



## AFRICAN SAFE MIGRATION INITIATIVE (ASMI-CAMEROUN)

Récépissé de Déclaration d'Association N° 051/RDA/C16/SASC.- du 10 septembre 2026

Siège social : Baressoumtou Aviation (Arrondissement de Nkongsamba 3ème), Département du Moungo, Région du Littoral, Cameroun

# SAFEGUARDING AND DATA PROTECTION POLICY

Safeguarding, PSEA, Child Protection, Survivor Confidentiality, Privacy and Information Security

**APPROVED - EFFECTIVE 3 OCTOBER 2026**

|                     |                                                                                               |
|---------------------|-----------------------------------------------------------------------------------------------|
| Document code       | ASMI-SDP-001                                                                                  |
| Version             | <b>1.0 - APPROVED</b>                                                                         |
| Document owner      | Executive Direction / Secretary General                                                       |
| Technical oversight | Safeguarding Lead: President / Executive Director; Data Protection Officer: MANCHO TEBO SALIF |
| Approval authority  | Executive Bureau - DEC-017/ASMI-CM/BE/2026                                                    |
| Effective date      | 3 October 2026                                                                                |
| Next review         | No later than 3 October 2028, or earlier if required                                          |
| Classification      | Internal - Controlled; safeguarding reports and personal data are confidential                |
| Supersedes          | ASMI-SAF-001 v0.9 DRAFT and ASMI-DAT-001 v0.9 DRAFT                                           |

*Controlled institutional policy approved by the Executive Bureau under Decision DEC-017/ASMI-CM/BE/2026. Printed or downloaded copies are uncontrolled unless entered in the Master Document Control Register.*

## CONTENTS

|    |                                              |    |                                             |
|----|----------------------------------------------|----|---------------------------------------------|
| 1  | Purpose                                      | 23 | Reporting safeguarding concerns             |
| 2  | Institutional and legal basis                | 24 | Immediate danger                            |
| 3  | Scope                                        | 25 | Survivor assistance and referral            |
| 4  | Definitions                                  | 26 | Management response and fair investigation  |
| 5  | Core principles                              | 27 | Personal-data breach response               |
| 6  | Zero tolerance for safeguarding inaction     | 28 | Data protection impact assessment           |
| 7  | Prohibited conduct                           | 29 | Roles and responsibilities                  |
| 8  | Safer recruitment, membership and onboarding | 30 | Partners, contractors and service providers |
| 9  | Programme and field safeguarding             | 31 | Confidentiality and media enquiries         |
| 10 | Child protection                             | 32 | Training                                    |

|           |                                         |                |                                                  |
|-----------|-----------------------------------------|----------------|--------------------------------------------------|
| <b>11</b> | Survivor-centred engagement             | <b>33</b>      | Monitoring and assurance                         |
| <b>12</b> | Data collection and privacy notice      | <b>34</b>      | Discipline and sanctions                         |
| <b>13</b> | Consent                                 | <b>35</b>      | Non-retaliation                                  |
| <b>14</b> | High-risk and sensitive data            | <b>36</b>      | Recordkeeping                                    |
| <b>15</b> | Data Sentinel and research standard     | <b>37</b>      | Policy review                                    |
| <b>16</b> | Digital security and access control     | <b>Annex A</b> | Safeguarding Concern and Immediate-Action Form   |
| <b>17</b> | WhatsApp, email and personal devices    | <b>Annex B</b> | Activity Safeguarding and Data-Risk Assessment   |
| <b>18</b> | Photographs, stories and communications | <b>Annex C</b> | Privacy Notice and Consent Record                |
| <b>19</b> | Data sharing and referrals              | <b>Annex D</b> | Access, Correction or Deletion Request           |
| <b>20</b> | Cross-border data transfer              | <b>Annex E</b> | Personal-Data Breach Report                      |
| <b>21</b> | Data retention and secure disposal      | <b>Annex F</b> | Data Protection Impact Assessment                |
| <b>22</b> | Individual rights                       | <b>Annex G</b> | Safeguarding and Data-Protection Acknowledgement |

## 1. PURPOSE

ASMI-Cameroun works with people who may face heightened vulnerability because of human trafficking, unsafe migration, cyber-employment scams, exploitation, displacement, financial hardship, age, disability, legal or immigration circumstances, or other forms of power imbalance. The organisation therefore has a duty to ensure that its people, programmes, partnerships, communications and data practices do not expose individuals to additional harm.

This Policy establishes a single institutional framework for:

- preventing sexual exploitation, abuse, harassment, child abuse, trafficking, violence, neglect and other safeguarding harm;
- protecting children, survivors and adults at risk;
- ensuring survivor-centred and trauma-informed engagement;
- protecting personal and sensitive information;
- regulating the collection, access, use, analysis, sharing, storage, retention and disposal of personal data;
- preventing unauthorised disclosure, exploitation or misuse of survivor information;
- establishing reporting and response procedures for safeguarding concerns and data incidents;
- strengthening accountability across ASMI-Cameroun programmes, personnel, volunteers, partners and service providers.

