Anyone can build AI. Not everyone can build AI with an ethical story. This is why you should work with me.

Closing Statement: A Self-Reliance Model for Refugee Camps—Built for Just 1,000 Dollars

This pilot is not a theoretical concept. It is a fully realizable, self-reliant model designed for refugee camps—and it can be built for less than 1,000 dollars. The cost is not just low; it is deliberate. It reflects a model that is simple enough to start immediately, modular enough to be assembled locally, and human-centered enough to be owned by the very communities it serves.

This entire initiative began with a simple but urgent question: What does a child with a developmental disability truly need in a refugee camp?

Not cloud infrastructure.
Not millions in R&D.
Just one small thing—
A wearable object they can hold, love, and trust.
A device that speaks to them, protects them, and becomes part of their daily life.

And yes, it can be built.
This is not speculative. It is demonstrable.

Using a few 28nm chips,
a repurposed toy board from Shenzhen,
a cartoon-shaped 3D-printed shell,
and a basic AI system that a single undergraduate can program—
the first prototype can be assembled with local labor and low-cost materials.

**The initial function of the AI is not recognition. It is attachment.
If the child does not want to wear it, nothing else matters.
The true architecture is not digital, but emotional.**

**In fact, the MVP's primary goal is not to impress but to belong—
to help the child form a bond with the object,
and to help the parent believe that someone, somewhere, has not forgotten them.**

**This is the starting point of my design.
Because in the case of children with developmental disabilities, emotional consistency and trust must come before any technical functionality.
Even the most advanced AI is meaningless if the child refuses to wear the device.**

**That is why this MVP is deliberately simple.
Not because simplicity is cheap—
but because it enables something more powerful: local ownership.**

**The full cost of assembling and field-testing a working prototype is less than USD 1,000.
This includes labor, materials, and basic 3D printing support.
I am fully prepared to cover this cost personally.**

**This amount is not symbolic. It is operational.
It demonstrates that a self-reliant assistive technology model can begin in a refugee camp—
with local technicians, unemployed youth, and caregivers taking part in the build process.
The goal is not to create dependency but to create systems that communities can call their own.**

**Major international actors—including UNHCR, IOM, GIZ, and USAID—have all publicly endorsed a shift
from short-term cash aid to long-term self-reliance strategies.
This pilot is a practical expression of that same vision.**

**A copy of this proposal has also been shared with the relevant thematic unit at the SIDA headquarters,
in the interest of exploring both regional and global coordination.**

**I do not ask for funding.
I simply ask for the opportunity to show what is possible.
Not through a brochure,
but through a real object,
in a real setting,
serving real children.**

**One working prototype.
One thousand dollars.
One chance at trust.**

Let us begin—with that.

Anyone can build AI. But building AI with integrity, purpose, and ethics — that's rare. That's why you should work with me.

"I am a national of the Republic of Korea."

Gyu-min Jeon (also known as Morgan J.)

I was born on January 17, 1982.

Email: gyumin.jeon.childsafe@gmail.com
My backup email is jekymin8232@gmail.com

I would like to mention that I am not fully fluent in spoken English. If you

have any questions or follow-up inquiries, I would greatly appreciate it if you could send them to me by email. Thank you very much for your understanding.

Full compliance with international standards such as GDPR, COPPA, and CCPA.

The protection of children's personal information—especially that of children with disabilities—must take absolute priority over any technological advancement. This project fully embraces that principle at the core of its design.

The AI-powered safety necklace for children with disabilities does not collect any personal identifying information such as names, birthdates, addresses, or photographs. Each device is assigned a unique identification number, which serves as the sole point of reference for communication with the central AI server. If the child switches to a new device, parents simply input the new device number through the companion smartphone app. The app never asks for the child's or guardian's personal information; the device number itself functions as the user ID.

The usage process is as follows:

1. **The caregiver purchases the child safety necklace.**
2. **A tamper-proof sticker on the device conceals the unique number. Once the sticker is removed, the number becomes visible.**
3. **The caregiver opens the app, enters the device number, creates a user ID and password, and completes the registration.**
4. **During registration, the caregiver is asked to describe the child's characteristics, behavioral patterns, or disability-related sensitivities in detail.**

The information submitted is strictly behavioral and anonymous in nature. No names or identifiers are ever

requested. This structure allows caregivers to share their child's unique traits honestly, without fear of stigma or social judgment. This is a key advantage of the system—enabling a highly personalized AI response without compromising privacy.

