IIRR Global Artificial Intelligence (AI) Policy

Introduction

This Global Artificial Intelligence (AI) Policy establishes the framework for the ethical, responsible, and secure development, procurement, and use of AI tools across IIRR. As a global organization working with rural communities and vulnerable populations, IIRR recognizes that AI technologies—while offering significant opportunities to enhance operational efficiency, knowledge management, and program impact—also introduce new risks related to privacy, data governance, bias, misinformation, and accountability.

This policy provides guidance to ensure that the adoption of AI aligns with IIRR's mission, values, and legal obligations, while protecting the rights and dignity of the individuals and communities we serve.

Objectives

The primary objective of this policy is to ensure that all AI systems used within IIRR support organizational goals without compromising data security, ethical standards, or beneficiary protection. It also aims to promote awareness of AI risks, set clear expectations for responsible use, identify appropriate governance mechanisms, and establish procedures for assessing and mitigating potential harms. By standardizing AI practices across global offices, the policy ensures consistency, transparency, reliability, and trust in all AI-assisted processes implemented within the organization.

Scope and Applicability

This policy applies to all IIRR staff, including employees, contractors, interns, volunteers, consultants, and third-party partners who use, deploy, procure, or interact with AI tools on behalf of the organization. The policy covers all AI systems and technologies, including but not limited to generative AI tools, machine learning models, automated decision-support systems, chatbots, data analytics platforms with predictive algorithms, and any software or digital tool that incorporates AI functionality. It applies across all offices and program locations worldwide and governs both organizational and externally provided AI solutions.

AI Governance and Organizational Responsibilities

The Global Headquarters holds responsibility for defining AI strategy, standards, and protocols, under the leadership of the Director of Global Operations in coordination with relevant program and compliance units and staff. Each regional or country office must designate an AI focal point who will work closely with the local IT focal point to ensure that all AI use complies with global standards, data protection laws, and contextual considerations. Any plans to adopt, develop, or integrate AI systems must be reviewed and approved by Headquarters before implementation to

ensure alignment with security, ethical, and operational requirements. Major AI-related initiatives must include risk assessments, legal reviews, and data governance evaluations.

Acceptable Use of AI Systems

AI tools are intended to enhance productivity, decision-making, and program delivery but must always be used responsibly and professionally. Staff may use approved AI systems for tasks such as summarizing information, drafting content, data analysis, translation, and workflow optimization, provided they maintain accuracy, confidentiality, and adherence to organizational guidelines. AI tools must never be used to produce misleading content, make automated decisions that affect beneficiaries without human oversight, or generate outputs that could damage IIRR's credibility or violate local laws.

Personal use of AI systems integrated into IIRR infrastructure is allowed only if it does not interfere with work responsibilities, compromise security, or involve inappropriate or sensitive content.

Ethical Use, Bias Mitigation, and Safeguarding

AI systems must be used ethically, with particular attention to the risks of bias, discrimination, misinformation, and potential harm to vulnerable groups. Staff must recognize that AI-generated information can be inaccurate or biased and must therefore critically evaluate outputs before relying on them for decision-making or communication.

AI must not be used in ways that perpetuate inequity, compromise human dignity, or influence communities through manipulation or automated profiling. Program data containing sensitive personal details must never be entered into external AI tools unless express permission has been granted and proper anonymization has been applied.

In all cases, human judgment remains central, and AI must support—not replace—professional expertise and beneficiary safeguarding responsibilities.

Data Protection, Privacy, and Confidentiality

All use of AI must comply with IIRR's Data Management Policy, international data protection laws such as the GDPR, and applicable national regulations. Staff must not input confidential, sensitive, or personally identifiable information into AI systems unless the tool has been approved by Headquarters for such use and meets required security and privacy standards. Where possible, data must be anonymized or pseudonymized before being processed by AI systems.

AI-generated outputs containing personal or sensitive information must be handled with the same level of protection as other organizational data. External AI vendors must provide verifiable assurances of data protection, model security, and compliance with relevant laws before their tools may be adopted.

