

Safeguarding & Protection

1. Child Protection & Safeguarding Policy
2. SEA Prevention & Response Policy
3. Survivor-Centred Response SOP
4. Safe Recruitment & Vetting SOP
5. Incident Reporting & Case Management SOP

Approved by: **National Board**

Updated: 2026-03-01

Review cycle: **Annual** (or earlier if legislation or practice changes)

Chapter 1. Child Protection & Safeguarding Policy

1) Policy Statement & Purpose

Labdaros ir paramos fondas „Adliga women at risk solidarity fund“ (hereafter “Adliga” or the Organization) is committed to creating and maintaining the safest possible environment for every child we engage with—directly or indirectly—through our programs, services, advocacy, communications, and partnerships. We uphold the United Nations Convention on the Rights of the Child (UNCRC), the EU Charter of Fundamental Rights, the General Data Protection Regulation (GDPR), and applicable laws of the Republic of Lithuania, including the Law on Fundamentals of Protection of the Rights of the Child and relevant criminal, social, and data-protection legislation.

Purpose. This Policy sets out our principles, standards, roles, and procedures for preventing and responding to abuse, neglect, exploitation, and all forms of harm. It defines how we:

- prevent risks through safer recruitment, training, program design, and culture;

- identify, report, and respond to concerns in a survivor-centred, child-friendly way; and
- meet our legal and ethical duties, including information-sharing, data protection, monitoring, and accountability.

Non-negotiables. We operate a **zero-tolerance** approach to abuse, exploitation, and retaliation against reporters/whistleblowers. Concerns will be acted upon **immediately** and in line with this Policy.

2) Scope

This Policy applies to all who work with or represent “” in any capacity:

- employees, board members, paid consultants;
- interns and volunteers (including ad-hoc event volunteers);
- contractors, vendors, photographers/filmmakers, translators;
- partner organizations and their staff when working on “Adliga” activities;
- any person engaged by or representing the Organization in activities involving children.

Compliance with this Policy is a condition of engagement. Breaches may result in removal from activities, termination of contracts, and/or referral to authorities.

3) Definitions (Plain Language)

- **Child:** any person under **18 years** of age.
- **Safeguarding/Child Protection:** all measures to prevent and respond to abuse, neglect, exploitation, or harm to children.
- **Abuse:** includes **physical, emotional/psychological, sexual** abuse, **neglect, grooming, online abuse, bullying, trafficking, sexual exploitation, child labour**, and **exposure to violence**.
- **PSEA (Protection from Sexual Exploitation & Abuse):** safeguarding against sexual exploitation/abuse perpetrated by staff, volunteers, partners, or others in a position of power.
- **Designated Safeguarding Lead (DSL) / Child Protection Officer (CPO):** named person with delegated responsibility for implementation, advice, and case management coordination.

- **Significant Harm:** a threshold indicating serious impact on health or development requiring urgent action.

4) Legal & Standards Framework

We align with:

- **UNCRC** and Optional Protocols;
- **Council of Europe** and **EU** child protection standards;
- **EU GDPR** and Lithuanian data-protection law;
- **Republic of Lithuania laws** on child rights protection, criminal law relating to offences against children, domestic violence, and labour/volunteering;
- **Good practice** guidance from international child-safeguarding bodies (e.g., Keeping Children Safe, Inter-agency standards).

Note: Where standards differ, **the higher standard applies**. For cross-border activities, we comply with local law **and** this Policy.

5) Roles & Responsibilities

- **National Board:** approves the Policy, ensures resourcing, receives annual safeguarding reports, and oversees serious incident notifications.
- **Executive Director:** accountable for implementation; appoints the **DSL/CPO**; ensures safe systems and culture.
- **DSL/CPO:** leads on prevention, advice, training, risk assessment, incident intake, referrals, liaison with authorities, documentation, and case reviews.
- **Safeguarding Committee** (min. 3 members incl. DSL, HR, Program Lead): reviews complex cases, oversees investigations, recommends actions, and monitors lessons learned.
- **Managers & Project Leads:** ensure risk assessments, safe staffing ratios, supervision, and compliance in their teams and events.
- **All Staff/Volunteers/Partners:** must follow the **Code of Conduct**, complete training, maintain professional boundaries, and **report concerns immediately**.

6) Code of Conduct (Standards of Behaviour)

All representatives must:

1. **Treat children with dignity and respect** at all times; use child-friendly, non-violent, non-discriminatory language.
2. **Prioritise safety:** follow risk assessments, supervision ratios, and site rules; stop or modify activities if risks emerge.
3. **Maintain professional boundaries:** no favouritism, gifts of significant value, lending/borrowing money, or private 1:1 meetings in non-public spaces.
4. **No physical punishment or degrading treatment.** Any necessary physical contact must be **appropriate, time-limited**, and for **safety or care** only.
5. **No sexual activity or romantic relationship** with a child or anyone under 18; **no sexualised communication** (including jokes, emojis, images).
6. **No alcohol/drugs** while responsible for children; never be under the influence during activities.
7. **Digital safety:** do not **friend/follow** children from personal accounts; use approved channels; no private messaging; comply with media/consent rules.
8. **Transport & visits:** follow transport policy; never transport a child alone unless **risk-assessed and authorised**; no home visits without prior approval, consent, and supervision plan.
9. **Media & images:** obtain written, informed consent from parent/guardian (and assent from the child); avoid identifying details; store securely; permit withdrawal of consent.
10. **Report concerns immediately** to the DSL/CPO—even if uncertain; **do not** promise secrecy.

Prohibited Conduct (examples): hitting, ridiculing, shaming; sexual conversations; giving personal contact details; sharing explicit material; photographing children without consent; taking children to your home; sleeping in the same room/tent; facilitating access to harmful content; retaliation against complainants.

7) Safer Recruitment & Vetting

- **Role design & advertising:** include safeguarding responsibilities and screening requirements.
- **Applications:** require a **self-declaration** of criminal history and conflicts of interest; collect complete work/volunteer history with gaps explained.
- **Interviews:** include safeguarding questions and scenario tests.
- **References:** obtain **two** written references including most recent employer/organization; verify authenticity.
- **Criminal record checks:** request appropriate **police clearance**/record extracts per Lithuanian and EU law; for non-Lithuanian nationals, request equivalent from country of origin/recent residence where feasible.
- **Eligibility:** exclude individuals barred by law from working with children or with relevant convictions/disciplinary findings.
- **Probation:** safeguarding conduct assessed during probation; unsatisfactory conduct results in termination.
- **Renewal:** re-checks for long-term staff/volunteers per risk profile (e.g., every 3 years).

8) Induction, Training & Culture

- **Induction:** all joiners receive the Policy, Code of Conduct, local referral pathways, and reporting channels; sign **Acknowledgement**.
- **Mandatory training:** safeguarding & PSEA, recognising abuse, boundaries, online safety, reporting, data protection, disability & inclusion, trauma-informed care.
- **Refresher:** at least **every 24 months** (or earlier after incidents or changes).
- **Specialist training:** for DSL/Committee; for roles with higher risk (drivers, camp leaders, media teams).
- **Culture:** leadership models safe behaviour; routine **toolbox talks** at events; visible posters with contact details; anonymous reporting options.

9) Safe Programming Standards

9.1 Risk Assessment

Before every project/event, complete and approve a **written risk assessment** considering location, activities, participant profiles (age, disability, language, trauma), staffing, transport, accommodation, weather, medical needs, and data handling.

9.2 Supervision & Ratios (minimums)

- Always **two approved adults** present (no 1:1 out of sight).
- **Ages 5-10:** 1 adult per **8** children (minimum 2 adults).
- **Ages 11-17:** 1 adult per **10** children (minimum 2 adults).
- For mixed-gender groups, include **at least one female** supervisor; adjust ratios for children with disabilities, higher-risk activities, or trips.

9.3 Venue & Activity Safety

Safe premises; separate toilets for adults/children (or controlled access); first-aid kit and trained first-aider; incident/missing-child procedures; accessible spaces and reasonable accommodations.

9.4 Physical Contact

Only when necessary for **care/safety**; explain what you are doing; seek assent; keep contact **observable**; record any unusual contact.

9.5 Transport & Trips

Parental/guardian consent and medical information required; approved drivers only; seatbelts/child seats; no lone transport; pre-agreed routes and check-in; emergency contact list.

9.6 Residential/Overnight

Separate sleeping arrangements by age/sex; staff rooms separate; curfew and supervision plan; safeguarding briefing; visitors controlled; lights-out checks by two adults.

