

Privacy, Consent and Responsible AI

Public principles for user authority, consent-based memory, privacy controls, safety, and honest development status.

Publisher	GGIRL Technologies LLC
Version	Version 1.0
Publication date	July 30, 2026
Primary domain	ggirltechnologies.com

Public status notice

This document distinguishes live assets, verified development milestones, active development, partial verification, and planned capabilities. It does not promise profit, guaranteed product releases, or universal availability.

Purpose

The Velvet ecosystem is being designed around stronger user authority, consent, privacy controls, and human-centered AI. This paper describes design principles and development goals, not absolute guarantees of security, anonymity, or availability.

User Authority

Users should have meaningful control over identity, visibility, private places, connections, memories, content, supported wallets, and data-sharing choices. Product behavior must respect account boundaries and must not mix personal intelligence across users.

Consent-Based Memory and Actions

Velvet Eye and Velvet Brain are designed to use memory and context carefully. Sensitive actions, public sharing, location disclosure, corrections, and other meaningful changes should require appropriate user confirmation.

Privacy Controls

- Data minimization and purpose-limited collection.
- Visibility controls appropriate to the product and context.
- Private Safe Zones and named-place memory.
- No public wealth-flexing or unnecessary hierarchy signals.
- Separation of private identity, public content, and creator-authorized destinations.
- Clear distinction between design intent and currently available controls.

Responsible AI

AI should work for people rather than replace them. Velvet systems should explain uncertainty, avoid inventing verified facts, preserve human confirmation, and fail safely when a decision could affect safety, privacy, money, identity, or public data.

Safety and Validation

Navigation, perception, communication, and community systems are validated incrementally. Automated observations should not silently become canonical public data when user confirmation or stronger evidence is required.

Limits and Availability

Privacy and AI capabilities vary by product and development stage. No statement in this paper should be interpreted as a promise that every described control is currently deployed, legally sufficient in every jurisdiction, or immune from technical failure.