ASMI-Cameroun applies a do-no-harm, survivor-centred, data-minimisation and need-to-know approach throughout its work.

## 2. INSTITUTIONAL AND LEGAL BASIS

ASMI-Cameroun is declared under Cameroonian association law as evidenced by Récépissé de Déclaration d'Association N° 051/RDA/C16/SASC.- dated 10 September 2026. The récépissé designates the organisation as African Safe Migration Initiative (ASMI-CAMEROUN) and records its registered office at Baressoumtou Aviation, Arrondissement de Nkongsamba 3ème, Mounjo Division, Littoral Region, Cameroon.

This Policy should be read together with:

- the Statutes of ASMI-Cameroun;
- the Internal Regulations of ASMI-Cameroun;
- the Member Commitment, Conduct, Safeguarding and Confidentiality Charter;
- applicable programme and partnership agreements;
- applicable Cameroonian law;
- donor requirements where applicable.

For data protection, ASMI-Cameroun shall take into account applicable requirements referenced in its existing data-protection framework, including Law No. 2024/017 of 23 December 2024 relating to personal data protection in Cameroon, its implementing requirements and other applicable legal obligations. Legal and regulatory references should be reviewed by a suitably qualified Cameroonian legal adviser before final adoption.

Where a donor or contractual requirement establishes a stronger safeguarding or data-protection standard than this Policy, ASMI-Cameroun should apply the stronger standard to the relevant activity unless it conflicts with applicable law.

## 3. SCOPE

This Policy applies to Executive Bureau members, active members, employees, volunteers, interns, consultants, temporary personnel, researchers and enumerators, contractors and service providers, partner personnel acting on behalf of ASMI-Cameroun, and visitors participating in ASMI activities where appropriate.

It applies across ASMI-related offices, meetings, community outreach, field visits, survivor referrals, training, research, surveys, transport, accommodation, events, websites, social media, WhatsApp, email, KoboToolbox, spreadsheets, databases, Power BI, photographs, videos, partnerships, referrals and other activities undertaken in ASMI-Cameroun's name.

Conduct outside formal working hours may also fall within this Policy when an ASMI relationship, position, beneficiary relationship or access to information is abused.

## 4. DEFINITIONS

| Term                | Meaning                                                                                                                                                   |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Safeguarding</b> | Measures taken to prevent and respond to harm caused or facilitated through ASMI-Cameroun personnel, operations, programmes, relationships or activities. |

| Term                               | Meaning                                                                                                                                                                                                       |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Sexual exploitation</b>         | Actual or attempted abuse of a position of vulnerability, differential power or trust for sexual purposes, including profiting socially, financially or otherwise from another person's sexual exploitation.  |
| <b>Sexual abuse</b>                | Actual or threatened physical intrusion of a sexual nature, whether by force or under unequal, coercive or exploitative circumstances.                                                                        |
| <b>Sexual harassment</b>           | Unwelcome sexual conduct that causes offence, humiliation, intimidation or creates a hostile or unsafe environment.                                                                                           |
| <b>PSEA</b>                        | Prevention of Sexual Exploitation and Abuse.                                                                                                                                                                  |
| <b>Child</b>                       | Any person below the age of 18 years.                                                                                                                                                                         |
| <b>Adult at risk</b>               | An adult whose circumstances, dependency, vulnerability or power imbalance may increase exposure to abuse or reduce the capacity for self-protection.                                                         |
| <b>Survivor-centred approach</b>   | An approach that prioritises the survivor's safety, dignity, rights, wishes, confidentiality, informed choice and wellbeing.                                                                                  |
| <b>Personal data</b>               | Information relating to an identified or identifiable natural person.                                                                                                                                         |
| <b>Sensitive or high-risk data</b> | Information whose disclosure or misuse could expose a person to significant harm, including identity, health, trafficking, sexual-violence, child, location, biometric, legal-status and similar information. |
| <b>Data subject</b>                | The individual to whom personal data relates.                                                                                                                                                                 |
| <b>Data breach</b>                 | Loss, theft, accidental disclosure, unauthorised access, alteration, destruction or unavailability of personal information.                                                                                   |
| <b>Informed consent</b>            | A voluntary, specific and informed agreement given after the individual understands what information will be collected, why, how it will be used, who may receive it and reasonably foreseeable risks.        |

## 5. CORE PRINCIPLES

**Do no harm:** The safety and dignity of the person take priority over publicity, fundraising, data collection, institutional reputation or operational convenience.