9.7 Inclusion & Accessibility

Non-discrimination in access; reasonable accommodations; child-friendly information; interpreters as needed; attention to refugees, migrants, minority children, and children with disabilities; zero tolerance for bullying.

9.8 Cash/Material Assistance

Transparent eligibility; two-person verification; records of distributions; no exchange of assistance for images/favours; grievance mechanism communicated to families.

10) Digital, Online & Communications Safety

- Use **official accounts** and approved platforms; avoid private one-to-one messaging with children.
- Parental/guardian consent for any online participation; moderate chats; pre-brief participants on respectful behaviour and privacy.
- **Images/Stories:** obtain **written consent** (Annex C/D); avoid full names, addresses, school names, geotags, and identifiable uniforms; store media securely; honour withdrawal of consent.
- **Data minimisation:** collect only what is necessary (GDPR); encrypt and restrict access; retain per schedule; securely delete when no longer needed.
- Never publish content that **shames**, sensationalises trauma, or creates **risk of re-identification** ("do no digital harm").

11) How to Recognise & Respond to Concerns

11.1 Indicators

Physical injuries; regression; fear or withdrawal; sudden sexualised behaviour; self-harm; persistent hunger/neglect; inconsistent stories; disclosures by child/peer/parent; concerning online interactions.

11.2 Receiving a Disclosure

- **Listen**, stay calm, and **believe** the child; thank them for telling you.
- **Do not** probe or investigate; ask only open prompts (e.g., "Can you tell me what happened?").
- Explain you **cannot keep secrets** and must share with people who can help.
- **Record** facts promptly using the **Incident/Concern Form** (Annex B): who/what/when/where; the exact words if possible; your observations.
- **Report immediately** to **DSL/CPO** (within **the same working day**, or **immediately** if risk of significant harm).

11.3 Immediate Risk

If a child is in **immediate danger**, call **112** and inform the **DSL/CPO** without delay.

11.4 Reporting & Escalation Timeline

1. Reporter informs DSL/CPO **immediately**.
2. DSL conducts **initial triage** (within **24 hours**): risk, safety plan, medical needs.
3. Where threshold is met, DSL **refers to VTAT/Police** promptly (normally **within 24 hours**); informs Executive Director and Chair (serious incidents).
4. DSL opens a **confidential case file**, logs actions/decisions, and coordinates follow-up and support.

11.5 Allegations Against Staff/Volunteers/Partners

- Remove the individual from child contact **pending assessment**; consider suspension.
- DSL ensures **external referral** to authorities where required.
- HR leads internal disciplinary process in parallel, ensuring due process and non-interference with official investigations.
- Protect complainants and witnesses from **retaliation**.

11.6 False or Malicious Allegations

All reports are handled **fairly**. If an allegation is found to be intentionally malicious, appropriate HR/disciplinary action may follow, while ensuring the well-being of the child involved.

12) Survivor-Centred Support

- Provide or refer to **medical care, psychosocial support**, crisis counselling, translation, disability accommodations, and legal information as appropriate.
- Involve families/guardians **when safe** and in the child's **best interests**
- Respect the child's **views and evolving capacities**; seek **informed assent/consent**.
- Ensure **safety planning** and practical protection measures.

13) Information-Sharing, Confidentiality & Data Protection

- Share personal information **only on a need-to-know basis** for safeguarding purposes and **in line with law**.
- Maintain **secure records** (locked cabinets/encrypted drives; access-controlled).
- Keep a **Safeguarding Register** of concerns, actions, and outcomes.
- Apply **retention periods**: incident files retained per legal/insurance advice (typically **7-10 years**); media/consent forms per project need.
- Cross-border transfers follow GDPR safeguards (SCCs/adequacy decisions).
- Children/families may request **access** to their data as permitted by law.

14) Partnerships, Vendors & Due Diligence

- Include safeguarding clauses in MoUs/contracts; require partners and vendors (e.g., transport, accommodation, media) to comply with **this Policy** or demonstrate **equivalent standards**.
- Conduct proportionate **due diligence** and capacity building; share referral pathways; include reporting obligations for incidents.
- Monitor partner compliance; address breaches up to termination.

15) Whistleblowing & Protection from Retaliation

We encourage good-faith reporting by any person (including anonymously where available). Retaliation against reporters, witnesses, or participants is **prohibited** and will lead to disciplinary action.

16) Monitoring, Learning & Review

- **Quarterly** management checks on training completion, incident logs, and corrective actions.
- **After-action reviews** following incidents; update risk controls and training.
- **Annual report** to the Board summarising cases (anonymised), trends, and improvements.
- **Annual policy review** or earlier if laws/contexts change.

17) Non-Compliance & Sanctions

Breaches may result in: removal from activities; disciplinary action up to dismissal; termination of contracts; reporting to professional bodies; and/or **referral to authorities**.

18) Policy Communication & Translations

This Policy is published internally (and externally when appropriate). Child-friendly versions and translations (LT/RU/EN/....) will be produced. Where versions differ, the **English** version controls unless Lithuanian law requires otherwise.

19) Acknowledgement

All representatives must sign the **Safeguarding Acknowledgement** confirming they have read, understood, and will comply with this Policy and the Code of Conduct.

Annexes (Templates)

Annex A — Staff & Volunteer Code of Conduct (Signature Page)

I, _____, agree to follow the Child Protection & Safeguarding Policy and Code of Conduct. I understand violations may lead to disciplinary action and referral to authorities.
Signature: _____ Date: _____ Role: _____

Key Commitments (summary): dignity & respect; safety first; professional boundaries; appropriate contact; no sexualised conduct; digital safety; consent for images; safe transport; immediate reporting.

Annex B — Incident/Concern Report Form

- Reporter name/role/contact: _____
- Child(ren) involved (initials/ID): _____
- Date/time/location of incident/concern: _____
- Description (factual; child's words where possible):

- Injuries/medical needs: _____
- Immediate actions taken: _____
- People present/witnesses: _____

- Risk level (immediate/significant/unknown): _____
- Reported to DSL/CPO (name/time): _____
- Next steps/referrals agreed: _____
- Signature/date: _____

Attach any sketches, screenshots, photos (with consent/need-to-know). Store securely.

Annex C — Photography & Media Consent Form

- Child's name & DOB: _____
- Parent/Guardian name & contact: _____
- Purpose of images/video: _____
- Where used: Organization website, social media, reports, press, other _____
- Data safeguards: Images stored securely; identifying details avoided; consent may be withdrawn at any time by contacting [email].

Consent:

☐ I consent to photo/video capture and use as described above.

☐ I do **not** consent.

Parent/Guardian signature: _____ Date: _____

Child assent (where age-appropriate): _____

Annex D — Parental/Guardian Consent & Medical Information (Activities/Trips)

- Event/Location/Dates: _____
- Emergency contact(s): _____
- Medical conditions/allergies/medications: _____
- Accessibility needs/dietary requirements: _____
- Doctor/Clinic contact: _____

- Transport permissions: ☐ To/from venue ☐ Overnight stay ☐ Swimming/other
- Photo/Media consent: ☐ Yes ☐ No (see Annex C)

Signature (Parent/Guardian): _____ Date: _____

Annex E – Risk Assessment Template

- Activity/Project: _____ Lead: _____
- Date/Time/Location: _____
- Participants: age ranges; vulnerabilities; languages; disability; numbers.
- Hazards & Risks: list; likelihood/severity; controls (ratios, PPE, accessibility).
- Safeguarding Controls: supervision plan; toilets; arrival/departure; missing-child protocol; digital rules; media consent handling.
- Emergency Plan: first-aiders; nearest medical facility; evacuation route; contacts.
- Approval: Lead ____ Manager ____ Date ____

Annex F – Referral Pathway & Key Contacts (Lithuania)

- Immediate danger: Call 112.
- DSL/CPO: *Name / phone / email*
- Deputy DSL: *Name / phone / email*
- State Child Rights Protection & Adoption Service (VTAT): *Local office phone/email*
- Police (non-emergency): *[local]*
- Child Helpline “Vaikų linija”: 116 111
- Ombudsperson for Children’s Rights: *[contact]*
- Specialised NGOs / Crisis Centres: *[insert partners & contacts]*

Instruction: This Annex must be completed and posted at all venues and included in staff/volunteer packs.

Annex G – Data Retention Schedule (Safeguarding Records)

- Incident/case files: 7–10 years after case closure (or more if litigation risk).
- Consent forms & media: retain for project lifecycle + up to 5 years, unless withdrawn earlier.
- Training records & acknowledgements: 5 years.
- Access strictly limited; secure deletion thereafter.

