Research Ethics and Data Protection Policy

Manāra Policy & Practice (Private) Limited

CUIN: 0321127 | Version 1.0 | Approved: 27 February 2026

Research Ethics and Data Protection Policy

Manāra Policy & Practice (Private) Limited

CUIN: 0321127 | Version 1.0

Document Title	Research Ethics and Data Protection Policy
Organisation	Manāra Policy & Practice (Private) Limited
Corporate ID	0321127
Version	1.0
Approval Date	27 February 2026
Approved By	Maliha Shah, Chief Executive Officer & Founder Ahmad Nadeem, Director & Co-Founder
Policy Owner	Chief Executive Officer
Next Review Date	27 February 2027
Classification	Public

Domestic Legal Framework

Constitution of Pakistan, 1973 (Art. 14 — Right to Privacy) • Prevention of Electronic Crimes Act, 2016 • Companies Act, 2017 • Anti-Money Laundering Act, 2010 • Protection Against Harassment of Women at the Workplace Act, 2010 (amended 2022) • Official Secrets Act, 1923 (where government sources are engaged) • Personal Data Protection Bill, 2023 / Draft Act, 2025 (pending enactment — monitored for compliance readiness)

Extraterritorial Frameworks (where applicable)

EU General Data Protection Regulation, 2016/679 • Regulation of Artificial Intelligence Act, 2024 — Pakistan Senate (pending enactment, monitored)

International Ethical Standards

Belmont Report Principles, 1979 • Declaration of Helsinki (WMA, as revised) • UN Declaration on the Rights of Indigenous Peoples, 2007 (where indigenous communities are engaged)

Why This Policy Exists

Research is how Manāra learns, and how it contributes. Whether we are mapping climate vulnerability in mountain communities, tracing the legal experiences of women across two countries, or documenting the heritage of displaced communities, the work requires people to share things that matter to them. Their stories, their data, their trust.

This Policy sets out how we handle that responsibility. It applies to everyone who works on research under Manāra's name, whether on our core team or as a collaborator on a specific project. It is not a compliance exercise and it is not optional. It is the minimum standard of care we owe the people whose knowledge makes our work possible.

Manāra regularly engages with people in contexts of real vulnerability: communities that have lost their homes to floods, women who have survived violence, indigenous communities whose languages and ways of life are under pressure, individuals who work in environments where what they say to a researcher could have consequences. The ethical obligation this creates is not discharged by producing a good report. It is discharged by ensuring the research process itself does no harm, respects each person's right to decide whether and how to participate, and protects the information they share.

This Policy draws on the Belmont Report principles of respect for persons, beneficence, and justice, as well as the Declaration of Helsinki and, where we engage with indigenous communities, the UN Declaration on the Rights of Indigenous Peoples. It reflects our obligations under Pakistan's Prevention of Electronic Crimes Act, 2016 and Companies Act, 2017, and, where our work touches EU-resident participants or European-funded projects, the extraterritorial reach of the EU General Data Protection Regulation. We also track the Personal Data Protection Bill currently progressing through Pakistan's legislature, and will update this Policy when it is enacted.

A note on the Official Secrets Act, 1923: when Manāra engages government officials as key informants or handles documents that may carry government sensitivity, this law has direct implications for what information can be held, shared, or published. Researchers must identify and flag any such materials to the Policy Owner before use.

1. Scope and Application

This Policy applies to:

- All primary research conducted by or on behalf of Manāra, including qualitative and quantitative data collection, key informant interviews, focus group discussions, surveys, oral histories, and participant observation.
- All secondary research that involves the processing of identifiable personal data, including data received from clients, partners, or government sources.
- All monitoring, evaluation, and learning activities in which Manāra collects or analyses data about program participants or beneficiaries.
- All knowledge products, publications, and communications derived from research data.
- All digital systems, platforms, and tools used to collect, store, process, or transmit research data.

- All members of Manāra's core team, collaborators, consultants, field enumerators, interpreters, and any third party engaged on research activities under Manāra's contractual or institutional responsibility.

This Policy does not apply to desk research or literature reviews that do not involve the collection or processing of personal data, unless such research directly informs an engagement with human participants.