This model strictly follows internationally recognized standards such as GDPR, COPPA, and CCPA by employing a zero personal data collection policy**. The number-based identification system is comparable to the tokenized security infrastructure used in the financial sector, offering a high level of technical safety. To further protect the device number, it is sealed with a sticker that must be manually removed. Even in the unlikely event of a data breach, there is no risk of personal information leakage because none is stored on the server.**

In conclusion, this design combines technical security, ethical integrity, practical usability, and full compliance with global privacy standards. It represents one of the most advanced strategies in the world for protecting the personal data of children.

Security can always be breached. The best security policy is to physically store no personal information at all.

zero data retention

The core strategy of this project is to design a system that collects no personal information whatsoever. This goes beyond strengthening cybersecurity—it represents a fundamental design philosophy that eliminates risk at the structural level. The following seven elements are central to this strategy and demonstrate both its feasibility and its strength under international scrutiny.

1. **Even if the behavioral data collected is fully anonymized, its storage location, encryption level, and deletion protocol must be clearly**

defined in order to achieve full compliance with international standards such as the GDPR. A transparent policy on how this anonymous data is transmitted, stored, and erased is essential for ensuring the system's ethical integrity.

2. **Because the device's unique identification number acts as the sole login ID, there is a potential risk that someone could gain unauthorized access by copying or misusing this number. To mitigate this, several safeguards are necessary:**

- **First, a two-layered security system should be implemented using both the unique ID and a user-generated passcode.**
- **Second, the system must physically prevent unauthorized re-registration by anyone other than the original caregiver. For example, if the device is resold or lost, the serial number cannot be reused or re-registered by a third party. Even if someone buys the device second-hand, the registration process will recognize it as already linked and will block access.**
- **Third, if a device needs to be re-registered—such as when the caregiver forgets their login credentials—only the original serial number can trigger the reactivation process. No email address, phone number, or personal detail is required. However, there is a strict limit: only three attempts at re-entering the user ID and password are allowed. If more than three attempts are made, the device becomes locked and must be physically replaced with a new unit. This ensures that only the original caregiver can access or reset the device, while deterring abuse or unauthorized usage.**

3. **Caregivers will receive clear instructions never to enter personal information such as names, birthdates, or addresses when describing the child's behavioral traits, sensitivities, or disability-related needs. The system only accepts anonymous behavioral descriptions to maintain full privacy and prevent social stigma.**
4. **The system is fundamentally offline. A centralized AI server performs temporary analysis of the child's behavioral data only once, then transmits the pattern to the individual device. Once the transmission is complete, the server automatically deletes the data.**
5. **If the caregiver later decides to delete the behavioral profile from the device or wishes to update it, the server will temporarily accept the new data for analysis and transmit the revised pattern. Again,**

once this process is completed, the server deletes the temporary data immediately and irreversibly.

6. **In this architecture, the central AI server never retains personal data or behavioral profiles long-term. Even in the unlikely event of a security breach, there is no data to extract. This reflects a "zero data retention" model—one of the strongest safeguards against digital intrusion.**
7. **Technically, all components of this strategy are feasible. They rely on already available technologies such as IoT-enabled devices, companion mobile apps, device-level authentication, and automatic server-side deletion systems. This is not an abstract idea; it is a practically achievable, high-integrity design.**

Importantly, this decentralized AI architecture—built on the principles of "offline learning + temporary server analysis + automatic deletion"—contrasts sharply with conventional AI systems that store and accumulate user data on centralized servers. This model is conceptually aligned with federated learning and is considered a next-generation privacy-by-design approach in AI ethics.

The core philosophy is not to "block hacking," but rather to "design a system in which there is nothing to steal even if hacking occurs." That is, the risk is neutralized by removing sensitive information entirely from the system.