Annex H — Acknowledgement & Annual Declaration

I confirm I have received, read, and understood the **Child Protection & Safeguarding Policy** and agree to comply. I declare any criminal history or investigations relevant to working with children below (or “none”). I will report any changes immediately.

Signature: _____ Printed name: _____ Role: _____ Date: _____

This Policy supersedes previous child protection documents of “Adliga”. Questions may be addressed to the DSL/CPO.

Chapter 2. Sexual Exploitation & Abuse (SEA) Prevention & Response Policy

1) Purpose and Statement of Commitment

“Adliga” is fully committed to the **prevention of, and response to, Sexual Exploitation, Abuse, and Sexual Harassment (SEA/SH)** in all activities, programmes, operations, communications, and partnerships. We adopt a **zero-tolerance** stance towards SEA/SH, recognising it as a grave breach of trust, human rights, professional ethics, and organisational values.

Purpose of this Policy:

- Prevent all forms of SEA/SH through strong standards, safer recruitment, training, culture, and risk management.

- Ensure a **safe, respectful, and equitable environment** for staff, volunteers, beneficiaries, and communities.
- Provide **clear, confidential reporting channels** and **timely, fair response procedures**.
- Ensure compliance with applicable laws and standards, including the **UN Secretary-General’s Bulletin on SEA (ST/SGB/2003/13)**, the **Istanbul Convention**, the **UN Convention on the Rights of the Child**, EU law including **GDPR**, and the laws of the **Republic of Lithuania**.

Do No Harm, Survivor-Centred, Rights-Based, and Trauma-Informed principles guide all prevention and response actions under this Policy.

2) Scope and Relationship to Other Policies

This Policy applies to all persons and entities associated with the Organization (see header). It operates alongside and is complemented by:

- **Child Protection & Safeguarding Policy** (for anyone under 18).
- **Code of Conduct and Anti-Harassment Policy**.
- **Whistleblowing & Complaints Procedure** (non-retaliation).
- **Data Protection/Privacy Policy** (GDPR) and **Records Management**.
- **Partner & Vendor Due Diligence Standards** and contractual clauses.

Where multiple standards apply, the **higher standard** governs. For cross-border work, comply with local law **and** this Policy.

3) Definitions (Plain Language)

Sexual Exploitation: Abuse of a position of vulnerability, differential power, or trust for sexual purposes, including profiting monetarily, socially, or politically. Examples: offering assistance, jobs, transport, or goods **in exchange for sex**; pressuring for sexual favours; transactional sex linked to aid or programme access.

Sexual Abuse: Actual or threatened physical intrusion of a sexual nature, by force or under unequal or coercive conditions; includes rape, assault, attempted rape, forced sex acts, forced prostitution, trafficking for sexual purposes.

Sexual Harassment (SH): Unwelcome sexual advances, requests for sexual favours, or other verbal/physical conduct of a sexual nature that creates an intimidating, hostile, degrading, humiliating, or offensive environment.

Child: Any person under **18 years**. **Sexual activity with a child is strictly prohibited** regardless of local age of consent or mistaken belief of age.

Beneficiary/Community Member: Any person who receives or may receive services, aid, or support from the Organization (incl. refugees, migrants, displaced persons, conflict-affected populations).

Associated personnel: Partners, suppliers, and any third party working for or representing the Organization.

4) Core Principles (adapted from IASC/UN)

1. **SEA/SH are acts of gross misconduct** and grounds for dismissal/contract termination.
2. **Exchange of assistance, benefits, goods, or services for sex is prohibited** ("transactional sex").
3. **Sex with anyone under 18 is prohibited**, regardless of local laws or consent claims.
4. **Sexual relationships with beneficiaries/participants are prohibited** due to power imbalance and risk of exploitation.
5. **Duty to report:** All personnel must report concerns or suspicions of SEA/SH.
6. **Managers bear enhanced responsibility** to prevent and respond promptly.
7. **Survivor-centred approach:** safety, dignity, choice, confidentiality, non-discrimination, and access to services come first.
8. **No retaliation** against reporters/whistleblowers or witnesses acting in good faith.

5) Prohibited Conduct (non-exhaustive)

- Any form of **SEA/SH** as defined above.
 - **Transactional sex**: soliciting or accepting sexual acts in exchange for money, employment, goods, aid, privileges, or promises thereof.
 - **Any sexual activity with a child** (under 18), including grooming, online exploitation, sexting with minors, or possession/distribution of child sexual abuse material.
 - **Sexual relationships with beneficiaries/participants**, even if apparently consensual.
 - **Use of sex workers** while on duty, on Organization premises, during travel for work, or when representing the Organization (prohibited at all times in programme locations due to exploitation risks).
 - **Sexualised communication** (jokes, comments, images, emojis), stalking, unwanted touching, coerced intimacy, or creating a sexualised work environment.
 - **Abuse of authority**: conditioning employment, promotions, access to services, or favourable treatment on sexual favours.
 - **Possession or display of pornography** on Organization devices or premises.
 - **Failure to report** SEA/SH concerns or interfering with a report or investigation.
 - **Retaliation** against reporters, survivors, or witnesses.
-

6) Roles and Responsibilities

- **National Board**: Approves policy; ensures resources; receives annual SEA reports and serious incident notifications.
- **Executive Director**: Accountable for implementation; appoints PSEA-FP/Alternate; ensures safe systems, training, and culture.
- **PSEA Focal Point (PSEA-FP)**: Primary contact for reports; triages risk; ensures survivor safety and referrals; coordinates investigations; maintains confidential case files and the **SEA Register**.

- **Managers & Supervisors:** Model appropriate conduct; ensure team induction/training; stop unsafe behaviour; escalate concerns promptly.
 - **HR & Safeguarding:** Embed SEA clauses in contracts; ensure safer recruitment and disciplinary processes; coordinate with legal/compliance.
 - **All Personnel:** Comply with this Policy; sign the **Code of Conduct**; complete training; report any concerns immediately.
 - **Partners/Contractors:** Maintain equivalent PSEA standards; notify us of incidents; cooperate with investigations; allow audits where contractually required.
-

7) Prevention: Safer Recruitment, Culture, and Risk Management

7.1 Safer Recruitment & Vetting

- Role descriptions specify PSEA responsibilities; advertisements reflect our zero-tolerance.
- Applications require full work history and **self-declaration** on misconduct.
- **Two references** (latest employer included) addressing conduct, incl. any safeguarding concerns.
- **Criminal record checks** proportionate to role/risk, including countries of recent residence where feasible.
- **No-rehire** of individuals dismissed for SEA/SH.

7.2 Induction & Training

- Mandatory **PSEA induction** before starting; refreshers **at least every 24 months**.
- Role-specific training for managers, investigators, case handlers, drivers, outreach and media teams.

7.3 Culture & Safe Environment

- Visible leadership commitment; posters on reporting channels; regular “safeguarding moments.”

- Alcohol policy: no alcohol while responsible for beneficiaries/events; never work under influence.
- **Conflict of interest** declarations for intimate relationships between staff (prohibited within line management chains).

7.4 Programme & Contextual Risk

- SEA risk analysis built into programme design and **pre-activity risk assessments** (cash/aid, accommodation, transport, distributions, digital engagement).
- Clear eligibility and complaint mechanisms for assistance; **no quid-pro-quo**.
- Safe facilities (lighting, separate toilets where feasible, chaperones, safeguarding signage).

7.5 Digital & Online

- Use official channels for communication; **no private messaging** with beneficiaries.
- No storing/sharing sexual content on organisational systems; strong privacy and security settings; moderation for online events.

8) Reporting Channels (Confidential; Good-Faith)

Anyone (staff, volunteers, beneficiaries, partners, public) can report concerns or suspicions. Reports may be **anonymous** where permitted.

Internal:

- **PSEA-FP:** *name / phone / email*
- **Alternate PSEA-FP:** *name / phone / email*
- **HR/Safeguarding inbox:** *insert dedicated email*

External / Anonymous:

- **Secure webform or hotline:** *insert link/number*
- **Complaint boxes** at venues (checked by PSEA-FP)
- **National authorities** (Police 112; specialised services—see Annex F)

Non-retaliation: Any retaliation, intimidation, or interference with a report is a serious breach and will be sanctioned.

9) Receiving and Escalating a Report (Timeline)

9.1 Immediate Safety & Medical Care

- If the survivor is in **immediate danger**, call **112**.
- Offer/arrange confidential access to **urgent medical care**: post-exposure prophylaxis (**PEP**) ideally **within 72 hours**; emergency contraception (within **120 hours**); STI screening; forensic examination where appropriate.
- Ensure safe lodging/transport if needed; implement a **safety plan**.