2. Definitions

The following terms carry specific meanings throughout this Policy:

Personal Data	Any information relating to an identified or identifiable natural person. This includes names, contact details, photographs, voice recordings, and any combination of data that could identify an individual even if no single item alone would do so.
Sensitive Personal Data	A subset of personal data that warrants heightened protection due to the particular risks its disclosure creates. This includes data relating to health, sexual orientation, gender identity, ethnicity, religion, political opinion, migration status, legal history, or experiences of violence or abuse.
Research Participant	Any individual who provides data, engages in an interview, participates in a focus group, completes a survey, or otherwise contributes information to a Manāra research activity, whether in a professional or personal capacity.
Vulnerable Population	Individuals or groups whose circumstances reduce their capacity to protect their own interests in a research context, including but not limited to minors, survivors of trauma or violence, internally displaced persons, persons with disabilities, individuals in financial dependency, and members of marginalised ethnic or religious communities.
Informed Consent	A process by which a research participant voluntarily agrees to take part in a study after receiving a clear, complete, and comprehensible explanation of what participation involves, what data will be collected, how it will be used, who will have access to it, and what their rights are.
Anonymisation	The irreversible processing of personal data so that the individual cannot be identified, directly or indirectly, by any means reasonably likely to be used.
Pseudonymisation	The processing of personal data so that it can no longer be attributed to a specific individual without the use of additional information, which is kept separately and subject to technical and organisational measures.
Data Controller	The entity that determines the purposes and means of processing personal data. Manāra acts as data controller for all research data it collects independently. Where Manāra processes data on behalf of a client, roles are determined by written agreement.

Data Processing	Any operation performed on personal data, including collection, recording, storage, retrieval, use, disclosure, and deletion.
Community Consent	A consultative process, in addition to individual consent, through which recognised community structures or representatives are engaged regarding research that affects a community as a collective. Required for research with indigenous or strongly cohesive communities.

3. Core Ethical Principles

All research conducted under Manāra's institutional responsibility is governed by the following six principles. These are not bureaucratic requirements; they are the values that give the research its integrity.

3.1 Respect for Persons

Every research participant is an autonomous individual whose right to decide whether, how, and on what terms to participate in research must be fully respected. Participation is always voluntary. No individual may be coerced, pressured, or offered disproportionate inducements to participate. Participants may withdraw at any time without consequence. Where individuals have diminished autonomy, additional protections are mandatory.

3.2 Do No Harm

Research must not expose participants to risks of physical, psychological, social, economic, legal, or reputational harm that are greater than those they would face in ordinary life. This obligation extends beyond the research encounter: Manāra must consider how the storage, publication, and dissemination of research data might affect participants long after the data was collected. Where risks cannot be eliminated, they must be minimised and clearly disclosed.

3.3 Beneficence

Research should generate benefits. Those benefits may accrue to participants directly, to their communities, to policy audiences, or to society more broadly. Research that serves only Manāra's commercial or reputational interests without contributing value to those who bear its risks is ethically insufficient. Manāra commits to ensuring that the communities and individuals who contribute to its research have meaningful access to findings that affect their lives.

3.4 Justice

The burdens and benefits of research must be distributed fairly. Vulnerable communities must not be used as convenient research sites when the intended beneficiaries of the research are others. Research designs must be examined for structural bias, including whose knowledge is centred, whose questions are asked, and whose voices are quoted and whose are anonymised.

3.5 Intellectual Honesty

Manāra's research must reflect what the evidence shows, not what clients, funders, or Manāra itself might prefer it to show. Findings must not be suppressed, selectively presented, or distorted to serve pre-determined conclusions. Methodological limitations must be disclosed. Where research conclusions are contested or uncertain, that uncertainty must be represented honestly.

3.6 Cultural Sensitivity and Humility

Manāra works across diverse cultural, linguistic, and institutional contexts. Research methods, consent processes, and data interpretation must be adapted to those contexts. Cultural sensitivity is not a courtesy; it is a methodological requirement. Imposing external frameworks without regard for local knowledge systems and community norms produces bad research and causes harm. Manāra will actively seek local expertise to inform research design in contexts where its own team has limited experience.

4. Informed Consent Standards

Informed consent is the foundation of ethical research. Obtaining valid informed consent is a process, not a form. A signature on a form does not constitute consent if the participant did not understand what they were agreeing to.

