WORLD LIBERTY CONGRESS · PLAYBOOK FOR LIBERTY

Freedom Technologies for the WLC Network

A practical guide to Nostr, Bitcoin, Bitchat, and Artificial Intelligence for democratic activists.

Purpose: help WLC members use technology to protect, connect, document, learn, and coordinate without confusing tools with strategy.

Core idea: Freedom technologies are tools that reduce authoritarian control over communication, money, evidence, knowledge, and coordination. They do not replace trust, strategy, security discipline, or local judgment.

1. What are “freedom technologies”?

For the WLC, freedom technologies are tools that help democratic movements keep civic life alive when regimes censor information, monitor communications, freeze bank accounts, block organizing, distort narratives, or isolate exiles from people inside the country.

- They should increase safety, not just convenience.
- They should reduce dependence on authoritarian-controlled systems.
- They should protect privacy where possible.
- They should support accountability and careful documentation.
- They should be simple enough for non-technical activists to use safely.
- They should always be paired with training and do-no-harm rules.

2. Start with a threat model before choosing a tool

A tool is only useful if it matches the risk. Before using any technology, ask five questions:

- What are we trying to protect: identity, location, money, messages, evidence, contacts, or plans?
- Who are we protecting it from: the regime, hackers, trolls, police, platform abuse, or criminal actors?
- What happens if the information is exposed?
- Who needs access, and who does not?
- Is this tool safe enough for our actual users, not just for technical experts?

3. Nostr: decentralized communication that is not controlled by one platform

Nostr (“Notes and Other Stuff Transmitted by Relays”) is an open, decentralized protocol designed for censorship-resistant social media and messaging. It uses cryptographic keys for identity, eliminating the need for central servers, and allows users to own their data and move freely between different apps, called clients, while maintaining their network.

Term	Meaning	How WLC can use it
Nostr	“Notes and Other Stuff Transmitted by Relays.” An open, decentralized protocol for censorship-resistant social media and messaging. It uses cryptographic keys for identity and does not require one central	Use it for resilient public or semi-public communication, diaspora updates, verification of authentic voices, and publishing when centralized platforms are blocked or manipulated.

	server.	
Bitcoin	Open-source peer-to-peer money that can move value without relying on a single bank or payment company.	Use carefully for small, accountable, high-risk contexts where banking systems are weaponized, always with training, legal awareness, and records.
Bitchat	A peer-to-peer messaging tool that can operate over Bluetooth mesh networks without normal internet access.	Use as a backup for local, low-sensitivity communication during blackouts, events, or connectivity disruptions after prior testing.
Artificial Intelligence	Tools that can help draft, translate, summarize, analyze, train, and compare cases, but can expose sensitive data if used carelessly.	Use for learning and productivity with strict redaction rules. Do not enter names, locations, testimony, or operational plans into unsafe systems.

What this means in simple terms

Nostr is not one company, one app, or one website. It is a shared protocol. A user can choose different apps, connect through different relays, and keep the same identity through their cryptographic key.

Why it matters for the WLC

Authoritarian regimes often pressure or block centralized platforms. Nostr can help members maintain public or semi-public communication channels that are harder to silence because they do not depend on a single server or company.

Step 1: Create a small pilot group

Start with a small, low-risk group. Test one or two trusted Nostr clients. Do not move sensitive operations to Nostr until the team understands the tool and the risks.

Step 2: Protect keys

A Nostr private key functions like a digital identity. If it is lost, the account may be lost. If it is stolen, someone else can impersonate the user. Train members to store keys carefully and never share them in chats, email, screenshots, or cloud notes.

Step 3: Verify official accounts

Create a clear verification plan so supporters know which WLC, regional, or campaign accounts are authentic. Publish official Nostr identities through existing trusted channels.

Step 4: Use Nostr for resilient public communication, not for sensitive planning

4. Practical ways WLC can use Nostr

Nostr may be useful for censorship-resistant publishing, diaspora communication, emergency updates, member education, and maintaining a public presence when mainstream platforms are blocked, manipulated, or taken down. It should be treated as a resilience layer, not as the only communication channel.

