accessto support mechanisms such as insurance, medical treatment, and evacuation. Note that some locally employed staff might live in International, they will not be forced to relocate if they wish to remain.

g. Do No Harm

We shall make all reasonable efforts to ensure that the measures we take to manage safety and security risks never put Programme Participants in greater danger than they would otherwise have been. Similarly, we will take all reasonablemeasures to ensure that locally recruited Staff are not placed at any greater risk due to their association with aPlan International Entity. In situations where operations are suspended or withdrawn due to security risks, we will take all reasonable measures to ensure continued safety and security for locally employed Staff.

h. Acceptance

We recognise that safety and security is greatly enhanced when our Staff and Associates are well integrated into the communities in which we work and where we are valued for our contributions. Therefore, we will always strive to build and maintain acceptance from local authorities, partners, communities and key stakeholders.

However, we recognise that all safety and security risks cannot be managed solely through gaining acceptance. As such, depending on the risks that have been identified and assessed, we may decide to complement the acceptance strategy by implementing additional standard and/or innovative mitigation measures.

i. Health and Well-Being

We acknowledge that support for Staff to manage physical and mental health and well- being is a vital part of effectively managing safety and security risks. This includes providing access tomedical and psychological care, sufficient rest periods during operations in difficult environments and time to recuperate upon return, and peer, management, and professional counselling support followingan incident. In every instance support must be provided by trained and qualified individuals.

j. No Weapons

Staff and Associates shall not take up arms or weapons, and armed personnel will not be allowed in our vehicles or premises, except under extreme circumstances and with explicit authorisation from PII's Chief Executive Officer (or duly authorized representative). In accordance with multiple principles described above, Staff and Associates compelled under duress to allow access to vehicles or premises by armed individuals should make all reasonable efforts to preventsaid access, but should in no way feel obligated to sacrifice their personal safety or well-being.

k. No Armed Elements or Military Assets

When working in the same area as military, police, or armed private security personnel, we will make all reasonable efforts to remain separate and distinct from them.

We recognise there will be some circumstances where it may be necessary to work in conjunction with armed forces or military assets to gain safe access to some areas. In such cases, we will take all necessary steps to ensure the associated risks to Staff, Programme Participants, the local community, and our ongoing operations are minimised. Decisions to work with armed entities can only be authorised by PII's Chief Executive Officer (or duly authorized representative).

l. No Bribes

Staff and Associates shall not offer any rewards, inducements or bribes to any person, group, or organisation. For additional information please refer to the Global Policy on Anti-Fraud, Anti-Bribery and Corruption.

m. No Ransoms

In the event of detention or kidnapping of Staff, we will do everything possible to ensure their release. However, it is our strict policy not to pay any ransom or provide goods under duress.

ROLES AND RESPONSIBILITIES

Our approach to safety and security management is based on shared ownership of risk between management and individual Staff. This enables individuals to feel empowered, leadership to make decisions objectively, and ensures accountability at all levels. However, it must be acknowledged that if leadership or individuals do not meet their obligations or fail to act in good faith with respect to our core principles, then legal, operational, financial, and reputational risks can spread to all Plan International Entities. Violation of these obligations or principles may result in disciplinary action or dismissal.

Individual Responsibilities

All Staff and associates shall ensure they:

- fully comply with this Global Policy and any other context-specific rules and regulations that may be in place when on official business, including when “off duty” while travelling or deployed by Plan International, without exception;
- remain informed about their local security environment and receive the necessary security briefings when travelling;
- conduct themselves in a way that does not reflect negatively on ~~us~~ Plan International or contradict our values and behaviours, and remain aware of their responsibilities under Plan International’s Code of Conduct;
- observe any local laws, and acknowledge local customs and cultural sensitivities; and
- report any security or safety incidents and near misses immediately to management (including any deliberate violations of this Policy or any other context-specific rules or regulations). In the rare instance where immediate reporting of a security or safety incident could place Staff at further risk then reporting can be delayed until it is safe to do so.

Executive and Governance Oversight and Accountability

For PII, the ultimate accountability for safety and security rests with the **Chief Executive Officer.** Routine execution and oversight of associated responsibilities may be delegated as appropriate**.**

PII management will inform the **International Board** about any safety and security risks that have significant implications on PII’s ability to deliver its strategy, as well as incidents resulting in loss of life or serious injury to Staff, Associates, or Programme Participants as a direct result of PII’s operations and where PIIis anticipated to carry some liability or reputational risk. Notification will occur as soon as reasonably possible.

For National Organisations, the ultimate accountability for safety and security rests with the **National Director.** Any safety and security risks that have significant implications on a National Organisation’s ability to deliver its strategy, or any incidents resulting in loss of life or serious injury, will be escalated to the respective governing body of the National Organisation.

The International Board or governing body of a National Organisation may escalate any matters they believe to have substantial impact for all Plan International Entities to the Chair of the **Members’Assembly**.

The relevant governing body will ensure, at a minimum:

- There is a framework of management policies, procedures, tools and resources that support managers and individuals to address safety and security risks;
- Operational management entities are informed of their responsibilities and obligations for managing safety and security risks upon taking up their duties;
- Appropriate services and insurances are in place to provide for medical, psychological, and security support and assistance; and
- Adequate funding to ensure necessary safety and security initiatives are met and the organisation has sufficient capacity to manage serious incidents and crises.

Operational Management and Accountability

PII Chief Executive Officer and National Directors are directly responsible for ensuring that safety and security risks within their areas of jurisdiction are being sufficiently managed in line withthis Global Policy. They will make decisions where there are immediate concerns with the safety and security of their Staff, Associates, and Programme Participants, as well as material assets and reputational issues.