Traditional systems, even when encrypted, still contain sensitive data like names, birthdates, and location history. In contrast, this system holds none of that. This makes it not just secure—but structurally invulnerable to meaningful data leaks. It does not rely on encryption alone; it removes the risk by removing the data.

While many regulations such as GDPR advocate for the principle of "collect only what you need," this project goes further by embodying a "collect nothing at all" policy. That makes it legally defensible and ethically strong—particularly when working with high-risk populations such as children, persons with disabilities, and refugees.

In conclusion, this is not merely a cybersecurity framework. It is an ethical architecture. No real names, biometrics, or sensitive dates are ever stored.

There is no social stigma risk, no reputational harm, and virtually no privacy liability. The unique ID functions like a tokenized key, similar to those used in secure financial systems.

This design is, in many ways, one of the most advanced privacy-first approaches in the world. Its aim is not to resist intrusion—but to render intrusion meaningless.

The goal of this system is not to block intrusion—but to render it meaningless. While most systems focus on preventing hacking attempts, this approach is designed so that even if a breach occurs, there is nothing of value to be stolen. This is not just a theoretical concept, but a practically implementable ethical design—and one of the most advanced protection strategies in the world.

To prevent children from misusing or tampering with the registration process, the smartphone companion app for the AI-powered safety necklace is not available through public platforms such as Google Play or the Apple App Store. Instead, the app can only be downloaded by the child's legal guardian through the official website, mcorp-ai.com&mcorpai.org This restricted access ensures that only parents or caregivers with verified credentials can obtain the application.

To download the app, the guardian must provide two pieces of information on the website:

1. **The unique device serial number assigned to the child's safety necklace**
2. **The last four digits of the guardian's mobile phone number (e.g., if the number is 010-1234-5678, the required input would be 5678)**

After verification, the app is securely sent to the registered phone number. However, to protect against misuse or repeated reinstallation, app access is strictly limited to a maximum of three downloads per device. This policy is clearly stated and

enforced. After the third attempt, all associated credentials—including the serial number and phone number—are permanently invalidated, and a new device must be purchased to regain access.

To prevent unauthorized access by the child, who may repeatedly attempt to request the app through the website, an additional security layer based on open-ended, personal questions is required. These questions are defined by the parent during initial registration and may include prompts such as:

- **What is your favorite color?**
- **What number is most meaningful to you?**
- **What is your wedding anniversary?**

The system only accepts responses that match all three predefined answers, known exclusively to the parent or guardian. Only after successfully answering all three questions, along with entering the device serial number and phone number suffix, can the user reset their login credentials and download the app again.

This approach ensures a highly secure and parent-controlled app distribution process, minimizing any risk of unauthorized use while maintaining accessibility for the intended caregiver.

Finally, mcorp-ai.com&mcorpai.org, as the official platform and data controller, must operate with full transparency and accountability. It must clearly present privacy policies and terms of use that comply with international standards such as the GDPR. No personal data beyond what is absolutely necessary should be collected or stored, and all practices must reflect the principles of ethical data governance.

Localized Assembly of AI Safety Necklaces and Refugee-Led Ecological Economies
A rights-based, sustainability-aligned model in line with the European Green Deal and the Sustainable Development Goals (SDGs)

A. Overview

This initiative proposes a rights-based, community-driven approach to inclusive innovation through the localized assembly and deployment of AI-powered wearable devices—hereafter referred to as "AI Safety Necklaces"—specifically designed for children with developmental and physical disabilities. These devices operate entirely offline, collect no personal data, and offer both daily guidance and emergency support, thereby enhancing safety and autonomy for children living in displacement-affected and low-resource settings. The broader aim is to establish an integrated, locally owned ecosystem of employment, healthcare, and sustainability within refugee communities. The model is structurally aligned with the EU's Green Deal, the Sustainable Development Goals (SDGs), and the principles of a Rights-Based Approach.

B. Technological Design and Manufacturing Feasibility

The AI Safety Necklace incorporates low-power, lightweight AI chips and functions effectively with 28nm technology—a mid-range, cost-efficient semiconductor process optimized for low-energy applications. This enables scalable collaboration with emerging semiconductor-producing countries such as India and Vietnam, thereby reducing dependency on high-cost advanced foundries. Designed in the form of child-friendly character pendants, the necklace can accommodate larger dimensions, enhancing modular layout, durability, and ease of assembly—features that make it ideal for localized, small-batch manufacturing.

