BEACONMATCH

The Ethical Framework

Title: BeaconMatch Privacy & Ethical Data Framework: Privacy by Design

Overview BeaconMatch is a digital public good intended for humanitarian aid. Unlike traditional social networks that thrive on data collection, BeaconMatch operates on a "Need-to-Know" basis to protect vulnerable populations in crisis zones.

Core Privacy Pillars * The Principle of Ephemeral Data: Data within the BeaconMatch mesh is temporary. Once a mission is verified via the QR Handshake, the associated "Need Card" and location data are immediately purged from the local mesh history.

- Anonymity & Mesh Identifiers: The system does not broadcast personal identifiable information (PII). It utilizes randomized "Mesh IDs" rather than phone numbers or real names for initial broadcasts.
- Identity Disclosure: Real names or "Verified Badges" are only revealed to a peer once a "Match" is confirmed through a Mutual Swipe.
- No Permanent Logs: Because there is no centralized server, there is no permanent history of user movements or requests that can be compromised.

Resistance to Surveillance * No "Kill Switch": Because the network is peer-to-peer and decentralized, no government or external entity can shut down the local network by disabling a central server.

- Metadata Protection: Local communication is end-to-end encrypted (AES-256), ensuring that third-party nodes passing a message cannot read its contents.

Ethical Integrity * "Bad Actor" Flagging: Local nodes can collectively ignore or "mute" a Mesh ID broadcasting fraudulent requests or harassment to maintain the integrity of the survival net.