AI Procurement, Development, and Integration

All AI-related procurement or development must adhere to IIRR's global guidelines for IT and digital systems. Before acquiring or deploying any AI system, the local AI focal point must consult with Headquarters to confirm compatibility with existing infrastructure, cybersecurity standards, and legal requirements. AI systems must undergo thorough evaluation, including risk assessments, bias reviews, vendor security checks, and cost-benefit analyses.

Staff are prohibited from independently deploying unapproved AI tools, browser extensions, open-source models, or third-party applications that have not been properly vetted. When integrating AI into existing workflows, offices must ensure that technical documentation, user training, and monitoring mechanisms are established.

Transparency, Documentation, and Accountability

All AI-supported work must be transparent and accountable. When AI outputs significantly inform organizational decisions, staff must document how the AI was used, the limitations of the tool, and the rationale for relying on its output. It must always be clear to internal and external stakeholders when AI has been used to produce content, analysis, or recommendations – particularly in research, public communications, monitoring and evaluation, and donor reporting. Staff remain responsible for the accuracy and appropriateness of all AI-assisted work. Accountability cannot be delegated to AI systems, and no AI tool may be used to make final decisions involving resource allocation, beneficiary eligibility, hiring, disciplinary actions, or other sensitive matters.

Security and Risk Mitigation for AI Systems

AI tools carry unique cybersecurity risks, including data leakage, model manipulation, prompt injection attacks, and exposure of confidential information. As such, AI systems must adhere to IIRR's cybersecurity standards alongside additional protections specific to AI. Only secure, approved platforms may be used, and systems must be updated regularly to address emerging threats. Staff must not use AI systems to bypass security protocols, create unauthorized software, generate harmful content, or manipulate digital infrastructure. Regular assessments of AI-related risks—including misuse, privacy breaches, and external threats—will be conducted at both headquarters and country-office levels.

Training, Awareness, and Capacity Building

IIRR is committed to building staff capacity to use AI responsibly and effectively. All staff must complete foundational AI training during onboarding and periodic refresher modules thereafter. These trainings will focus on ethical use, data protection, risk mitigation, bias awareness, and practical application of approved AI tools. Specialized training will be provided for teams working with sensitive data, developing AI-integrated workflows, or conducting technical evaluations. A culture of responsible AI use is encouraged, where staff actively question outputs, flag concerns, and prioritize human oversight.

Last update: December 2, 2025

Monitoring, Compliance, and Enforcement

IIRR reserves the right to monitor the use of AI systems on organizational networks in accordance with applicable laws and privacy standards. Regular audits, evaluations, and reviews will be conducted to ensure compliance with this policy, identify emerging risks, and continuously improve AI governance. Staff who violate this policy—including through misuse of AI tools, disclosure of sensitive information, or unauthorized procurement—may be subject to disciplinary action, including loss of access privileges, formal reprimands, or termination, depending on the severity of the breach. All offices are required to report concerns or incidents related to AI misuse promptly to Headquarters.

Policy Review and Revision

This AI Policy is a living document and will be reviewed annually or more frequently as AI technologies evolve, legal requirements change, or organizational needs shift. Revisions will be coordinated by the Global Headquarters in consultation with IT, Legal, HR, and program leadership, ensuring that updates reflect global best practices, safety considerations, and ethical standards. Staff will be notified of any changes and may be required to complete supplementary training or updated policy acknowledgements as part of the implementation process.

Conclusion

AI technologies present significant opportunities to enhance IIRR's work, but they must be approached with caution, responsibility, and respect for the communities we serve. This policy provides a unified global framework that protects data, promotes ethical practices, and ensures that AI use supports IIRR's mission of empowering rural communities. Every staff member shares responsibility for using AI safely, transparently, and effectively. Adherence to this policy will strengthen organizational integrity, safeguard beneficiaries, and uphold the trust of donors, partners, and stakeholders across the world.