**Survivor-centred practice:** Survivors shall be treated with respect, dignity, fairness and without blame or stigma.

**Best interests of the child:** Where a child is involved, the child's safety and best interests shall be a primary consideration.

**Informed choice:** People should understand what ASMI can and cannot do before agreeing to provide information or participate in an activity.

**Confidentiality:** Information shall be shared only with persons who genuinely need it for an authorised purpose.

**Data minimisation:** ASMI shall collect only the information necessary to achieve a clearly defined programme, protection, administrative or evidence objective.

**Purpose limitation:** Information collected for one purpose shall not automatically be used for another unrelated purpose.

**Accuracy:** ASMI shall take reasonable steps to ensure material information is accurate and updated when necessary.

**Storage limitation:** Personal data shall not be retained indefinitely without a valid operational, legal, contractual or safeguarding reason.

**Accountability:** ASMI must be able to explain why information was collected, who accessed it, how it was protected, why it was shared and when it should be deleted.

**Non-discrimination:** No person shall be treated unfairly because of nationality, sex, gender, disability, ethnicity, language, religion, immigration circumstances, economic situation or other personal status.

**Non-retaliation:** No person acting in good faith shall face retaliation for raising a safeguarding, ethics or data-protection concern.

## 6. ZERO TOLERANCE FOR SAFEGUARDING INACTION

ASMI-Cameroun has zero tolerance for inaction toward credible safeguarding concerns. Every credible report of sexual exploitation, abuse, harassment, violence, trafficking, child abuse, neglect or other serious harm must receive a timely, survivor-centred and fair response.

This does not mean that an allegation automatically establishes guilt. ASMI-Cameroun shall respect fairness, confidentiality and due process while taking proportionate measures to protect people from further harm.

## 7. PROHIBITED CONDUCT

- engaging in sexual exploitation or abuse;
- engaging in sexual activity with a child under any circumstances;
- exchanging money, employment, assistance, transport, referrals, documents, opportunities or preferential treatment for sex or sexualised conduct;
- grooming or sending sexualised communications to children or vulnerable beneficiaries;
- producing, possessing or distributing child sexual-abuse material;
- facilitating trafficking, forced labour or exploitation;
- physically or emotionally abusing beneficiaries;
- humiliating, intimidating, bullying, harassing or discriminating against another person;
- retaliating against a complainant, survivor, witness or whistleblower;
- undertaking unnecessary secretive or private contact with children;
- transporting or accommodating a child privately without an authorised safeguarding arrangement;
- exploiting ASMI position or access for personal gain;
- publishing survivor identities or case details without appropriate informed consent and risk review;
- accessing information that is not required for assigned duties;
- sharing confidential information with unauthorised persons;
- copying confidential ASMI data to personal email, unauthorised cloud storage or unapproved systems;
- providing identifiable survivor information to media, friends, relatives or social-media audiences without authorisation.

## 8. SAFER RECRUITMENT, MEMBERSHIP AND ONBOARDING

ASMI-Cameroun shall apply proportionate safeguarding and confidentiality controls when recruiting personnel, admitting active members or engaging volunteers. These may include:

- identity verification;
- reference checks where appropriate;
- assessment of conflicts of interest;
- safeguarding questions during recruitment;
- review for known links with trafficking, fraudulent recruitment or migration-facilitation networks where reasonably possible;
- signing of the Member Commitment, Conduct, Safeguarding and Confidentiality Charter;
- safeguarding and data-protection orientation;
- clear role descriptions and authority limits;
- access restrictions based on assigned duties.

No new member or volunteer shall automatically receive access to sensitive survivor information merely because they have joined ASMI-Cameroun. Access must follow role necessity.

## 9. PROGRAMME AND FIELD SAFEGUARDING

Before community outreach, survivor engagement, field research, transport, events, distributions or similar activities, the responsible programme lead shall assess relevant risks, including participant vulnerability, venue safety, privacy, transport, crowd management, gatekeeper power, sexual exploitation or extortion, photography, data collection, partner conduct, emergency contacts and reporting mechanisms.

---

ASMI shall, as far as reasonably possible:

- use visible and professional interactions;
- avoid unnecessary one-to-one contact with children;
- avoid repeated questioning of survivors;
- avoid collecting survivors or children from homes without an approved reason and consent;
- provide safe reporting options;
- ensure staff understand their roles before field activities;
- stop or modify activities where serious unmanaged risks are identified.

## 10. CHILD PROTECTION

---

When engaging with a child, ASMI-Cameroun shall:

- make the child's best interests a primary consideration;
- communicate in an age-appropriate manner;
- obtain appropriate consent and/or assent as required by the circumstances and applicable law;
- minimise questioning;
- avoid coercion, punishment, shame or sexualised language;
- avoid publishing the child's full name, school, exact location, migration history or other identifying information;
- ensure photographs or recordings undergo specific consent and safeguarding review;
- limit child-related information to authorised persons.