4.1 Elements of Valid Consent

To be valid, consent must be:

- Informed: The participant must have received a clear explanation of the study's purpose, what participation involves, what data will be collected, how it will be used, who will have access to it, and what their rights are.
- Voluntary: No coercion, undue pressure, or disproportionate inducements may be applied. Participants in dependent relationships with Manāra's clients (for example, beneficiaries of a program being evaluated) must be explicitly assured that their participation or non-participation has no bearing on their access to services or benefits.
- Comprehensible: Consent materials must be provided in a language and at a literacy level the participant can understand. In contexts of low literacy, oral consent with witness documentation is acceptable.
- Specific: Consent must be obtained for each distinct use of data. Where Manāra seeks to use data collected for one purpose for a secondary purpose, fresh consent must be obtained unless the data has been fully anonymised.
- Revocable: Participants must be informed that they may withdraw consent at any time without consequence. Upon withdrawal, their identifiable data must be deleted unless retention is legally required.

4.2 Consent Documentation

The standard for consent documentation varies by context:

- Written consent is the default and must be used for all research involving sensitive personal data, vulnerable populations, or data likely to be shared with funders or published.
- Oral consent, documented by the researcher in writing and countersigned by a witness, is acceptable where written consent poses safety risks to the participant, where literacy is limited, or where the formality of written consent would undermine participation in specific cultural contexts. The rationale for using oral consent must be documented in the project ethics file.
- Implied consent (for example, completion of an anonymous online survey with a clear information notice) is acceptable only for genuinely anonymous data collection with no sensitive content.

4.3 Enhanced Consent for Vulnerable Populations

Where research involves vulnerable populations, standard consent procedures are insufficient on their own. The following table sets out the enhanced requirements by population category:

Population Category	Protections Required	Consent Standard	Escalation Required
Children and minors (under 18)	Parental/guardian consent; child assent where appropriate; age-appropriate language; no identifying images	**Enhanced**	Yes
Survivors of gender-based violence	Trauma-informed protocols; survivor-led disclosure; no re-traumatisation; anonymisation mandatory	**Enhanced**	Yes
Internally displaced persons	Voluntary participation assured; no linkage to aid eligibility; interpreter provided where needed	**Enhanced**	Yes
Indigenous and minority communities	Community-level consent in addition to individual consent; culturally appropriate process	**Enhanced**	Yes
Government or institutional informants	Standard written consent; clarity on attribution policy	Standard	No
Private sector respondents	Standard written consent; confidentiality assured	Standard	No
General adult population	Standard written or verbal consent depending on methodology	Standard	No

4.4 Community Consent

For research conducted with indigenous communities, closely cohesive minority communities, or any community where collective decision-making norms apply, individual consent is necessary but not sufficient. Manāra must engage recognised community structures or representatives at the design stage to seek community-level agreement before individual recruitment begins. The process for seeking community consent must itself be culturally appropriate and must not assume that formal community structures speak for all members. Community consent does not override individual consent; it precedes it.

5. Data Collection, Storage, and Protection

5.1 Data Minimisation

Manāra will collect only the personal data that is genuinely necessary for the research objectives. Before any data collection instrument is finalised, the project lead must review each data field and confirm its necessity. Data that is 'nice to have' but not required for the analysis must not be collected. Where aggregate or anonymised data would serve the research purpose, individual-level identifiable data must not be collected.

5.2 Data Classification

All research data must be classified at the point of collection according to the following three-tier system:

- Tier 1: Public data. Fully anonymised data or data from public sources that presents no risk to individuals. No special handling requirements.
- Tier 2: Confidential data. Pseudonymised data, data from institutional informants who have requested confidentiality, and any data whose disclosure could cause professional or reputational harm. Must be stored in access-controlled systems. Not for external distribution without authorisation.
- Tier 3: Sensitive personal data. Identifiable data from vulnerable populations, data relating to health, violence, sexual orientation, migration status, or legal history. Must be encrypted, stored on systems accessible only to named individuals, and subject to enhanced handling and deletion protocols.

