

SneakernetUSA Safe Haven Roadmap

· @GT

Purpose

Sneakernet gives every participant an air-gapped safe haven: a place where their ideas, files and intellectual property live out of reach of any network.

The guiding hypothesis: in the future there will be two kinds of AI, good and bad, and only one can offset the other. People starting out with few resources need a protected space for their work before they can safely use either.

Sneakernet operates as a program of UrbanFamilyUSA and serves the people it helps. The protocol is the product; the hardware is whatever carries it.

A second goal is education: helping people understand what about AI is actually worth fearing. People fear most what they don't understand, and a panic of misunderstanding could lead to banning all AI, good and bad alike. Clear understanding protects against both the real dangers and that overreaction.

Core principles

Five rules hold no matter what device a participant uses.

1. **Hardware-agnostic.** The protocol is written so it can convert whatever qualifying device a participant already has. No single brand or model is required.
2. **Dedicated device.** A vault is used only as a vault. A device that is also someone's everyday phone or computer cannot be air-gapped, whatever software it runs.
3. **Physical transfer only.** Files move in and out by encrypted removable media carried by hand. Never by WiFi, Bluetooth, cable to a networked machine, or cloud sync.
4. **Encryption at rest.** Every vault uses full-disk encryption, and every transfer drive is encrypted.
5. **Assume someone will try to get in.** Design for people trying to get around the air gap. Any device showing anomalies is isolated ("digital solitary") until checked.

Device qualification

A device qualifies as a vault at Tier 1 or Tier 2. Tier 3 devices stay the participant's everyday "outside" device.

Tier	Description	Qualifies as vault?	Example
1	Dedicated device, wireless radios physically removed, full-disk encryption	Yes (preferred)	Refurbished business laptop with WiFi/Bluetooth card pulled

2	Dedicated device, radios disabled in firmware/BIOS, full-disk encryption	Yes	Laptop or AIO whose WiFi is built onto the board
3	Still used daily, or radios only switched off in settings	No	Everyday phone, tablet in airplane mode

Teacher checklist before converting a device

- Participant agrees the device will be used only as a vault
- WiFi and Bluetooth removed (Tier 1) or disabled in firmware (Tier 2)
- Operating system version and security patch level verified, not taken from the box label
- Full-disk encryption turned on and passphrase recorded safely by the participant
- Encrypted transfer drive issued and tested
- Storage is reliable for long-term use (not a microSD card as the main store)

Transfer hygiene

The transfer drive, and the person carrying it, is the weakest point in the system; this routine protects it.

1. **Dedicated transfer drives.** Each participant's encrypted drive is used only for moving files to and from their vault, never for anything else.
2. **Check before it goes in.** Files are reviewed on the outside device before they are copied to the transfer drive.
3. **No autorun.** The vault never opens or runs anything automatically when a drive is inserted.
4. **Documents, not programs.** Only data files go into the vault; software is installed by a teacher during setup, not carried in later.
5. **Drive stays with its owner.** A transfer drive is never lent, shared, or plugged into an unknown machine.
6. **When in doubt, isolate.** A drive or vault acting strangely goes into "digital solitary" and is reported to the program lead.

Roadmap

[embed: node/9ea7317e-cbc7]

Each phase starts only when the gate before it is met. The pilot is the current phase; dates will be set once the vault location and reference laptop are decided.

Roles

Role	Who	Responsibilities
Founder / program lead	UrbanFamilyUSA	Owns the protocol, sets the reference setup, trains teachers, answers escalations

Teacher	Participants with natural teaching skill (est. 10-20%)	Qualifies and converts devices, teaches the transfer routine, reports problems back
Participant	People UrbanFamilyUSA serves	Keeps the vault dedicated, follows the transfer routine, protects the passphrase

Teachers are found by what they already do, such as helping neighbors with technology, rather than by who volunteers. Each teacher gets a kit: a printed walkthrough, a script for the first few conversions, and a direct line back to the program lead.

Open questions

- Will vaults live with participants at home, or at a central location where people bring files?
- Which refurbished laptop model becomes the reference device for the pilot?
- What anomalies should trigger "digital solitary"? (to be surfaced by live testing)
- Confirm with a nonprofit accountant or attorney: transferring Sneakernet to UrbanFamilyUSA, unrelated business income, private benefit rules
- Publish the concept openly under the nonprofit's name to establish it as the originator?
- What role, if any, do the existing A14 boxes play (e.g. AI assistant for participants rather than vaults)?

Resources

Free guides for members, teachers and the nonprofit. AI-driven attacks mostly use ordinary routes (scams, fake sites, malware, stolen passwords), so general digital-safety guides apply directly. Check each guide's license before printing or adapting it.

Audience	Resource	What it covers
Members	EFF Surveillance Self-Defense	Basics, tool guides, phishing, two-factor, password managers, privacy with AI tools; each guide shows a last-reviewed date
Members	Security in-a-Box	Beginner toolkit for protecting computers, phones and social media, with step-by-step software guides
Teachers	EFF Security Education Companion	Articles, lesson plans and teaching materials for community trainers
Teachers	Internews Field Guide to Incident Response	What to do after phishing, malware or a compromised device
Nonprofit	ICT4D Collective short guide for small civil society organisations	13-page, non-technical basics for low-resource organizations (v7, 2026)

Nonprofit [Access Now Digital Security Helpline](#)

Free direct help for civil society: incident response and community security strategy

Nonprofit [Digital protection guides comparison](#)

Front Line Defenders spreadsheet: update dates, Creative Commons licensing, languages