No member may privately promise a child employment, money, migration assistance, travel opportunities, visas or other benefits on behalf of ASMI-Cameroun without confirmed institutional authority and resources.

## 11. SURVIVOR-CENTRED ENGAGEMENT

---

ASMI personnel shall listen without blame or judgment. Survivors shall not be pressured to identify an alleged trafficker, speak publicly, appear in photographs, participate in fundraising, contact police or family members, participate in an investigation, or provide more information than is necessary.

Before collecting case information, ASMI should explain why the information is requested, how it may be used, who may access it, possible limits to confidentiality, whether participation is optional and what assistance ASMI can realistically provide.

ASMI shall never promise money, tickets, visas, repatriation, employment, medical assistance or other support unless confirmed resources and institutional authority exist.

## 12. DATA COLLECTION AND PRIVACY NOTICE

---

Before collecting personal information, ASMI-Cameroun should identify the purpose of collection, the minimum information required, persons affected, authorised users, intended recipients, retention requirements, potential risks, and the appropriate lawful basis or consent mechanism.

Where reasonably possible, the person should be informed of ASMI-Cameroun's identity, the reason for collection, which fields are required or optional, intended use, potential recipients, possible cross-border transfers, retention arrangements, available rights, and how to raise a complaint or concern. Information should be provided in English, French or another accessible format where reasonably necessary.

## 13. CONSENT

---

Consent must be specific, informed, understandable, voluntary, recorded where appropriate, and capable of being withdrawn for future consent-based processing. ASMI must not treat silence as consent or unnecessarily bundle unrelated optional purposes.

Separate consent should normally be considered for:

- survivor case management;
- referral to another organisation;
- cross-border data sharing;
- photography and video;
- media or storytelling;
- research;
- publication;
- direct fundraising communications.

Consent is not the only possible legal basis for processing. Where another lawful basis is relied upon, ASMI shall document the justification and relevant safeguards.

---

## 14. HIGH-RISK AND SENSITIVE DATA

Information relating to trafficking survivors, children, sexual violence, identity documents, health, legal status and precise locations requires heightened protection. ASMI shall:

- restrict access to named authorised persons;
- separate direct identifiers from analytical data where feasible;
- use unique case references instead of names in broad registers;
- avoid putting survivor names in email subject lines and filenames;
- limit downloaded copies;
- review access regularly;
- delete duplicates when no longer required;
- use aggregation or anonymisation for reporting whenever possible;
- review precise locations and small statistical categories for re-identification risk before publication.

---

## 15. DATA SENTINEL AND RESEARCH STANDARD

ASMI-Cameroun's Data Sentinel approach shall prioritise aggregated prevention intelligence over unnecessary identifiable survivor data. Research, surveys and dashboards must have a clear decision or prevention purpose.

Before collection, programme and data personnel should determine:

- what decision the data will support;
- what indicators are necessary;
- which information is genuinely required;
- how respondents will be informed;
- how confidentiality will be protected;
- how data quality will be assessed;
- how findings will be anonymised or aggregated;
- when identifiable source data should be deleted.

Where possible, ASMI should analyse scam typologies, recruitment methods, routes, risk patterns, demographic trends, geographic risk levels and prevention indicators without publishing identifiable survivor information.

---

## 16. DIGITAL SECURITY AND ACCESS CONTROL

Access shall be based on minimum role necessity. ASMI users must:

- use individual accounts wherever possible;
- use strong passwords;
- use multi-factor authentication where available;
- never share passwords, authentication codes or access tokens;
- lock devices when unattended;
- keep devices updated;
- verify recipients before sending sensitive information;
- avoid public Wi-Fi for highly sensitive work unless appropriate security measures are available;
- report lost or stolen devices promptly;
- avoid storing sensitive organisational information on personal devices unless authorised.

Generic accounts and unrestricted shared folders should be avoided for confidential information. Access to restricted data shall be reviewed at least quarterly and whenever a person changes role, leaves ASMI or no longer requires access.

---

## 17. WHATSAPP, EMAIL AND PERSONAL DEVICES

WhatsApp and similar platforms may be used for operational coordination but should not become permanent repositories for detailed survivor case information.

Personnel shall not unnecessarily share passport images, national identity cards, medical records, exact survivor addresses, immigration records or highly detailed survivor histories in general WhatsApp groups.

Where urgent information must be communicated digitally, share only the minimum information necessary, use the smallest authorised recipient group, remove unnecessary copies where appropriate, and transfer the official record to ASMI's approved secure system. Sensitive case information must never be posted in the general ASMI-Cameroun WhatsApp group or public Community channels.