5.3 Storage and Access Controls

The following standards apply to all research data stored in Manāra systems:

- Tier 3 data must be encrypted at rest and in transit. Encryption must use current industry-standard protocols (AES-256 or equivalent).
- Access to identifiable research data is restricted to named team members with a documented operational need. Access permissions must be reviewed at the close of each project phase.
- Identifiable data must not be stored on personal devices without encryption and password protection. If a team member's device is lost or compromised, this must be reported to the Policy Owner immediately.
- Research data must not be shared via unsecured email. Secure file transfer methods must be used for all external data sharing.
- Cloud storage platforms used for research data must have data processing agreements reviewed before use. Platforms that process data in jurisdictions without adequate data protection laws may be used for Tier 1 and Tier 2 data only, with written approval from the Policy Owner.

5.4 Third-Party Tools and AI Platforms

The use of third-party digital tools, including AI-powered transcription, analysis, and writing platforms, for research data requires careful management. The following framework governs permitted and prohibited uses:

Tool Category	Permitted Use	Prohibited Use	Required Safeguard
AI transcription services	Transcription of non-sensitive interviews	Transcription of interviews with	Participant informed in consent form; data

	with institutional respondents	vulnerable populations, survivors, or minors	deleted from platform post-use
AI writing and analysis tools	Drafting, summarising, and editing non-sensitive research outputs	Processing identifiable participant data or verbatim quotes from sensitive interviews	No personal data input; outputs reviewed for accuracy before use
Cloud storage (Google Drive, OneDrive)	Storage of anonymised datasets and research outputs	Storage of identifiable data unless encrypted and access-controlled	Encryption enabled; access restricted to named team members
Video conferencing platforms	Remote interviews and focus groups with institutional respondents	Recording of sessions involving vulnerable populations without explicit consent to the platform	Recording only with consent; stored on secure internal system, not platform cloud
Survey tools (Google Forms, KoBoToolbox)	Quantitative data collection	Collection of sensitive personal data without verified data processing agreements	Data processing agreement reviewed; data exported and deleted from platform promptly

The Policy Owner must maintain an updated register of all third-party platforms used in research activities, including the data types processed and the basis for compliance with this Policy. This register is reviewed annually.

5.5 Cross-Border Data Transfers

Manāra's research frequently crosses jurisdictional boundaries, with data collected in Pakistan processed or shared with international clients, partners, or academic institutions. The following rules apply:

- Personal data relating to participants in Pakistan must not be transferred to jurisdictions without adequate data protection frameworks without explicit participant consent or equivalent safeguards.
- Where Manāra processes data related to EU residents, GDPR requirements apply regardless of where Manāra is headquartered. This includes lawful basis requirements, data subject rights, and breach notification obligations.
- Any cross-border data transfer must be documented in the project ethics file, including the receiving jurisdiction, the legal basis for transfer, and any safeguards applied.

6. Data Retention and Disposal

Data must not be retained longer than necessary for the purposes for which it was collected. The following retention schedule applies to all research data held by Manāra:

Data Category	Retention Period	Disposal Method	Rationale
Anonymised research datasets	10 years from project closure	Secure deletion	Secondary analysis value
Identifiable participant data	3 years from project closure, unless consent withdrawn earlier	Secure deletion with certificate	Legal minimum; minimise risk

Signed consent forms	5 years from project closure	Secure destruction	Audit requirement
Interview recordings (raw)	12 months post-transcription, unless participant consents to longer retention	Secure deletion	Minimise identifiability risk
Transcripts (anonymised)	10 years from project closure	Secure deletion	Research value
Project correspondence with participants	3 years from project closure	Secure deletion	Accountability
Financial records related to research	7 years	Secure deletion	Tax and audit compliance under Pakistani law

At the close of each project, the project lead is responsible for ensuring that retention schedules are applied, disposals are documented, and the ethics file is updated accordingly. Disposal of sensitive personal data must be confirmed in writing and records retained for audit purposes.

Where a donor or client contract specifies longer retention periods, the contract requirement governs, provided participants were informed of the retention period in their consent documentation.

7. Publication, Dissemination, and Attribution

7.1 Anonymisation in Publications

Research outputs published by Manāra, including policy briefs, research reports, working papers, blog posts, and presentations, must anonymise individual participants unless the participant has provided explicit written consent to be identified. Anonymisation must be meaningful: changing a name while retaining identifying contextual details (role, location, specific incident) does not constitute anonymisation. Where any doubt exists about whether a participant could be identified from published material, the safer approach governs.

