moonshot

Standards for Referrals

Requirements for Conducting Interventions

The document outlines Moonshot's practice standards for intervention programs to respond to violent extremism (VE) and other harms online. The purpose is to ensure all interventions we conduct are ethical, legal, and apply current best practices in violence prevention and safeguarding.

OCTOBER **2022**

MOONSHOTTEAM.COM

Practice Standards for Online Referrals

- **Do No Harm:** ‘Do No Harm’ (DNH) is a guiding principle used to help practitioners avoid causing harm (unintended or otherwise) through their actions and behaviors. All Moonshot projects follow DNH principles, meaning they regularly evaluate, assess, and mitigate any potential impacts - both positive and negative - that stem from a campaign or intervention (e.g. considering if an intervention might further entrench negative perceptions or vulnerabilities among the target audience, rather than illuminating an alternative). Time and event-driven DNH processes and checks are required.

- **Purpose and Scope:** All interventions must have a clearly defined scope: the public safety issue being addressed, target audience, objectives, and methodology.

- **Partner Due Diligence and Onboarding:** Project teams should conduct a thorough assessment of potential partners capacity and delivery record. It is essential to know whether a partner has the capacity to cope with increased demand for information or services, both during and after a project is delivered. If partners require training to deliver services to specific audiences, implement new security measures, or other programming enhancements, Moonshot will support them to ensure these are in place prior to an intervention. Interventions will not be initiated without written confirmation, from all parties, that all practice standards have been met and they are ready to receive referrals.

- **Duty of Care:** Moonshot should ensure a standard of reasonable care for our teams, partners, and any beneficiaries of an intervention. This involves, for example, planning for the safety of partners, and putting security measures in place for scenarios where the safety of an individual or group is threatened as a result of a project.

- **Managing, Monitoring and Reporting Risks:** Projects should document every risk that may occur in a risk matrix, assess their likelihood and severity, and develop adequate strategies to mitigate and manage them, including allocating a responsible person. Threat reporting processes relevant to the location of operation must also be in place.

- **Data Protection and Civil Liberties:** Data management, compliance and prevention practices are governed by national and subnational legislation covering data processing, privacy and civil rights. All Moonshot projects must ensure lawful, secure, and proportionate data collection, storage and retention, particularly in relation to Personally Identifying Information (PII). Moonshot abides by the standards set in the European Union General Data Protection Regulation (GDPR) in the collection, handling and process of data in all its operations, including those in the US and Canada.

- **Measuring Impact and Implementing Findings:** Projects should have a monitoring and evaluation framework in place to understand their impact (short, medium, and long-term). This is not only essential to understanding whether an approach is working, but also helps to prevent and mitigate harm. Ongoing monitoring and evaluation will highlight unintended consequences, adapt to evidence that things may not be going as planned, build on activities that amplify positive impact, and document important lessons.

- **External Reviews and Quality Assurance:** Moonshot requires external reviews and quality assurance from subject matter experts prior to launching a campaign or intervention, to ensure that a project’s methodology, assets and targeting strategies are appropriately tailored, localized and culturally sensitive, and are not likely to cause harm.

Practice Standards for Service Providers

Corresponding documentation/policies are highlighted where applicable.

- **Case Management Protocols:** including clear, accurate, secure record keeping and seeking supervision input when required. Case Management systems should maintain data for monitoring and evaluation (such as anonymized and aggregated data on cases, referral sources, and the number of 'appropriate' referrals received), as well as more detailed or sensitive information (identified risk factors; treatment plans; client contact information) that is stored in a confidential and secure format. Providers should have clear protocols to determine new client's vulnerabilities and their eligibility for services. They should be able to develop individualized support and risk management plans, and monitor and evaluate the effectiveness of an intervention. Procedures to close a case should be well defined and prepared (e.g. aftercare services or referrals to other relevant services).