9.2 Acknowledgement and Triage

- Acknowledge receipt to reporter (if known) **within 2 working days**.
- **PSEA-FP** conducts initial **risk assessment within 24 hours** and decides on immediate protective measures and referrals.
- Consider mandatory reporting to authorities when required by law or when risk to a child/vulnerable person exists.

9.3 Investigation Decision

- Within **5 working days**, ED/PSEA-FP decide whether to open an internal administrative investigation (based on threshold).
- **Conflict-free, trained investigator(s)** appointed; use external investigator if required by complexity or conflict.

9.4 Investigation Process

- Terms of Reference; evidence plan; interviews conducted with **informed consent** and **without re-traumatisation**; interpreters as needed.
- Confidentiality and **need-to-know** sharing only; secure evidence handling.
- **Target timeframe**: conclude within **30-45 calendar days** (extensions documented).
- Standard of proof for internal decisions: **balance of probabilities**.

9.5 Outcome & Case Closure

- Findings and recommendations submitted to ED/HR; disciplinary actions decided per **Sanctions Matrix** (Annex G).
- Offer survivor ongoing support; communicate outcome as appropriate, respecting privacy and law.
- Record lessons learned and update risk controls.

9.6 Law Enforcement & External Reporting

- Where allegations potentially constitute criminal offences, consult legal counsel and consider reporting to **Police/Prosecutor** (respecting survivor's wishes where legally permissible).
 - Notify donors/regulators as required by agreements/law.
-

10) Survivor-Centred Support & Confidentiality

- **Safety, dignity, and choice** guide all actions. Obtain informed consent/assent; respect the survivor's decisions to report (except where law mandates).
 - Provide or refer to **medical, psychosocial, legal, and protection services**; ensure disability-inclusive and language-appropriate access.
 - Maintain **confidentiality** of survivor identity and case details; share only on a **need-to-know** basis.
 - Keep survivors informed about process milestones and available support.
 - **Non-discrimination**: no bias based on gender, age, nationality, status, sexual orientation, disability, or other grounds.
-

11) Data Protection and Records (GDPR-Aligned)

- Store SEA reports in a **restricted, encrypted** repository; assign case numbers; maintain an **SEA Register**.
- Lawful bases: **legitimate interests, legal obligation, vital interests**; special-category data safeguarded.

- Retention: normally **10 years** from closure (or per legal/insurance advice); media/evidence per case need.
 - Data breaches involving SEA files must be escalated immediately to the DPO and managed per GDPR timelines (72-hour notification where required).
-

12) Sanctions and Corrective Actions

Depending on severity and findings, measures may include:

- **Summary dismissal** or contract termination; removal from beneficiary contact; mandatory training; written warning; demotion; probation.
- **Reporting to authorities** and professional bodies.
- **Contract remedies** for partners/vendors: suspension, termination for cause, claw-back, debarment, audit rights.
- **Programme controls**: revise distributions, staffing, venue access, or complaint mechanisms.

False/Malicious Allegations: Good-faith reports are protected even if unsubstantiated. Knowingly false, malicious allegations may result in disciplinary action.

13) Partnerships, Vendors, and Due Diligence

- Contracts and MoUs include **PSEA clauses** (Annex H) requiring equivalent standards, incident notification, cooperation with investigations, and audit access.
 - Conduct proportionate **safeguarding due diligence** prior to engagement and **monitor compliance** during delivery.
 - Non-compliance may lead to corrective actions up to termination.
-

14) Communications, Media, and Advocacy

- **No identifying details** of survivors or alleged perpetrators are shared publicly without lawful basis and explicit consent from the survivor (where safe).
 - Media inquiries are handled by authorised spokespeople only; litigation holds applied where required.
 - No **NDAs** that prevent lawful reporting to authorities or regulators.
-

15) Monitoring, Learning, and Review

- Quarterly management reviews of training completion, incident response times, and corrective actions.
 - Annual anonymised SEA report to the Board.
 - **Annual Policy review** or earlier after legal/operational changes or serious incidents.
-

16) Acknowledgement

All personnel and associates must sign an **Acknowledgement & Annual Declaration** confirming they have read, understood, and will comply with this Policy and the Code of Conduct.

Annexes (Templates)

Annex A — Staff & Volunteer PSEA Code of Conduct Addendum (Sign & Return)

I, *name*, commit to: (1) zero tolerance for SEA/SH; (2) no transactional sex; (3) no sexual activity with anyone under 18; (4) no relationships with beneficiaries; (5) maintain professional boundaries and appropriate communications; (6) report concerns immediately; (7) protect confidentiality; (8) cooperate fully with investigations; (9) never retaliate against reporters or survivors.

Signature: ____ **Date:** ____ **Role:** ____

Annex B — SEA/SH Incident Report Form

- Reporter (name/role/contact or anonymous code):
- Date/time/place of incident/concern:
- Alleged survivor (initials/ID/age/sex; de-identify where needed):
- Alleged perpetrator (role/relationship if known):
- Description (facts; survivor's exact words where possible; avoid opinions):
- Immediate risks/safety needs:
- Immediate actions taken (medical, safety, 112):
- Others informed (PSEA-FP/HR/Police):
- Attachments (photos/screenshots/medical notes—handle securely):
- Reporter signature/date (if not anonymous):

Submit via secure channel to PSEA-FP. Store in encrypted SEA Register.

Annex C — Survivor Assistance & Referral Pathway (Lithuania)

- Emergency/Police: 112
 - Rape Crisis / Sexual Violence Centres: *insert local contacts*
 - Hospitals/PEP access points: *insert*
 - Psychosocial support (NGOs/helplines): *insert*
 - Legal aid clinics: *insert*
 - Shelters/safe accommodation: *insert*
 - Child cases: Coordinate also with State Child Rights Protection & Adoption Service (VTAT) and Child Helpline 116 111 if needed.
-

Annex D — Investigation SOP (Summary)

1. Intake & Triage (risk, safety, medical referrals) → 2) ToR & Investigator appointment (conflict-free) → 3) Evidence plan (documents, interviews, digital) → 4) Interviews (survivor-centred; support person allowed; interpreters) → 5) Analysis (balance of probabilities) → 6) Findings &

Recommendations → 7) Management decision & sanctions → 8) Closure & Lessons learned.

- Safeguards: confidentiality; data security; non-retaliation; fair treatment; right to be heard; appeal pathway on process grounds.
-

Annex E — Complaint & Whistleblowing Channels (Poster Text)

You have the right to be safe from sexual exploitation, abuse, and harassment.

If you experience or witness SEA/SH, report it confidentially:

- PSEA-FP: *name / phone / email*
 - Anonymous: *webform/box/hotline*
 - Police: **112**
*We will listen, support you, and keep your information private.
Retaliation is forbidden.*
-

Annex F — Data Protection & Confidentiality Protocol (SEA Files)

- Access restricted to PSEA-FP, ED, assigned investigator, HR/legal (need-to-know).
 - Encryption at rest and in transit; unique case ID; audit trail.
 - Retention: 10 years from closure unless extended for legal reasons.
 - Breach response: escalate to DPO within **24 hours**; assess notification duties.
-

Annex G — Sanctions Matrix (Guide)

- Gross misconduct with substantiated SEA/SH → summary dismissal; police report; debarment; donor notification.
- Boundary violations / inappropriate conduct (no SEA) → written warning; training; supervision; reassignment.
- Failure to report or interference → disciplinary action up to dismissal.
- Retaliation → disciplinary action up to dismissal.

- Partner/vendor breach → corrective action plan; suspension; termination for cause; debarment.
-

Annex H — Model PSEA Clause for Partners & Vendors

- Partner maintains PSEA policy equivalent to ours; ensures staff training; vets personnel; establishes reporting channels; notifies us of incidents within **48 hours**; cooperates with investigations; allows audits; accepts termination for serious breach.
 - Flow-down: Partner must impose equivalent obligations on its subcontractors.
-

Chapter 3. Survivor-Centred Response SOP

Related policies: Incident Reporting & Case Management SOP; Child Protection & Safeguarding Policy; SEA Prevention & Response Policy; Non-Discrimination & DEI; Code of Conduct; Whistleblowing & Complaints; GDPR & Data Protection; Privacy Policy; Data Breach Response Plan; IT & Cybersecurity Policy; Records Retention & Destruction Schedule; Duty of Care Policy; Travel & Field Safety Policy; Infiltration & Internal Surveillance Policy; Media, Storytelling & Image Consent Policy; Partner Due Diligence & Vetting SOP; Partner Disclosure Policy.