7.2 Institutional Attribution

Attribution of quotes and findings to institutions or organisations, as distinct from named individuals, is permitted where the institutional position is relevant and the institution's leadership has been made aware of the research. Attributing views to an organisation that were expressed by one individual without institutional endorsement is misleading and must be avoided.

7.3 Community Access to Findings

Where research has been conducted with communities, Manāra commits to making findings accessible to those communities in a form they can understand and use. This does not require translation into every local language in every case, but it does require active consideration of how to share findings meaningfully. A research output that is only accessible to English-speaking international audiences does not discharge Manāra's obligation to the communities whose knowledge and experiences it drew upon.

7.4 Client Confidentiality and Research Integrity

Where research is conducted under a client commission, the client may legitimately require confidentiality of findings for a defined period. However, no client agreement may require Manāra to suppress, distort, or misrepresent research findings, to refrain from correcting factual inaccuracies in public discourse, or to attribute findings to sources that did not produce them. Manāra will not enter into contracts that compromise the intellectual integrity of its research outputs.

8. Data Breach Response

A data breach is any unauthorised access to, disclosure of, alteration of, or destruction of personal data. This includes loss of a device containing unencrypted research data, accidental emailing of identifiable data to an unauthorised recipient, and unauthorised access to research files by a third party.

8.1 Detection and Reporting

Any team member who discovers or suspects a data breach must report it to the Policy Owner within 24 hours of discovery. The report must include: what data may be affected, how many individuals may be affected, how the breach occurred or is suspected to have occurred, and what steps have already been taken.

8.2 Assessment and Containment

Upon receiving a breach report, the Policy Owner will assess the severity of the breach using the following criteria: the sensitivity of the data involved, the number of individuals affected, the likelihood of harm to those individuals, and whether the data has been accessed by an external party. Immediate containment measures must be implemented, including revoking access, securing affected systems, and recovering data where possible.

8.3 Notification

Where a breach involves Tier 3 sensitive personal data and there is a reasonable likelihood of harm to affected individuals, the following notifications are required:

- Affected participants must be notified as soon as practicable, in a manner appropriate to the context and the sensitivity of the situation. The safety of participants must be the primary consideration in deciding the timing and method of notification.
- Clients and donor partners must be notified in accordance with contractual obligations, typically within 72 hours of the breach being assessed.
- Where the breach involves data of EU residents, GDPR requires notification to the relevant supervisory authority within 72 hours and to affected individuals without undue delay.

8.4 Post-Breach Review

Within 30 days of resolving a data breach, the Policy Owner must conduct a documented review identifying the root cause, the adequacy of the response, and the measures implemented to prevent recurrence. This review must be presented to both Directors and retained in the governance file.

9. Roles and Responsibilities

9.1 Policy Owner: Chief Executive Officer

- Maintain and periodically review this Policy.
- Approve research design protocols for projects involving Tier 3 data or vulnerable populations.
- Maintain the register of third-party data processing tools.
- Assess and respond to data breach reports.
- Ensure all new team members and collaborators receive ethics induction before engaging on research activities.
- Report annually to the Board on research ethics compliance and any incidents or breaches.

9.2 Project Leads

- Complete a Research Ethics Checklist (Annex A) for every project before data collection begins.
- Develop and maintain a project ethics file containing consent forms, data classification records, storage protocols, and retention schedules.
- Ensure all team members and collaborators engaged on their project have read this Policy and signed the Research Ethics Declaration (Annex B).
- Monitor compliance with this Policy throughout the project lifecycle.
- Ensure timely disposal of data in accordance with the retention schedule at project closure.

9.3 All Team Members and Collaborators

- Read and comply with this Policy before engaging on any research activity.
- Sign the Research Ethics Declaration (Annex B) before participating in data collection.
- Report any concern about research ethics compliance or any data breach to the project lead or Policy Owner immediately.
- Participate in ethics induction and any training required by the Policy Owner.

10. Governance and Review

This Policy is approved by the Directors of Manāra Policy & Practice (Private) Limited — Maliha Shah and Ahmad Nadeem — and is recorded in the Directors' Resolutions register. Manāra operates with two Directors who together constitute the decision-making authority of the company. Policy approval does not require a formal board of the kind larger organisations maintain; it requires a documented resolution signed by both Directors. This Policy enters into force on the date of that resolution and supersedes any prior guidance on research ethics or data protection within the organisation.