---

## 18. PHOTOGRAPHS, STORIES AND COMMUNICATIONS

---

Survivor dignity and safety take priority over communication and fundraising objectives. ASMI shall not publish identifiable survivor photographs, stories, names, exact locations or case histories without specific informed consent, an assessment of foreseeable harm and approval through the appropriate internal communication and safeguarding process.

Consent for receiving assistance does not constitute consent for publicity. Children require enhanced safeguards. Even with consent, ASMI may decide not to publish information where the safeguarding risk remains too high.

---

## 19. DATA SHARING AND REFERRALS

---

Before sharing personal information externally, ASMI should verify the recipient, the recipient's authority, the purpose, the minimum required information, consent or another lawful basis, security of the transmission method and any restrictions on further use.

Where ASMI makes a referral to another organisation, only information necessary for that referral should be transferred. Partners and providers receiving ASMI-controlled personal data should be subject, where appropriate, to written confidentiality and data-protection obligations.

---

## 20. CROSS-BORDER DATA TRANSFER

---

Because ASMI-Cameroun may work on transnational trafficking and migration matters, personal information may sometimes need to be shared across borders. Before transferring high-risk personal information outside Cameroon, ASMI should assess necessity, recipient, destination, legal and institutional safeguards, security arrangements, survivor safety, and the relevant consent or lawful basis. Cross-border sharing shall be limited to what is necessary.

---

## 21. DATA RETENTION AND SECURE DISPOSAL

---

Each important dataset should have an owner, purpose, retention trigger, retention period and disposal method. ASMI shall periodically review active survivor and high-risk datasets.

Duplicate passport copies, identity documents, exports and downloads should be deleted when they are no longer required. Where a complaint, audit, legal matter or investigation requires preservation, relevant records may be placed on legal or administrative hold. Paper records containing confidential information shall be securely destroyed when disposal is authorised. Anonymised statistics may be retained for longer periods where re-identification risk is sufficiently reduced.

---

## 22. INDIVIDUAL RIGHTS

---

Where applicable under law and ASMI procedures, individuals may request information about how their personal information is used, access to their information, correction of inaccurate information, restriction or objection, or deletion where appropriate.

Identity shall be verified proportionately before releasing information. ASMI shall not reveal information concerning another survivor, witness, reporter or third party simply because a request is received. Complex requests shall be escalated to the Data Protection Officer and, where necessary, qualified legal advice.

---

## 23. REPORTING SAFEGUARDING CONCERNS

---

Safeguarding concerns may be reported to the Safeguarding Lead (President / Executive Director), the Secretary General, another non-conflicted Executive Bureau member, the official ASMI-Cameroun email, or another officially designated confidential reporting channel. Where a report involves one of these persons, the matter shall be directed to another non-conflicted authorised person.

Serious safeguarding concerns should be escalated immediately and, as an internal standard, no later than 24 hours after receipt where reasonably possible. The receiving person shall:

- listen calmly;
- prioritise immediate safety;
- collect only information necessary for protection and routing;
- avoid investigating during initial disclosure;
- avoid confronting the alleged person;
- avoid promising absolute secrecy;
- explain confidentiality limits;
- record the concern under a restricted reference;
- refer the matter to authorised safeguarding leadership.

---

## 24. IMMEDIATE DANGER

Where there is credible immediate danger, urgent medical need or serious threat to a child or adult at risk, ASMI shall prioritise safety. Emergency or trusted protection services may be contacted where appropriate, with the informed participation of the affected person wherever reasonably possible and consistent with applicable legal duties.

Any disclosure without consent because of an urgent lawful necessity must be limited to the minimum information required and documented.

---

## 25. SURVIVOR ASSISTANCE AND REFERRAL

ASMI may provide information and referral options concerning psychosocial support, legal assistance, protection, shelter, medical services, security, reintegration services, competent authorities and humanitarian organisations.

ASMI shall explain, where known, eligibility, potential cost, provider confidentiality practices and reporting obligations. Referral shall not be conditioned on participation in an ASMI investigation. Follow-up should use the contact method and time considered safe by the survivor.

---

## 26. MANAGEMENT RESPONSE AND FAIR INVESTIGATION

Where a serious safeguarding allegation concerns ASMI personnel or operations, the Executive Bureau shall ensure an appropriately independent and competent response. This may include appointment of a non-conflicted decision lead, a trained investigator and external professional support where appropriate.

- Interim protective measures may be applied without presuming guilt.
- Support records should, where feasible, remain separate from disciplinary or investigative files.
- Investigations should minimise repeated interviews, protect confidentiality, give the person concerned a fair opportunity to respond at an appropriate stage, preserve evidence, and document findings and reasons.
- Internal administrative findings do not replace criminal determinations by competent authorities.

---

## 27. PERSONAL-DATA BREACH RESPONSE

Anyone who suspects a data breach must report it immediately. Examples include sending a case file to the wrong person, losing a phone containing survivor information, unauthorised access to Drive, accidental public sharing, stolen credentials, loss of paper files or unauthorised publication of survivor details.