1) Purpose & Scope

This SOP establishes clear, consistent, survivor-centred procedures to receive, support, and manage disclosures of harm, including sexual exploitation, abuse and harassment (SEA), gender-based violence (GBV), child abuse/neglect, trafficking, torture/ill-treatment, discriminatory violence, workplace harassment/bullying, and other serious harms. It applies to all personnel (staff, volunteers, interns, Board), contractors, suppliers, partners, beneficiaries, artists in residence, and visitors.

Objectives: (a) prioritise safety, dignity, choice, consent, confidentiality, and non-retaliation; (b) ensure timely access to medical, psychosocial, legal, and

safeguarding support; (c) comply with law (incl. child-protection duties) and GDPR; (d) document fairly and learn from cases to prevent reoccurrence.

2) Principles (Survivor-Centred & Rights-Based)

1. **Do No Harm:** actions must reduce—not increase—risk.
 2. **Safety & Dignity:** immediate safety first; respectful, non-judgmental interactions.
 3. **Choice & Consent:** survivors decide if/when to share, seek services, or report—**except where law mandates reporting** (e.g., child protection, imminent serious risk).
 4. **Confidentiality & Privacy:** information shared strictly **need-to-know**; data minimised, secured, and time-bound.
 5. **Non-Discrimination & Inclusion:** zero tolerance for bias; **accessible** services and reasonable accommodations.
 6. **Participation & Empowerment:** survivors informed of options in plain language and preferred language; interpreters provided where possible.
 7. **Fairness & Due Process:** impartial handling of concerns; presumption of innocence for respondents while protecting survivor safety.
 8. **Accountability & Learning:** transparent decisions, documented rationales, and improvement actions.
-

3) Definitions (Plain Language)

- **Survivor:** any person who has experienced harm or alleged harm related to our work or context.
- **SEA:** sexual exploitation, abuse, or harassment, including exchange of assistance for sex, coercion, or unwanted sexual contact.
- **GBV:** violence directed at a person based on gender or gender norms (domestic/intimate-partner violence, sexual assault, stalking, forced marriage, etc.).
- **Child:** anyone under **18**.

- **Informed consent:** freely given, specific, informed, **revocable** agreement by a person with capacity.
 - **Capacity & best interests:** for children/at-risk adults, decisions consider legal guardianship, capacity, and best-interest standards; consult DSL.
-

4) Roles & Responsibilities

- **Executive Director (ED):** accountable; approves high-risk decisions, sanctions, external notifications; informs National Board as needed.
- **DSL/CPO (Policy co-owner):** leads safeguarding cases; oversees survivor-centred practice; liaises with child-protection authorities.
- **PSEA Focal Point:** co-leads SEA/GBV cases; ensures survivor options and support pathways.
- **Ethics & Compliance Officer (ECO):** manages cross-cutting misconduct/retaliation; maintains **Survivor Case Register** with minimal data; ensures non-retaliation.
- **Data Protection Officer (DPO):** ensures GDPR compliance, DPIAs, lawful bases, and breach notifications where personal data are involved.
- **IT & Security Lead:** supports secure evidence handling and digital safety measures.
- **HR/People & Culture:** coordinates workplace measures (adjusted duties, leave, safety arrangements) and potential disciplinary processes.
- **Finance Manager/Chief Accountant (FM/CA):** enables emergency funds for safe transport, medical/legal costs per policy.
- **Comms Lead:** manages any internal/external communication with privacy safeguards.
- **Programme/Partner Leads:** support immediate safety and referrals; ensure cooperation and safe environments.
- **All personnel/partners:** respond respectfully, avoid probing, report via channels, and protect confidentiality.

Contacts (to fill): DSL/CPO; PSEA FP; ECO; DPO; IT Lead; HR Lead; FM/CA; **confidential inbox:** *survivor@adliga.fund*.

5) Reporting & Access to Support

Channels: confidential inbox/webform; anonymous box/hotline; direct to DSL/PSEA/ECO/DPO/any manager; to **Board Chair** if ED implicated. Multiple languages and accessible formats.

No retaliation: good-faith reporters/witnesses are protected. **Emergency:** call local emergency services; ensure immediate safety.

6) First Response (What Any Staff Member Must Do)

Listen → Believe → Support → Protect Privacy → Refer

- **Believe & validate** without judgment; avoid blame.
- **Do not investigate;** record only essential facts in the **Intake Form** (Annex B).
- **Explain confidentiality & options** (medical, psychosocial, legal, reporting).
- **Obtain consent** before sharing information, except where required by law/safety.
- **Prioritise safety:** if risk is imminent, follow safety steps and call emergency services.

SLAs:

- **Immediate (same day):** child protection, SEA, imminent risk → alert **DSL/PSEA** and **ECO**.
 - **≤ 24 hours:** acknowledge other disclosures; ensure survivor is offered support options.
 - **Medical time-sensitive care:** inform survivor of urgent options (e.g., emergency contraception and post-exposure prophylaxis per local clinical guidance, typically **within 72 hours**).
-

7) Triage, Risk & Safety Planning

- Open **Case File** with minimal data; assign **Case Lead** (DSL/PSEA/ECO) and case ID.
 - Conduct **Rapid Risk Assessment** (Annex A): safety (including children in household), health, digital risks, intimidation, retaliation, housing.
 - Develop **Safety & Support Plan** with the survivor within **48-72 hours** (Annex C), including safe contacts, code words, transport, accommodation, device safety, and workplace adjustments.
 - Consider **interim measures**: separation of parties, access suspension, duty relocation, escort/transport, emergency grants.
-

8) Information, Consent & Referrals

- Provide a Rights & Options Sheet (Annex D) in the survivor's preferred language (where possible), covering:
 - Medical care (including forensic options where available and survivor chooses).
 - Psychosocial support and counselling.
 - Legal advice and protection orders.
 - Reporting routes: internal, authorities, donors; and implications.
 - Obtain specific consents for each referral or information-sharing using Annex E – Consent to Share/Report; record preferences and any limits (e.g., no name, no contact by phone).
 - For children/at-risk adults, follow legal duty to notify authorities; still respect the person's safety and dignity and inform them appropriately.
-

9) Medical & Forensic Considerations (If Survivor Chooses)

- Offer information on time-sensitive options and accompaniment to services when requested.
- Preserve evidence if the survivor wishes to consider legal action (avoid washing/changing clothes where practical; store items in paper bags).

- Respect the decision not to undergo forensic exam or to delay; update the Safety & Support Plan accordingly.
-

10) Case Handling & Investigation Interface

- If an internal investigation is required (see Incident SOP), ensure survivor-centred arrangements: interview location of survivor's choosing, support person, interpreter, breaks, ability to submit written statements.
 - No direct confrontation between survivor and respondent.
 - Manage conflicts of interest; assign independent investigators where needed.
 - Keep survivor informed of process steps and timelines without sharing confidential details about others.
-

11) Privacy, Data Protection & Records

- Process only minimum necessary personal data under a lawful basis (legal obligation, vital interests, legitimate interests, or consent as appropriate).
 - Store Case Files in restricted DMS folders; encrypt sensitive files; maintain access logs.
 - Use pseudonyms/initials where feasible in working notes.
 - Respect data-subject rights (access, rectification, restriction); balance with confidentiality and third-party rights; coordinate via DPO.
 - Retention: adults – 10 years after closure; children – see Safeguarding Policy (to age 28 or 10 years after closure, whichever later).
 - Manage data breaches per the Data Breach Response Plan.
-

12) Accommodation, Work & Security Measures

- HR/Managers implement reasonable accommodations (schedule changes, remote work, leave, workspace moves).

- Security steps may include access restrictions, no-contact directives, escorts, and device/account protections.
 - For field settings, coordinate safe transport/housing per Travel & Field Safety.
-

13) Multi-Agency Coordination

- With consent (or legal duty), convene case conferences with vetted providers (medical, psychosocial, legal, shelter, police/child services).
 - Use Annex F - Multi-Agency Case Note to record actions and responsibilities.
 - Share only what is necessary; document legal bases and consents.
-

14) Communication & Media

- All external communication requires ED/Comms approval; never identify survivors without explicit written consent.
 - Take down harmful content swiftly (see Media Policy takedown SOP); maintain a communications log in the Case File.
-

15) Case Closure, Feedback & Appeals

- Close a case when actions are complete and risks managed; draft Closure Report (Annex H) with decisions, support provided, and lessons.
 - Offer a Feedback & Complaints route (Annex I) without retaliation.
 - Provide appeal options per Incident SOP where applicable.
-

16) Staff Wellbeing & Vicarious Trauma

- Provide access to confidential counselling or EAP where available; encourage debriefs.
- Managers monitor for vicarious trauma/burnout (Annex J - Manager Guide) and adjust duties after critical incidents.