This Policy will be reviewed annually. The Policy Owner will lead the review and present any proposed changes to both Directors for approval. A new signed resolution is required each time the Policy is amended. An interim review will be triggered by: a data breach, a material change in Manāra's research activities or geographic scope, the introduction of new digital tools that change

how research data is handled, or the enactment of the Personal Data Protection Act or the Regulation of Artificial Intelligence Act in Pakistan.

Any waiver of the requirements of this Policy in specific project circumstances must be approved in writing by the Policy Owner and documented in the project ethics file. A waiver of process does not excuse the underlying ethical obligation. Where legal counsel is required on a specific compliance question, Manāra will engage a qualified legal advisor on that basis.

11. Related Documents

- Code of Ethics and Professional Conduct
- Gender Equality, Inclusion, and Anti-Harassment Policy
- Financial Management Policy
- Consultant and Collaborator Agreement Template
- Conflict of Interest Policy
- Research Ethics Checklist (Annex A)
- Research Ethics Declaration (Annex B)

Directors' Resolution and Approval

We, the Directors of Manāra Policy & Practice (Private) Limited (CUIN: 0321127), having reviewed the Research Ethics and Data Protection Policy Version 1.0, hereby approve this Policy and resolve that it shall enter into force with immediate effect from the date of our signatures below. This resolution is recorded in the Directors' Resolutions register of the company.

Approved by **Maliha Shah** Chief Executive Officer & Founder Signature: *Approved electronically* Date: 27 February 2026	**Approved by** **Ahmad Nadeem** Director & Co-Founder Signature: *Approved electronically* Date: 27 February 2026

ANNEX A

Research Ethics Checklist

To be completed by Project Lead before data collection begins

This checklist must be completed and signed by the Project Lead for every project that involves primary data collection or the processing of personal data. It must be filed in the project ethics file before any participant engagement begins. Where a question is answered 'No' or 'Not sure', the Project Lead must consult the Policy Owner before proceeding.

Part 1: Project Details

Project Title	
Project Lead	
Client / Funder	
Date of Completion	
Geographic Scope	
Anticipated Data Collection Period	
Project Ethics File Reference	

Part 2: Participant and Population Assessment

Complete this section to identify the nature of participants and the level of ethical scrutiny required.

Question	Yes	No	N/A	Notes / Action Required
Does the project involve human participants?	☐	☐	☐	
Does the project involve children or minors (under 18)?	☐	☐	☐	
Does the project involve survivors of violence, trauma, or abuse?	☐	☐	☐	
Does the project involve internally displaced persons or refugees?	☐	☐	☐	
Does the project involve indigenous or minority communities?	☐	☐	☐	
Does the project involve individuals in a dependency relationship with the client (e.g. program beneficiaries being evaluated)?	☐	☐	☐	
Does the project involve participants in politically sensitive environments where identification could create safety risks?	☐	☐	☐	

Does the project involve government officials or others for whom attribution could have professional consequences?	☐	☐	☐	
Does the project involve collection of sensitive personal data (health, sexual orientation, legal history, migration status)?	☐	☐	☐	

If any of questions 2 through 9 are answered 'Yes', enhanced consent procedures apply. Refer to Section 4.3 of the Policy and consult the Policy Owner before designing the consent process.

Part 3: Consent and Participant Information

Question	Yes	No	N/A	Notes / Action Required
Has a Participant Information Sheet been prepared that explains: the study purpose, what participation involves, how data will be used, who will have access, retention period, and participant rights?	☐	☐	☐	
Is the Participant Information Sheet available in a language the participant understands?	☐	☐	☐	
Where written literacy is limited, has an oral consent protocol with witness documentation been prepared?	☐	☐	☐	
Has a consent form been designed that includes a revocation clause?	☐	☐	☐	
Where the project involves minors, has parental/guardian consent documentation been prepared in addition to child assent materials?	☐	☐	☐	
Where the project involves indigenous or closely cohesive communities, has a community consent process been designed and agreed with community representatives before individual recruitment?	☐	☐	☐	
Have participants been clearly informed that participation is voluntary and that declining or withdrawing has no consequences for their access to services or benefits?	☐	☐	☐	
Has the consent process been reviewed and approved by the Policy Owner where enhanced consent is required?	☐	☐	☐	
Where data will be shared with international partners or donors, have participants been informed of this in the consent documentation?	☐	☐	☐	
Where recordings will be made (audio or video), has explicit consent been obtained specifically for recording, separate from consent to participate?	☐	☐	☐	