  Expected documentation: Case management protocols for intake, case planning, and client pathway documentation

- **Adequate Staffing and Resourcing:** adequate staffing and resourcing (technical and financial) must be in place for the duration of the referral program to support vulnerable service users. This may include full time practitioners as well as consultants.

- **Expertise in Identifying and Assessing Indicators of Risk and Vulnerability:** including safeguarding concerns that require referral to police or external social service agencies. Partners should use a defined analytical method, such as Structured Professional Judgment tools (VERA; ERG 22+; YSET), and be capable of conducting a threat assessment during initial screenings. Practitioners using these tools must have the knowledge to apply and interpret their findings in a given context, and a clear understanding of the project's defined audience and their potential vulnerabilities.

  Expected documentation: Risk, needs and/or threat assessment framework to support assessment of client vulnerabilities and/or protective factors.

- **Data Protection and Civil Liberties:** including complying with all relevant national and subnational legislation and mandated reporting requirements. Service providers must have robust digital and information security policies in place, covering device and account security at minimum. Providers must communicate confidentiality expectations to clients, as well as any instances in which confidentiality will be broken (i.e. in the case of a specific threat of self-harm or harm toward others). Personal data should never be disclosed or made available for purposes other than those originally specified, except with the consent of the data subject or by the authority of law.

  Expected documentation: Privacy policy, digital and information security policy, consent procedures, information-sharing agreements applicable to third parties (e.g. Moonshot).

- **Establishing Boundaries with Clients:** including working within online security protocols and maintaining personal wellbeing while carrying out potentially challenging work. In addition to providing clarity on how client's personal information is used, providers should also be clear about what can and cannot be provided as part of their program.

  Expected documentation: Code of ethics.

- **Formalized Security and Risk Escalation Protocols:** If during the course of an online or offline intervention, a candidate referred to a provider discloses information that indicates a security risk, or a risk of harm to another individual, the provider must be capable of escalating this through an immediate referral to police or social services. This process must be clearly communicated, regularly reviewed, and included in any training/onboarding.

__Expected documentation:__ Risk escalation procedure (mandated reporting procedure), risk assessment, risk log.

- **Providing an Accessible and Non-Judgemental Service:** including actively reducing barriers to engagement, responding to messages in a timely manner, and focusing on achieving positive change. Client engagement should be voluntary, and during the intake process, providers must explain the purpose, conditions and goals of participating in an intervention.

- **Maintaining a Robust Monitoring and Evaluation Process:** Partners must have a framework to collect and analyze data related to delivery, and identified metrics/indicators (e.g. number of referrals p/w). They should regularly evaluate internal processes (case management; assessment tools; confidentiality) and be capable of sharing this data to improve the design and delivery of their program, and mitigate any risk of harm.

  __Expected documentation:__ Monitoring and evaluation plan/list of metrics.

- **Staff Training and Supervision:** Providers should set clear quality standards and guidelines for their work, convene their staff regularly to discuss interventions or case work, and ensure that supervision is available for all team members. For disengagement and deradicalization services, staff should ideally have access to a broader, interdisciplinary practitioner team with physiological expertise, and be able to hold debriefing workshops to support service delivery, assess security risks, and ensure their own wellbeing.

  __Expected documentation:__ Internal guidelines for quality management and practice standards; training and debriefing plan for practitioners.

Checklist for Making Referrals to Service Providers

Service providers who receive referrals from Moonshot must have the following documents or processes in place.

- Clear client management pathway and service offer
- Protocols for case intake, planning, and management
- Risk communication and escalation guidelines for all staff and partners
- Data security policy
- Digital security policy
- Monitoring and evaluation plan

For psychosocial service providers, the following should also be in place:

- Internal code of ethics, or an external set of standards (eg NASW Code of Ethics)
- Aftercare services or an exit strategy for all program participants

Ideally, staff will have received:

- Training to ensure familiarity with target audiences, and potential vulnerabilities and protective factors
- Training to recognize and mitigate bias
- Digital security training, to protect staff and clients’ physical security, and the confidentiality of data collected during interventions