17) Training, Quality Assurance & KPIs

- Induction for all staff/volunteers on survivor-centred practice; annual refreshers for DSL/PSEA/ECO/HR/Managers.
 - QA reviews quarterly against this SOP (Annex K – QA Checklist).
 - KPIs (quarterly): SLA compliance (acknowledgement, risk assessment, support plan within 72h), percentage with documented consent forms, survivor feedback response rate, corrective actions closed, recurrence rate.
-

18) Review & Continuous Improvement

- Review this SOP annually or after significant incidents/legal changes; report updates to the National Board.
 - Integrate lessons learned into policies, training, and programme design.
-

Annexes (Forms, Tools & Templates)

Annex A — Rapid Risk Assessment (Survivor Safety)

- Risks (physical, psychological, digital, housing, dependents); likelihood/impact; mitigations; responsible person; review date.

Annex B — Intake & Initial Disclosure Form

- Survivor preferred name/contact; language/access needs; brief description; immediate risks; consent notes; referrals offered; case ID.

Annex C — Safety & Support Plan

- Safe contacts; code words; transport/housing; medical/psychosocial/legal referrals; workplace accommodations; digital safety steps; review dates.

Annex D — Rights & Options Information Sheet

- Medical; forensic; psychosocial; legal; reporting routes; privacy; withdrawal of consent; emergency contacts.

Annex E — Consent to Share/Report

- Who; what; why; lawful basis; expiry; withdrawal; signature/recorded consent note.

Annex F — Multi-Agency Case Note / Conference Template

- Participants; confidentiality reminder; actions; owners; timelines; follow-up.

Annex G — Evidence Preservation Quick Guide

- Steps for preserving items/communications; secure storage; chain of custody (cross-ref to Incident SOP Annex F).

Annex H — Case Closure Report

- Actions delivered; outcomes; survivor feedback; lessons; recommendations; sign-offs.

Annex I — Survivor Feedback/Complaint Form

- Experience; what helped/harmed; desired changes; consent for contact; accessibility options.

Annex J — Manager Guide: Vicarious Trauma & Burnout

- Signs; supportive conversation prompts; referral pathways; workload adjustments.

Annex K — Quality Assurance Checklist

- Registration; SLA timings; consent forms; privacy controls; support plan; multi-agency notes; closure; lessons logged.

Chapter 4. Safe Recruitment & Vetting SOP

Policy owner: Executive Director / HR & People and Culture Lead (with Ethics & Compliance Officer, ECO; Designated Safeguarding Lead, DSL/CPO; PSEA Focal Point; Data Protection Officer, DPO; IT & Security Lead; Finance Manager/Chief Accountant, FM/CA; Procurement Lead)

Related policies: Code of Conduct; Non-Discrimination & DEI; Conflict of Interest (COI); Whistleblowing & Complaints; Child Protection & Safeguarding; SEA Prevention & Response; Duty of Care; Travel & Field Safety; IT & Cybersecurity; GDPR & Data Protection; Privacy Policy; Data Breach Response Plan; Records Retention & Destruction Schedule; Fraud Response Plan; Financial Policy; Procurement & Ethical Purchasing; Partner Due Diligence & Vetting SOP; Partner Disclosure Policy; Infiltration & Internal Surveillance Policy.

1) Purpose & Scope

This SOP defines safe, fair, and lawful recruitment and vetting processes for employees, volunteers, interns, consultants/contractors (natural persons), and Board members. It aims to protect children and adults at risk, prevent SEA, fraud, and infiltration, ensure equity and inclusion, and comply with Lithuanian/EU law and GDPR.

Covers the entire lifecycle: workforce planning → job design → advertising → screening → interviews → vetting → decision → conditional offer → onboarding & probation → periodic re-checks.

2) Principles

- **Do No Harm & safeguarding first:** roles with access to children/beneficiaries receive enhanced vetting and supervision.
- **Legality, fairness & non-discrimination:** objective criteria, inclusive language, reasonable accommodations, and equal opportunity.
- **Privacy-by-design (GDPR):** minimal data, transparent notices, secure handling, defined retention.
- **Proportionality & relevance:** vetting depth matches role risk (tiered checks).
- **Transparency & accountability:** documented rationale, scoring, and approvals; right to feedback.
- **Integrity & anti-corruption:** COI declarations, gifts prohibition, and reference verification.

- **Security & infiltration risk control:** identity, right-to-work, access control, and red-flag awareness—**never** based on protected characteristics.
-

3) Roles & Responsibilities

- **National Board:** approves SOP; appoints/oversees Board recruitment; receives annual recruitment/vetting report and serious-case summaries.
- **Executive Director (ED):** accountable for implementation/resources; approves high-risk/exception cases.
- **HR & People and Culture Lead (Policy owner):** stewards process and templates; ensures DEI/accessibility; runs checks; maintains **Recruitment & Vetting Register**.
- **Ethics & Compliance Officer (ECO):** ensures integrity, COI handling, red-flag triage, and non-retaliation for complaints.
- **DSL/CPO & PSEA Focal Point:** define child-safe/SEA vetting standards; review high-risk roles; advise on supervision.
- **DPO:** ensures GDPR notices, DPIAs (where needed), and lawful processing.
- **IT & Security Lead:** joins for privileged-access roles; ensures AUP, MFA, and JML controls.
- **FM/CA:** reviews roles with finance custody/approval powers; advises on bonding/insurance if needed.
- **Hiring Manager:** drafts JD/person spec; chairs panel; ensures structured selection and reference completion.
- **Interview Panel:** trained on anti-bias & safeguarding; uses structured rubrics.
- **All staff:** declare COIs; avoid informal promises; maintain confidentiality.

Designated contacts (to fill): HR Lead; ECO; DSL/CPO; PSEA FP; DPO; IT Lead; FM/CA; **recruitment inbox:** *recruit@adliga.fund*.

4) Process Overview (Flow)

1. **Workforce planning & requisition** (Annex A) → risk tiering and approvals.
 2. **Job design**: JD & Person Specification (Annex B) with safeguarding/SEA statements.
 3. **Advertising & outreach**: inclusive language, DEI targets, accessibility (Annex C).
 4. **Applications & screening**: eligibility & shortlisting matrix (Annex D).
 5. **Interviews & assessments**: structured questions, safeguarding/values scenarios, scoring rubric (Annex E/F).
 6. **Vetting** (tiered): identity, right-to-work, references, criminal record (where lawful & role-relevant), safeguarding/PSEA, COI, sanctions/PEP (when relevant), qualifications, gaps, financial integrity for finance roles, IT security for privileged access (Annex G – Vetting Matrix).
 7. **Decision & documentation**: panel report, rationale, adverse-action notes (Annex H).
 8. **Conditional offer** subject to checks (Annex I) + **Privacy Notice to Applicants** (Annex R).
 9. **Onboarding & probation**: contracts & policies, training, JML access, supervision (Annex J/K).
 10. **Periodic re-checks & renewals** for high-risk roles (Annex G).
-

5) Workforce Planning & Job Design

- Conduct role risk assessment (exposure to children/beneficiaries, funds/assets, data, privileged IT access, travel/field work).
- Define essential vs. desirable criteria; avoid degree inflation; focus on competencies and lived experience where appropriate.
- Include child-safe and SEA-safe statements and duty of care commitments in JD.
- Set reasonable accommodations and flexible options in postings.

6) Advertising & Outreach (DEI & Accessibility)

- Use inclusive language and diverse channels; encourage applications from under-represented groups.
 - Provide plain-language JD, salary bands, location/remote options, key requirements, and selection stages.
 - Offer accessible formats; accept equivalent experience; allow application support on request.
 - Avoid asking for photos or unnecessary personal data.
-

7) Applications & Shortlisting

- Acknowledge receipt; remove non-relevant identifiers in initial screening where feasible (anonymised shortlisting).
 - Use a Shortlisting Matrix aligned with the Person Spec; at least two reviewers score independently, then reconcile.
 - Keep notes and scores in the Recruitment Register; provide feedback upon request where feasible.
-

8) Interviews & Assessments

- Structured interviews with consistent questions, including: safeguarding/SEA scenarios; ethical dilemmas; DEI and trauma-informed practice; job-specific competencies.
 - Practical exercises (e.g., writing task, role-play, case study) where relevant; accessible alternatives provided.
 - Panel trained on bias mitigation; ensure gender and perspective diversity where possible.
 - Document scores/comments using Interview Scoring Rubric (Annex F).
-

9) Vetting & Background Checks (Tiered)

Apply proportional checks based on risk tier (Annex G). Obtain explicit consent and provide privacy notice.