Part 4: Data Classification and Storage

Question	Yes	No	N/A	Notes / Action Required
Has all data to be collected been classified as Tier 1 (Public), Tier 2 (Confidential), or Tier 3 (Sensitive Personal Data) in accordance with Section 5.2 of the Policy?	☐	☐	☐	
Is Tier 3 data limited to what is strictly necessary for the research objectives? Has a data minimisation review been completed?	☐	☐	☐	
Have storage systems been identified and confirmed as appropriate for the data tier (encryption for Tier 3, access controls for Tier 2 and above)?	☐	☐	☐	
Has access to identifiable data been restricted to named individuals with a documented operational need?	☐	☐	☐	
Are third-party platforms proposed for data collection, storage, or analysis? If yes, have their data processing terms been reviewed and recorded in the ethics file?	☐	☐	☐	
If AI tools will be used in the research process, has the applicable row of the Third-Party Tools table in Section 5.4 of the Policy been reviewed and applied?	☐	☐	☐	
Where data will be transferred internationally, has the legal basis for transfer been identified and documented?	☐	☐	☐	
Has a project-specific data retention and disposal schedule been prepared and filed?	☐	☐	☐	
Is there a named individual responsible for executing data disposal at project close?	☐	☐	☐	

Part 5: Risk to Participants and Do No Harm Assessment

Question	Yes	No	N/A	Notes / Action Required
Has a risk assessment been conducted identifying potential harms to participants (physical, psychological, social, economic, legal, reputational)?	☐	☐	☐	
Could participation in this research expose participants to increased risk from authorities, community members, family members, or other parties?	☐	☐	☐	
Could publication of findings, even with anonymisation, allow identification of individuals in small or closely-knit communities?	☐	☐	☐	
Has a plan been developed to manage foreseeable adverse reactions during data collection (e.g. distress during interviews on sensitive topics)?	☐	☐	☐	

Are referral pathways available for participants who may need psychological, legal, or other support as a result of participation?	☐	☐	☐	
Have research methods been reviewed for potential cultural insensitivity, power imbalances, or structural bias in whose knowledge is centred?	☐	☐	☐	
Have local experts or community representatives been consulted to review the research design for contextual risks not identified by the core team?	☐	☐	☐	
Could the research data, if accessed by an unauthorised party, create risks for participants beyond ordinary life circumstances?	☐	☐	☐	
Has a plan been developed for securely destroying raw data if a security risk to participants emerges after collection?	☐	☐	☐	

Part 6: Team Readiness

Question	Yes	No	N/A	Notes / Action Required
Have all team members and collaborators engaged on this project read the Manāra Research Ethics and Data Protection Policy?	☐	☐	☐	
Have all team members and collaborators signed the Research Ethics Declaration (Annex B) for this project?	☐	☐	☐	
Have field enumerators or interviewers received briefing on ethical data collection protocols specific to this project?	☐	☐	☐	
Where interpreters are engaged, have they been briefed on confidentiality obligations and signed a confidentiality undertaking?	☐	☐	☐	
Is the Project Lead contactable throughout the data collection period to address ethical issues that arise in the field?	☐	☐	☐	
Has a clear escalation pathway been communicated to all team members for raising ethical concerns during the project?	☐	☐	☐	

Part 7: Checklist Sign-Off

I confirm that I have completed this checklist honestly and to the best of my knowledge. Where items are marked 'No' or where notes indicate required actions, I commit to resolving those items before data collection begins or to seeking approval from the Policy Owner for any justified exception.

Project Lead	Policy Owner Review (required where enhanced consent applies)
Name: _____	Name: _____
Signature: _____	Signature: _____
Date: _____	Date: _____

Completed checklists must be filed in the project ethics file. A copy must be submitted to the Policy Owner for all projects involving enhanced consent requirements.

ANNEX B

Research Ethics Declaration

To be signed by every team member and collaborator before engaging on research activities

This Declaration must be signed by every individual who will collect, process, store, or have access to research data as part of a Manāra project. This includes core team members, collaborators, field enumerators, interpreters, and any third party engaged on research activities under Manāra's contractual responsibility. The signed Declaration must be filed in the project ethics file before the individual engages in any participant-facing activity.