### 27.1 Containment

Stop further disclosure, revoke access, recover messages or devices where safe, change credentials where necessary and preserve evidence.

### 27.2 Internal notification

Notify the Data Protection Officer and the responsible institutional authority immediately.

### 27.3 Risk assessment

Assess the information involved, number and type of persons affected, whether survivors or children are involved, likely physical, financial, discriminatory, legal or reputational harm, whether the information has been recovered and whether cross-border exposure occurred.

### 27.4 Notification

Determine whether affected persons, authorities, donors, partners or other parties must be notified under applicable law or agreement.

### 27.5 Corrective action

Document root cause, corrective action, responsible person and deadline. No person shall conceal a data breach to avoid embarrassment or disciplinary action. Good-faith reporting of an error shall be encouraged.

---

## 28. DATA PROTECTION IMPACT ASSESSMENT

A Data Protection Impact Assessment should be completed before introducing processing that may create significant privacy or safeguarding risks, including large-scale sensitive-data collection, systematic collection involving children, biometric data, automated profiling, public risk dashboards using granular information, dataset matching, cross-border case-management platforms or new digital tools handling survivor data.

The assessment should examine purpose and necessity, data flow, people affected, systems and providers, access, sharing, retention, threats, likelihood and severity of harm, controls and remaining risk. A project with unresolved high risk should not proceed without appropriate Executive Bureau consideration and any legally required review.

---

## 29. ROLES AND RESPONSIBILITIES

---

### 29.1 Executive Bureau

- approve this Policy;
- provide oversight;
- ensure serious incidents are addressed;
- approve major corrective action;
- ensure appropriate resources and responsibilities are assigned.

### 29.2 President / Executive Director

- provide executive oversight;
- ensure implementation across ASMI operations;
- authorise appropriate institutional responses;
- ensure survivor protection takes priority over publicity or institutional convenience;
- ensure conflicts of interest are managed.

### 29.3 Secretary General

- support controlled documentation and confidential recordkeeping;
- maintain policy administration, incident and decision records;
- support institutional compliance and secure archives;
- coordinate secure records and institutional compliance with the Data Protection Officer.

### 29.4 Safeguarding Lead / Executive Direction

- receive and securely route safeguarding concerns;
- support risk assessments and immediate safeguarding action;
- maintain restricted safeguarding records;
- advise programmes on safeguarding controls;
- support safeguarding training.

### 29.5 Data Protection Officer

- The designated Data Protection Officer, MANCHO TEBO SALIF, shall maintain data-processing records;
- advise on privacy risks and high-risk processing;
- coordinate data-breach response;
- support individual-rights requests and access reviews;
- support training.

### 29.6 Programme and Data / M&E Personnel

- integrate safeguarding and privacy into programme design;
- minimise unnecessary data collection;
- ensure field teams understand reporting duties;
- complete relevant risk assessments;
- apply data-minimisation and anonymisation;
- maintain data quality and restrict identifiable datasets;
- review dashboards for re-identification risk.

### 29.7 All Members and Volunteers

- comply with this Policy;
- protect confidential information;
- respect safeguarding boundaries;
- report serious concerns and data breaches;
- use information only for assigned duties;
- participate in required training;
- cooperate with authorised safeguarding and data-protection measures.

---

## 30. PARTNERS, CONTRACTORS AND SERVICE PROVIDERS

---

ASMI-Cameroun should assess safeguarding and data-protection risks before sharing sensitive information with partners or service providers. Where appropriate, agreements should address confidentiality, safeguarding standards, permitted use of information, access controls, security, incident reporting, further sharing, return or deletion of information, and cooperation with legitimate investigations or data-rights requests.

ASMI may suspend a referral or data-sharing relationship where credible unmanaged risks to beneficiaries exist.

---

## 31. CONFIDENTIALITY AND MEDIA ENQUIRIES

---

Safeguarding reports, survivor case information and personal data shall not be discussed casually within or outside the organisation. No ASMI member shall make a public statement confirming a survivor's identity, confidential allegations, the identity of a complainant or restricted case information unless specifically authorised and legally appropriate. Media enquiries concerning safeguarding matters shall be directed to the authorised institutional spokesperson.

---

## 32. TRAINING

---

Before receiving unsupervised access to survivor information, children, adults at risk or restricted databases, relevant personnel shall receive appropriate orientation covering safeguarding, PSEA, child protection, confidentiality, safe referral, data protection, digital security, reporting procedures and survivor-centred communication. Refresher training should be conducted periodically and following major policy changes or incidents.