Core checks (all roles):

- **Identity & right-to-work** (government ID, residence/work permit).
- **Two references**, including one **most recent line manager** (Annex L).
- **COI declaration** (Annex M).
- **Gaps in employment** explained (written) and verified where feasible.

Enhanced checks (where relevant by role):

- **Criminal record certificate** (lawful, proportionate, and relevant to role; not blanket). For **child/vulnerable-adult roles**, require child-safety-appropriate clearance per national rules; no placement in such roles with relevant disqualifying offences.
- **Safeguarding & PSEA self-declaration** (Annex N) + policy acceptance.
- **Qualifications/licences** verification (e.g., clinicians, drivers, accountants).
- **Sanctions/PEP/adverse media** for senior/representational/finance roles.
- **Financial integrity checks** (where lawful) for roles with payment approval/cash custody.
- **IT security vetting** for privileged access: prior admin experience, secure-practice knowledge, and NDA/AUP acceptance.
- **Infiltration/Integrity red-flags** review (behaviour-based; non-discriminatory) per Integrity Policy.

Volunteers & interns: scaled checks; for those with beneficiary contact, treat as staff for safeguarding vetting.

Contractors/consultants (natural persons): same tiering applies; ensure contractual warranties and right to remove personnel.

10) Decision, Adverse Findings & Risk Mitigation

- Panel compiles **Selection Report** (Annex H) summarising scores, strengths, risks, and recommended mitigations/supervision.
 - If adverse findings arise, conduct a **Vetting Risk Assessment** (Annex O) to decide on rejection, conditional hire (e.g., restricted duties, enhanced supervision, training), or escalation to ED/ECO/DSL.
 - Respect **rehabilitation** principles; evaluate relevance, time elapsed, and risk to beneficiaries/finances/data.
-

11) Conditional Offer, Contracting & Pre-Start Controls

- Issue **Conditional Offer** (Annex I) subject to satisfactory checks.
 - Before start: sign **Code of Conduct, Safeguarding & PSEA commitments, Confidentiality/NDA, IT AUP, and Privacy Acknowledgement**.
 - For drivers/field roles: complete **medical/fitness-to-work** (role-based), licence check, and **Duty of Care** briefing.
-

12) Onboarding, Supervision & Probation

- Implement **Joiner-Mover-Leaver (JML)** within **1 business day** of start (accounts/access least privilege; MFA; equipment issue).
 - Mandatory **induction training** within **30 days**: safeguarding/SEA, DEI, Code of Conduct, privacy/GDPR, Incident SOP, Duty of Care/Field Safety, anti-corruption.
 - **Probation** plan with goals and check-ins (e.g., 2 weeks, 3 months, end of probation); extend or end per policy.
 - Assign a **supervisor/mentor** and define a supervision cadence; restrict unsupervised contact with beneficiaries until induction complete and references verified.
-

13) Periodic Re-Checks & Renewals

- **Annual** re-attestation: Code of Conduct, Safeguarding/PSEA, COI; access reviews (see IT Policy).

- **Every 2-3 years** or upon role change: renewed checks for high-risk roles (child-facing, finance approvals, privileged IT access).
 - **Event-driven** re-checks after incidents, allegations, or significant role scope changes.
-

14) Records, Privacy & Retention

- Keep Recruitment & Vetting files in secure HR DMS with role-based access; retain audit trail of decisions.
 - **Retention:** unsuccessful candidate files **12 months** (unless consent to keep longer); hired candidates → move relevant items to personnel file (retain per **Records Schedule**).
 - Provide **Applicant Privacy Notice** (Annex R); honour data subject rights via DPO; avoid unnecessary sensitive data; no undisclosed social-media monitoring.
-

15) Complaints, Appeals & Non-Retaliation

- Candidates may raise concerns via **Whistleblowing & Complaints**; decisions can be appealed to HR/ECO panel (documented).
 - Strict **non-retaliation** for good-faith complaints.
-

16) Exceptions & Emergency Hiring

- ED may approve **time-bound exceptions** (Annex P) with compensating controls (e.g., supervised duties only; no systems/beneficiary access) and deadline to complete full vetting (**≤ 30 days**).
 - Document rationale, risk, and review date.
-

17) Monitoring, KPIs & Audit

Track quarterly: time-to-hire; % vacancies with structured JD/person spec; DEI outreach metrics; % panels trained; SLA on reference completion; %

hires with completed induction ≤ 30 days; re-checks on time; findings and CAP closure rate.

Conduct spot audits of files and decisions; report to National Board annually.

18) Review & Continuous Improvement

HR/ECO review this SOP annually or after legal/practice changes; integrate lessons from incidents, audits, and feedback; update annexes and training accordingly.

Annexes (Templates, Forms & Tools)

Annex A — Job Requisition & Risk Tiering Form

- Need, budget, role risk (children/beneficiaries, funds, data, IT access, travel), approvals.

Annex B — JD & Person Specification Template

- Purpose; duties; competencies; safeguarding/SEA statement; DEI commitment; accessibility notes.

Annex C — Inclusive Advertising & Outreach Checklist

- Channels; language; salary transparency; accessibility; accommodations; closing date; privacy link.

Annex D — Shortlisting Matrix

- Criteria; weights; reviewer scores; decision; notes.

Annex E — Structured Interview Question Bank

- Values/ethics; safeguarding/SEA scenarios; DEI; conflict resolution; job-specific competencies.

Annex F — Interview Scoring Rubric

- Scale definitions; exemplar answers; red-flag indicators.

Annex G — Vetting Matrix by Role Risk

- Core vs. enhanced checks for Staff, Volunteers/Interns, Board, Finance, Drivers, IT Admins, Child-facing roles.

Annex H — Selection Report Template

- Scores; strengths; risks; mitigations; decision; approvals.

Annex I — Conditional Offer Template

- Conditions; start date; documents needed; policy acknowledgements.

Annex J — Onboarding Checklist (JML)

- Accounts; equipment; inductions; supervisor; probation plan; access review date.

Annex K — Induction & Mandatory Training Log

- Modules; dates; completion status; refresher due.

Annex L — Reference Check Form

- Relationship; dates; role; performance; conduct; safeguarding; rehire status; verification notes.

Annex M — Conflict of Interest Declaration (Candidate)

- Relationships; outside roles; mitigation/recusal plan.

Annex N — Safeguarding & PSEA Self-Declaration

- Relevant history; investigations; commitments; signature.

Annex O — Vetting Risk Assessment (Adverse Findings)

- Finding; relevance; time elapsed; context; risk rating; decision; controls; review date.

Annex P — Exception & Risk Acceptance Form (Emergency Hire)

- Justification; controls; end date; approvals.

Annex Q — Volunteer/Intern Agreement Template

- Scope; supervision; training; safeguarding; expenses; insurance; confidentiality.

Annex R — Applicant Privacy Notice (GDPR Art. 13/14)

- Controller; purposes; lawful bases; recipients; transfers; retention; rights; contact.

Chapter 5. Incident Reporting & Case Management SOP

Related policies: Whistleblowing & Complaints Policy; Code of Conduct; Non-Discrimination & DEI; Child Protection & Safeguarding Policy; SEA Prevention & Response Policy; GDPR & Data Protection Policy; Privacy Policy; Data Breach Response Plan; IT & Cybersecurity Policy; Records Retention & Destruction Schedule; Fraud Response Plan; Financial Policy; Procurement & Ethical Purchasing Policy; Conflict of Interest (COI) Policy; Media, Storytelling & Image Consent Policy; Infiltration & Internal Surveillance Policy; Partner Due Diligence & Vetting SOP; Partner Disclosure Policy; Sustainability Guidelines.

1) Purpose & Scope

This SOP establishes clear, consistent, survivor-centred procedures for reporting, triaging, investigating, resolving, and learning from incidents and complaints that may impact people, programmes, funds, or data. It applies to all personnel (employees, volunteers, interns, Board), contractors, suppliers, partners, beneficiaries, and visitors in any location or medium (in-person or digital).

Incident types covered (non-exhaustive):

- **Safeguarding:** child protection concerns; abuse/neglect; exploitation of adults at risk.
- **SEA:** sexual exploitation, abuse, or harassment.
- **Workplace conduct:** harassment, bullying, discrimination, retaliation, COI breaches, Code of Conduct violations.
- **Fraud/financial irregularities:** theft, bribery, corruption, asset misuse.
- **Privacy/security:** personal data breach; IT/cybersecurity incidents.
- **H&S/physical security:** injuries, threats, facility incidents.
- **Partner/vendor issues:** contract breaches, sub-standard practice, disclosure failures.