Section 1: Declarant Details

Full Name	
Role on this Project	
Organisation / Affiliation	
Project Title	
Project Lead	
Date of Declaration	

Section 2: Declarations

By signing this Declaration, I confirm each of the following statements. I understand that a false declaration may result in removal from the project and may constitute a breach of my engagement agreement with Manāra.

☐	**Policy Review** I have read and understood the Manāra Research Ethics and Data Protection Policy (v1.0) in its entirety. I understand that this Policy is binding on me for the duration of my engagement on Manāra research activities.
☐	**Participant Welfare** I commit to treating every research participant with dignity and respect. I will not subject any participant to coercion, deception, undue pressure, or any form of conduct that could cause physical, psychological, social, economic, legal, or reputational harm.
☐	**Voluntary Participation** I understand that participation in research must be entirely voluntary. I will not imply, suggest, or state that a participant's access to services, benefits, employment, or any other resource depends on their participation or non-participation in research.
☐	**Informed Consent** I will obtain valid informed consent from every participant before collecting any data, using the consent procedures approved for this project. I will not begin data collection from any individual who has not given consent or who has withdrawn consent. Where a participant withdraws

	consent, I will immediately cease collection from that individual and report this to the Project Lead.
☐	**Enhanced Protections** Where I am working with vulnerable populations, including children, survivors of violence, displaced persons, or indigenous communities, I will apply the enhanced consent procedures and participant protections required by the Policy and communicated to me in my project briefing.
☐	**Data Handling** I will handle all personal data in accordance with the classification, storage, access, and transfer requirements of the Policy. I will not store personal data on unencrypted personal devices, share it via unsecured channels, or use it for any purpose other than those stated in the participant consent documentation.
☐	**Third-Party Tools** I will not input identifiable personal data or sensitive participant information into AI platforms, cloud tools, or third-party services except as expressly permitted by the Policy and the Project Lead.
☐	**Confidentiality** I will maintain the confidentiality of all participant information, client information, and unpublished research data that I access in the course of this project. This obligation continues after the conclusion of my engagement on the project.
☐	**Conflict of Interest** I am not aware of any personal, financial, or professional interest that would compromise my ability to conduct this research impartially. If a potential conflict arises during the project, I will disclose it to the Project Lead immediately.
☐	**Intellectual Honesty** I will report data accurately and honestly. I will not fabricate, falsify, selectively omit, or misrepresent research data or findings. I will clearly distinguish between evidence and interpretation in my work.
☐	**Breach Reporting** If I become aware of, or suspect, a data breach, an ethics violation, or conduct that is inconsistent with this Policy, I will report it to the Project Lead or the Policy Owner immediately. I understand that failure to report a known breach may itself constitute a policy violation.
☐	**Continuing Obligation** I understand that my obligations under this Declaration apply throughout the project lifecycle, including after data collection has concluded, and that the confidentiality obligation is indefinite.

Section 3: Acknowledgement of Project-Specific Protocols

Complete this section to confirm receipt and understanding of project-specific ethics guidance.

	Item	Received	N/A
1.	Project ethics briefing from Project Lead	☐	☐
2.	Participant Information Sheet for this project	☐	☐
3.	Consent form template for this project	☐	☐
4.	Data classification and storage instructions for this project	☐	☐
5.	Escalation and breach reporting contacts for this project	☐	☐
6.	Any population-specific protocol for vulnerable groups involved in this project	☐	☐

Section 4: Signature

I have read and understood every declaration in Section 2 of this document. I sign this Declaration freely and without duress. I understand that it is a binding commitment for the duration of my engagement on Manāra research activities and that my confidentiality obligations continue indefinitely thereafter.

Declarant	Witnessed by (Project Lead)
Full Name: _____	Full Name: _____
Signature: _____	Signature: _____
Date: _____	Date: _____

The signed original of this Declaration must be retained in the project ethics file. Where a Declaration is signed electronically, a PDF copy bearing the electronic signature constitutes the original for filing purposes.

Escalation contacts for ethical concerns arising during this project:

Contact	Name	Email / Phone
Project Lead		
Policy Owner (CEO)		
Alternative escalation		