---

## 33. MONITORING AND ASSURANCE

---

ASMI-Cameroun should periodically review access permissions, safeguarding incidents, data breaches, programme risk assessments, consent practices, retention schedules, partner compliance, training completion and corrective actions. Safeguarding and data trends may be analysed for organisational learning, but reports used for learning should be anonymised or aggregated wherever possible.

---

## 34. DISCIPLINE AND SANCTIONS

---

Violations of this Policy may result in measures including verbal or written warning, restriction or withdrawal of data access, removal from an activity, temporary suspension, membership disciplinary action, contract termination, dismissal where applicable, or referral to competent authorities where legally appropriate.

Serious misconduct includes sexual exploitation or abuse, child abuse, retaliation, deliberate confidentiality breaches, deliberate unauthorised disclosure of survivor information, interference with safeguarding investigations, concealment of serious incidents, and misuse of personal information for private gain. Sanctions shall be applied consistently with ASMI-Cameroun's Statutes, Internal Regulations, contractual obligations and due-process requirements.

---

## 35. NON-RETALIATION

---

No person shall be punished, threatened, harassed or disadvantaged for making a safeguarding, privacy or ethics report in good faith. Knowingly false or malicious allegations may themselves be addressed under applicable disciplinary procedures, but an allegation that cannot be substantiated is not automatically malicious.

---

## 36. RECORDKEEPING

---

Safeguarding and data-protection records shall use unique references wherever possible. ASMI should maintain separate restricted records for safeguarding concerns, survivor support, investigations, data breaches, consent records, rights requests and high-risk data assessments. Access shall be limited to authorised persons.

---

## 37. POLICY REVIEW

---

This Policy shall be reviewed at least every 24 months, following major legal changes, after a serious safeguarding or data incident, when ASMI materially changes its programmes or data systems, or when donor or regulatory requirements require revision. Material amendments require appropriate institutional approval.

## ANNEX A - SAFEGUARDING CONCERN AND IMMEDIATE-ACTION FORM

Purpose: Captures only information needed to protect the person at risk and route the concern safely. This form is confidential and restricted.

| Field / Information                                             | Response |
|-----------------------------------------------------------------|----------|
| Restricted reference; no name in filename                       |          |
| Date, time, channel and receiving person                        |          |
| Person at risk / reference ID and safe contact method           |          |
| Concern in reporter's or survivor's own words                   |          |
| Immediate danger, child-protection, medical or retaliation risk |          |
| Alleged person's relationship to ASMI, if known                 |          |
| Consent and confidentiality limits explained                    |          |
| Immediate safety / referral action                              |          |
| Person notified and secure record location                      |          |

Declaration: I recorded the information as received, did not promise absolute confidentiality and did not undertake an unauthorised investigation.

| Role                                         | Name / Signature / Date |
|----------------------------------------------|-------------------------|
| Receiving person                             |                         |
| Safeguarding Lead / non-conflicted authority |                         |

## ANNEX B - ACTIVITY SAFEGUARDING AND DATA-RISK ASSESSMENT

| Field / Information                                                 | Response |
|---------------------------------------------------------------------|----------|
| Activity, location, dates and lead                                  |          |
| Participants: children, adults at risk, survivors or general public |          |

| Field / Information                                                 | Response                           |
|---------------------------------------------------------------------|------------------------------------|
| Venue, one-to-one interaction, selection, transport and crowd risks |                                    |
| Privacy, photography, digital, data and location risks              |                                    |
| Partner, vendor and referral risks                                  |                                    |
| Controls, responsible person and deadline                           |                                    |
| Reporting and emergency contacts                                    |                                    |
| Residual risk                                                       | Low / Moderate / High              |
| Decision                                                            | Proceed / Modify / Stop / Escalate |

| Role                  | Name / Signature / Date |
|-----------------------|-------------------------|
| Activity lead         |                         |
| Safeguarding reviewer |                         |
| Authorised approver   |                         |

## ANNEX C - PRIVACY NOTICE AND CONSENT RECORD

| Field / Information                    | Response |
|----------------------------------------|----------|
| Activity / project and ASMI data owner |          |
| Information collected and purpose      |          |
| Required versus optional fields        |          |
| Potential recipients                   |          |
| Cross-border sharing, if applicable    |          |
| Retention arrangement                  |          |

| Field / Information                      | Response                                                                                                 |
|------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Rights, complaint and safe contact route |                                                                                                          |
| Separate consent choices                 | Case management / Referral / Research / Photography / Video / Publication / Cross-border sharing / Other |

Declaration: I received information in a language and format I understand. I understand the stated purposes and the choices available to me.

| Role                                 | Name / Signature / Date |
|--------------------------------------|-------------------------|
| Data subject / lawful representative |                         |
| ASMI receiving person                |                         |
| Interpreter / witness, if used       |                         |