- **Infiltration/integrity:** hostile surveillance, unauthorised recording, insider threat.
 - **Other:** any act/omission that risks harm to people, property, reputation, or compliance.
-

2) Principles

- **Do No Harm & survivor-centred:** safety, dignity, and privacy first—especially for children and survivors of violence.
 - **Legality & human rights:** actions must be lawful, necessary, proportionate, and documented.
 - **Non-retaliation:** no adverse action against good-faith reporters, witnesses, or participants in investigations.
 - **Confidentiality:** restrict information to a **need-to-know** basis.
 - **Fairness & due process:** impartiality, presumption of innocence, and right to be heard, consistent with safeguarding needs.
 - **Data minimisation & GDPR:** collect only what is necessary; secure handling and retention.
 - **Accountability & learning:** complete, accurate case files; lessons integrated into improvements.
-

3) Roles & Responsibilities

- **Executive Director (ED):** overall accountability; approves sanctions and high-risk decisions; informs National Board as required.
- **Ethics & Compliance Officer (ECO): SOP owner** and primary intake for misconduct/whistleblowing; manages **Case Register**; assigns Case Lead; ensures non-retaliation.
- **Designated Safeguarding Lead (DSL/CPO):** leads child protection/adult-at-risk cases; liaises with authorities.
- **PSEA Focal Point:** co-leads SEA cases with DSL/ECO; ensures survivor-centred approach.

- **Data Protection Officer (DPO):** leads privacy assessment; manages DSRs; co-leads data breach notifications (72-hour rule).
- **IT & Security Lead:** handles cyber/IT incidents and forensics; supports evidence handling.
- **Finance Manager/Chief Accountant (FM/CA):** leads fraud/financial irregularity inquiries; implements holds and recovery.
- **HR/People & Culture Lead:** manages workplace conduct cases; coordinates corrective/disciplinary actions.
- **Communications Lead:** prepares internal/external statements when approved.
- **Programme/Partner Leads:** support fact-finding; implement interim safeguards and CAPs.
- **All personnel & partners:** report concerns promptly; preserve evidence; cooperate.

Escalation contacts (to fill): ECO; DSL/CPO; PSEA FP; DPO; IT Lead; HR Lead; FM/CA; Comms Lead; **incident inbox:** *incidents@adliga.fund*.

4) Reporting Channels & Accessibility

- Confidential inbox/portal (email/webform), anonymous box/hotline, direct to ECO/DSL/DPO or any manager; to Board Chair if ED is implicated.
 - Multiple languages and accessible formats; interpreters where possible.
 - Accept verbal, written, or third-party disclosures; document promptly with consent and safeguarding considerations.
 - Provide information on rights, support, and next steps upon receipt.
-

5) Intake, Triage & SLAs

5.1 Registration

- Assign **Case ID** and create a **Case File** on secure DMS; log in **Case Register** with minimal personal data.

5.2 Acknowledgement SLAs

- **Immediate (same day):** child protection, SEA, imminent safety risks.
- **≤ 24 hours:** data breach indicators, serious fraud/corruption, physical security.
- **≤ 2 working days:** other complaints/incidents.

5.3 Initial triage

- Determine **type, severity** (Low/Medium/High/Critical), and **conflicts of interest**; assign Case Lead (see RACI in Annex B).
 - Implement **immediate safety measures** (separate parties, suspend access, safeguarding referrals).
 - Notify required focal points (DSL/PSEA/DPO/IT/FM/HR) and agree a plan.
-

6) Risk Rating & Decision Tree

- Rate likelihood × impact using Annex A – Risk Matrix.
 - Use the Decision Tree (Annex C) to determine: internal handling vs. external referral; need for legal/law-enforcement notification; survivor support; donor notification; insurance notice.
 - For data breaches: evaluate against 72-hour supervisory-authority notification (see Data Breach Plan).
 - For child protection: follow mandatory reporting laws; consult DSL/CPO.
-

7) Investigation Standards

- **Impartiality:** declare and manage investigator COIs; reassign if needed.
- **Planning:** Investigation Plan (scope, witnesses, evidence, timeline).
- **Evidence handling:** maintain **Chain of Custody** (Annex F); preserve originals; work on copies; secure storage.

- **Interviews:** trauma-informed; witness support person allowed; interpreters; do not promise outcomes. Use **Interview Guide** (Annex E).
 - **Documentation:** time-stamped notes; file naming per Records Standard; version control.
 - **Privacy:** GDPR-compliant processing; restrict access to Case File; pseudonymise where feasible.
-

8) Case Actions, Outcomes & Sanctions

- **Corrective actions** may include training, supervision changes, resource controls, **CAP** (Annex H).
 - **Sanctions** may include warnings, suspension, termination, vendor remedies, fund recovery, reporting to authorities/regulators, and **debarment** (see Partner SOP).
 - **Safeguarding:** survivor care plan; safe referral to specialised services; respect consent and confidentiality (subject to legal duties).
 - **Data breach:** notifications and remediation per Plan.
-

9) Communications & Stakeholder Management

- Use **approved templates** (Annex I) for staff notifications, donor updates, authority reports, and public statements.
 - Communications must be **factual and minimal**; avoid identifying survivors; align with legal advice.
 - Keep a **communications log** in the Case File.
-

10) Closure, Appeals & Learning

- Case is **closed** when actions are complete and risk is controlled.
- Draft a **Closure Report** (Annex J): findings, decisions, actions, dates, lessons learned, and responsible owners for follow-ups.
- Offer an **appeal route** where policy allows; record outcomes.

- Feed lessons into training, policy updates, and risk registers; brief the National Board on trends.
-

11) Records, Privacy & Retention

- Store Case Files in restricted DMS folders linked to the Case Register.
 - Retention: generally 10 years after closure (or as required by law/donor); safeguarding/SEA and children's files per Safeguarding Policy (longer as specified).
 - Redact/anonymise reports used for learning; manage access logs.
 - Respect data subject rights (access, rectification, restriction) with DPO oversight—balance with confidentiality and third-party rights.
-

12) Training, QA & KPIs

- Induction for all staff/volunteers; annual refresher for managers and focal points.
 - QA reviews: quarterly sample of Case Files against this SOP (Annex K – QA Checklist).
 - KPIs (tracked quarterly): acknowledgement and triage SLA compliance; time to closure by severity; percentage of cases with CAP; training completion; recurrence rate; lessons-learned actions implemented.
-

13) Exceptions & Emergency Provisions

- In emergencies, ED/ECO may take immediate measures (suspension/access blocks) pending full process; document rationale and proportionality.
 - For humanitarian urgency, minimal intake may be accepted with follow-up within 5 working days.
-

Annexes (Templates & Tools)

Annex A — Risk Matrix (Likelihood × Impact)

- Severity criteria for Safeguarding/SEA, Data, Fraud, H&S, Conduct, Integrity; thresholds for escalation.

Annex B — RACI & Roles Map

- For each incident type: who is **Responsible, Accountable, Consulted, Informed** (ECO, DSL/PSEA, DPO, IT, HR, FM/CA, Comms, ED, Board).

Annex C — Decision Tree

- Triage → Safety → Legal duties → Notify authority/donor? → Investigation? → Actions → Closure.

Annex D — Intake & Case Registration Form

- Reporter (name/anonymous), contact, date/time, type, location, parties, summary, immediate risks, consent, preferred contact, accessibility needs.

Annex E — Interview Guide & Notes Template

- Preparation; rapport; open questions; cultural and trauma considerations; closing; signature.

Annex F — Evidence Log & Chain of Custody

- Item ID; description; source; date/time; collector; storage; transfers; signatures.

Annex G — Safety & Support Plan (Survivor/At-Risk)

- Risk assessment; referrals; accommodations; contact protocol; follow-ups.

Annex H — Corrective Action Plan (CAP)

- Findings; actions; owners; deadlines; verification; status.

Annex I — Notification Templates

- Authority (data breach ≤72h; safeguarding); donor update; internal staff; public Q&A.

Annex J — Case Closure Report

- Summary; findings; decisions; actions; outcomes; lessons learned; recommendations.

Annex K — Quality Assurance (QA) Checklist

- Registration; SLA; safeguarding; GDPR; evidence; decisions; actions; communications; retention; sign-offs.

Annex L — Dashboard & KPI Fields

- Case ID; type; severity; dates; SLA flags; actions; closure; lessons; owner; privacy flag; appeal outcome.