Executive Directors of the Regions have overall responsibility for ensuring safety and security risks within their regions are sufficiently managed in line with this Global Policy. They do this byproviding oversight and guidance to Directors of the Sub-regions and Country Directors andapproval for decisions made in the management of safety and security risk as well as ensure appropriate budget and resources are allocated to offices. Any safety and security risks that negativelyimpacts the ability of PII to deliver on activities within the region must be directly escalated to the Executive Director of the Region.

Country Directors are directly responsible for ensuring that safety and security risks within the relevant country are being sufficiently managed in line with this Global Policy. They have the authority to make decisions where there are immediate concerns with the safety and security of Staff, assets or property. They are responsible for ensuring all essential elements are in place and functioning, appropriate budget and resources are allocated to safety and security, and that the office is compliant with other PII policies or procedures related to safety and security not referenced in this Global Policy.

PII's Director of Safety and Security is responsible for establishing the global safety and security strategy, monitoring the implementation of associated initiatives and polices, providing support to incident response and Crisis management, and acting as a point of escalation for security issues at the regional level. They are authorized to temporarily halt any activities where an identified lapse of security risk management in a Plan International Entity could reasonably result in the loss of life or serious injury to any Staff, Associate, or Programme Participant. They will delegate global responsibilities to the Global Security Advisor or other global security staff as required.

Regional Safety and Security Advisors are responsible for providing advice, guidance, and practical support on all matters of safety and security at the regional level. They will act as points of escalation for **Security Focal Points/Managers** in country offices for all safety and security risks that negatively impact the ability of PII to deliver on activities within the region.

Security Focal Points/Managers will be appointed in each PII office andeach National Organisation to provide support and advice to decision-makers and key stakeholders onmatters of safety and security.

For PII, in high-risk contexts, this position will be filled by a dedicated safety and security professional. In lower-risk contexts management may choose to appoint a part-time focal point, however in such cases management will encourage volunteers to be recruited for the position and the **Regional Safety and Security Advisor** will be included in the selection process.

The Staff mentioned above will ensure, at a minimum:

- The necessary policies, procedures, tools and resources to support Staff, Associates, and Programme Participants and effectively manage safety and security risks are in place;
- Safety and security risks within their areas of jurisdiction have been accurately identified and evaluated in accordance with risk assessment guidelines, and associated mitigation measures are implemented;
- Any measures implemented to mitigate safety and security risk comply with appropriate local or national legislation or regulations;
- Incident reporting mechanisms are established and functioning, and all incidents are properly recorded, reviewed, and widely shared so that lessons learned are incorporated into future operations;
- Incident response and Crisis management protocols are routinely tested or evaluated and necessary insurances, service providers, and resources are in place;
- Incoming Staff and Associates receive a context-specific safety and security briefing within ~~24~~ 48 hours of arrival~~;~~ (24 in high-risk contexts);
- The local security environment is continuously monitored and changes to the standing risk assessment are shared with all Staff and Associates; and
- All Staff and, if required, Associates are appropriately trained for their role and location.

Support Functions

Other departments or teams at PII or National Organisations, such as People and Culture, Global Assurance, Procurement, Legal and Risk Management will have functional interests in ensuring standards are set or achieved within their relevant discipline(s), which contribute to improving the safety and security of Staff, property, assets and organisational reputation, and that these standards are being consistently met. For example, in many offices People and Culture teams are responsible for meeting national health and safety laws.

TERMS AND DEFINITIONS

“Associate” refers to a range of contracted paid and non-paid individuals who have committed to work with or support a Plan International Entity. It includes, among others, board members, volunteers (including community volunteers), interns, sponsors, researchers, donors, consultants and contractors, staff and/or representatives of partner organisations and local governments (when operating in partnership agreement with a Plan International Entity). The extent and limitations of a Plan International Entity’s duty of care towards an Associate with respect to safety and security must be specified in an appropriate contract or agreement between the Plan International entity and the associate.

“Crisis” is defined as an ongoing event or occurrence whose nature, severity or broader consequence for Plan warrants a response beyond the capacity of normal management mechanisms, and therefore requires organisation-wide coordination, management and support. This can include, but is not limited to, detention or abduction of Staff, a complete breakdown of order a country, either as a result of civil unrest or natural disaster, or legal, financial, or reputationalrisks that have the potential to affect the wider organization.

“National Organisation” or “NO” refers to a legal entity that has signed a Members’ Agreement and License Agreement with PII.

“PII” refers to Plan, International, Inc., including when operating through one of its subsidiaries. It generally includes international headquarters, regional offices, liaison offices, and country offices.

“Safety Risk” is defined as a circumstance or set of circumstances that may result in harm against Staff, Associates, Programme Participants, material assets, or organisational reputation that are non-violent in nature oran unintentional act. This includes risks associated with vehicle use and other significant safety risks inthe broader operational context, but is not intended to address compliance with local Health, Safety and Environment legislation. This policy does not address working in infectious disease contexts or health care settings as these policy decisions are managed by public health specialists.

“Security Incident” is defined as an event or occurrence that disrupts or negatively affects normal operations and/or has caused or is likely to cause consequences for Staff, Programme Participants, organisationalreputation, or material assets.

“Security Risk” is defined as a circumstance or set of circumstances that may result in harm against Staff, Associates, Programme Participants, material assets, or organisational reputation that are violent in nature or an intentional act of aggression. This also includes non-violent but intentional acts such as surveillance, harassment of an individual based on any protected characteristic, arbitrary detention, and threat or blackmail against our operations.

“Staff” refers to individuals who receive a regular salary for work in any Plan International Entity as well as individuals paid by or through a Plan International Entity but located in another entity.