## ANNEX D - ACCESS, CORRECTION OR DELETION REQUEST

| Field / Information                                    | Response                                                               |
|--------------------------------------------------------|------------------------------------------------------------------------|
| Request reference and date                             |                                                                        |
| Requester and proportionate identity verification      |                                                                        |
| Nature of request                                      | Access / Correction / Deletion / Restriction / Objection / Information |
| Exact scope                                            |                                                                        |
| Systems / projects searched                            |                                                                        |
| Third-party, safeguarding or legal-hold considerations |                                                                        |
| Decision and action                                    |                                                                        |
| Date response issued                                   |                                                                        |
| Complaint / escalation route                           |                                                                        |

| Role | Name / Signature / Date |
|------|-------------------------|
|------|-------------------------|

| Role                    | Name / Signature / Date |
|-------------------------|-------------------------|
| Request handler         |                         |
| Data Protection Officer |                         |

## ANNEX E - PERSONAL-DATA BREACH REPORT

| Field / Information                                                     | Response |
|-------------------------------------------------------------------------|----------|
| Incident ID, discoverer and discovery time                              |          |
| System, device or record involved                                       |          |
| What happened and whether ongoing                                       |          |
| Data categories, people and approximate volume                          |          |
| Children, survivors or other high-risk persons involved                 |          |
| Containment and evidence preserved                                      |          |
| Potential physical, financial, legal, discrimination or reputation risk |          |
| Notifications made / required and rationale                             |          |
| Root cause, corrective action, owner and deadline                       |          |

| Role                    | Name / Signature / Date |
|-------------------------|-------------------------|
| Incident lead           |                         |
| Data Protection Officer |                         |
| Executive authority     |                         |

## ANNEX F - DATA PROTECTION IMPACT ASSESSMENT

| Field / Information                               | Response                                               |
|---------------------------------------------------|--------------------------------------------------------|
| Project, owner and proposed launch date           |                                                        |
| Purpose, necessity and alternatives               |                                                        |
| People affected, data flow, systems and providers |                                                        |
| Lawful basis, consent and notice                  |                                                        |
| Access, sharing, transfer and retention           |                                                        |
| Threats, likelihood, severity and affected rights |                                                        |
| Controls and residual risk                        |                                                        |
| Consultation and unresolved issues                |                                                        |
| Decision                                          | Approve / Approve with modifications / Escalate / Stop |

| Role                    | Name / Signature / Date |
|-------------------------|-------------------------|
| Project owner           |                         |
| Data Protection Officer |                         |
| Safeguarding reviewer   |                         |
| Executive approver      |                         |

## ANNEX G - SAFEGUARDING AND DATA-PROTECTION ACKNOWLEDGEMENT

I confirm that I have received and understood the ASMI-Cameroun Safeguarding and Data Protection Policy. I understand that I must protect survivor and beneficiary confidentiality; never exploit, abuse, harass, groom or retaliate; protect children and adults at risk; collect only information necessary for authorised duties; not share confidential information without authority; report safeguarding concerns and data breaches promptly; and cooperate with authorised safeguarding and data-protection measures.

| Field                                | Response |
|--------------------------------------|----------|
| Name                                 |          |
| Role / Function                      |          |
| Member / Personnel ID, if applicable |          |
| Signature                            |          |
| Date                                 |          |
| Supervisor / Orientation Officer     |          |
| Supervisor Signature / Date          |          |

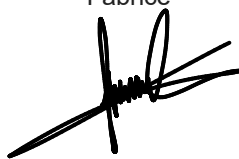
## APPROVAL AND ENTRY INTO FORCE

This Policy was formally approved by the ASMI-Cameroun Executive Bureau on 3 October 2026 under Decision DEC-017/ASMI-CM/BE/2026 and enters into force on the same date. It supersedes the separate draft safeguarding and data-protection policies identified in the document-control section and shall be recorded in the Master Document Control Register.

| Approval record         | Details                 |
|-------------------------|-------------------------|
| Decision No.            | DEC-017/ASMI-CM/BE/2026 |
| Meeting / Decision Date | 3 October 2026          |
| Effective Date          | 3 October 2026          |

## Statutory signatories / responsible officers

The President and Secretary General below are statutory officeholders recorded on Récépissé de Déclaration d'Association N° 051/RDA/C16/SASC.-. MANCHO TEBO SALIF is designated as Data Protection Officer by DEC-017/ASMI-CM/BE/2026; this is an operational appointment and does not amend the statutory composition of the Bureau Exécutif.

|                                                                                                                  |                                                                                                                                |                                                                                                            |
|------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| M. ACHU NGANDO<br>Fabrice<br> | Mme NKODJOU JAMBWE<br>Ilarie Bongevanie<br> | MANCHO TEBO SALIF<br> |
|------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|

**ASMI-CAMEROUN**

Data • Prevention • Protection | Safe Migration. Secure Future.