C. Community-Based Assembly and Refugee Employment

The device's assembly process is intentionally simple, consisting of modular chip installation, circuit connection, and

casing attachment. It requires no prior technical expertise, allowing displaced persons to participate effectively after one to two days of basic training. Instead of high-cost formal employment, the model emphasizes inclusive micro-employment—enabling a greater number of individuals to gain livelihoods while stimulating localized economic activity. Quality control is maintained through visual instruction guides and a minimal supervisory framework, ensuring accessibility and scalability in fragile contexts.

D. Tent-Based Assembly Sites and Integrated Services

Each pop-up assembly site requires only essential tools and electricity, and can be established for an estimated USD 1,000 to 3,000. These are more than production spaces—they also serve as decentralized hubs offering basic healthcare and food distribution. Medical essentials and staple foods such as maize, wheat, and protein sources are provided free of charge to workers and residents alike, thereby strengthening food and health security through a layered, community-wide safety net.

E. Cooperative Ownership and Internal Solidarity Mechanisms

Refugees employed in assembly are offered cooperative shareholding status. A portion of their income is voluntarily pooled into a solidarity fund that supplies food and medicine to non-employed community members. This model extends beyond transactional labor by promoting ownership, accountability, and mutual aid. External corporations are invited to purchase equity in these cooperatives, thereby contributing directly to community welfare while advancing ESG and CSR metrics and qualifying for ethical certification labels such as M-Corp.

F. Corporate Partnerships and ESG Integration

Global firms may support this model by acquiring shares in refugee-led cooperatives, directly contributing to asset-building for displaced persons. These contributions can be reported as positive ESG performance and social impact under sustainability disclosure standards. For refugees, selling their equity stakes enables access to start-up capital—facilitating

microenterprise initiatives such as food trucks, community agriculture kits, and ecological souvenir businesses. This, in turn, fosters a resilient, locally anchored entrepreneurial ecosystem.

G. Long-Term Vision: Ecological Economy and Community Tourism

All operational revenue from the AI assembly program is reinvested into the construction of ecological infrastructure within refugee settlements. This includes the development of biodiverse ecological parks designed to promote agroecology and sustainable land use. Activities include compost-based earthworm cultivation and the production of high-quality organic soil, positioning the community as a net exporter of bio-based agricultural inputs. In parallel, these ecological zones can host community-led ecotourism initiatives—attracting visitors, fostering cultural exchange, and creating new income streams through the sale of local goods and services.

H. Transparency and Public Sector Partnership Pathways

To ensure accountability, this model can be co-administered through transparent financial and operational partnerships with NGOs or United Nations agencies. It is highly adaptable for pilot projects funded through EU digital inclusion grants, development cooperation instruments, and emergency response frameworks. As a decentralized, community-led innovation in both technology and inclusive economics, it offers a compelling model for European public institutions seeking to support refugee-led ecological resilience and digital equity.

A Cooperative Solidarity Mechanism in Refugee Communities: “One Job Sustains Ten Lives”

This model transcends conventional job creation by establishing a solidarity-based ecological economy rooted in mutual aid and

collective responsibility. Within the cooperative assembly program, each employed refugee participates not merely as a worker, but as a shareholding member of the cooperative. A designated portion of their income is voluntarily contributed to a Solidarity Fund, a community-managed pool used to distribute essential food and medicine to non-employed members of the settlement.

This structure enables a single productive role to safeguard the survival and dignity of up to ten individuals, reflecting a dynamic where economic participation directly translates into social protection. In fragile environments, this configuration functions as both a livelihood guarantee and a community-anchored resilience mechanism.

Rather than reinforcing dependency through traditional wage labor, this system embodies the principles of Creating Shared Value (CSV), the Social and Solidarity Economy (SSE), and ethical asset redistribution. Participating as cooperative shareholders empowers individuals not only economically, but also symbolically—restoring agency, dignity, and ownership over one’s future.

This is not simply a model of employment.
It is a model of collective security, distributed agency, and inclusive recovery.