- Use Nostr first for public or semi-public communication, not sensitive operations.
- Do not post private names, locations, case details, witness information, or internal plans unless cleared for public release.
- Treat cryptographic keys like identity documents: protect them carefully and train users before they publish.
- Create a verification plan so supporters know which accounts are authentic.
- Train members before asking them to use Nostr in a crisis.

5. Bitcoin: financial freedom, not speculation

Bitcoin can be useful to activists when regimes weaponize banking systems, block transfers, freeze accounts, or punish organizations for receiving support. For WLC, Bitcoin should be taught as a practical freedom tool for small, accountable, high-risk contexts, not as an investment scheme.

- Use small amounts for training, emergency support, or micro-stipends where appropriate.
- Keep simple records: amount in BTC, USD equivalent at time of transfer, date, purpose category, and approval record.
- Separate recipient confidentiality from donor accountability: protect people, but keep auditable records.
- Teach wallet basics slowly: receiving, sending, backup, loss risk, and scams.
- Do not pressure activists to use Bitcoin if local risk, legal status, or technical capacity makes it unsafe.
- Do not store large sums on phones used for high-risk activism.
- Make clear that Bitcoin price volatility can reduce value; plan accordingly.

6. Bitchat: local messaging when the internet is down

Bitchat is a decentralized peer-to-peer messaging app that can operate over Bluetooth mesh networks without internet, phone numbers, accounts, or central servers. It may be useful in blackouts, events, protests, disasters, or settings where normal connectivity is unreliable. It should be tested calmly before any crisis.

- Use it for local, low-sensitivity communication first.
- Test it in training settings before relying on it.
- Remember that Bluetooth range is limited and depends on nearby devices.
- Do not assume any app is perfectly secure.
- Avoid sharing names, locations, or sensitive plans unless the risk is understood.
- Have backup channels. One tool should never be the whole plan.

7. Artificial Intelligence: a force multiplier with strict safety rules

AI can help WLC members translate, summarize, draft, analyze, prepare training materials, compare cases, brainstorm tactics, structure reports, and develop scenarios. It can save time and improve clarity. But it can also create security risks if activists enter sensitive names, operational plans, private testimony, or unverified allegations into unsafe systems.

Good AI uses	Risky AI uses	Safer practice
Draft a public statement	Upload confidential witness testimony	Use anonymized summaries and remove identifying details.
Translate a training handout	Paste a member list or internal chat	Translate sanitized text only.
Create a 90-day campaign outline	Ask for covert operational instructions	Ask for legal, ethical, nonviolent, safety-focused planning.
Summarize public reports	Use AI as the only source of factual verification	Verify with trusted human sources and documents.
Generate role-play exercises	Share real names of at-risk activists	Use fictionalized scenarios.

8. The WLC freedom technology decision tree

Use this simple decision tree before adopting a tool.

- If the tool is for public messaging, ask: will it resist censorship and help people verify authenticity?
- If the tool is for private coordination, ask: who can see metadata, contacts, locations, and backups?
- If the tool is for money, ask: what are the legal, volatility, security, and recordkeeping risks?

- If the tool is for evidence, ask: does it preserve chain of custody and protect victims?
- If the tool is for AI analysis, ask: have all names, locations, and sensitive details been removed?
- If the tool is too hard for members to use safely, do not deploy it widely yet.

9. Recommended WLC technology roles

Task	Why it matters	What to do now
Digital safety lead	Helps members with basic security habits and referrals.	Should not become a bottleneck for all decisions.
Bitcoin educator	Trains small groups in safe, accountable Bitcoin basics.	Must emphasize safety, records, and legal context.
Nostr coordinator	Supports decentralized publishing, authentic account verification, relay/client testing, and resilient public communication.	Must train members to protect keys and separate public communication from sensitive operations.
AI trainer	Teaches members how to use AI safely for drafting, translation, and learning.	Must enforce redaction and no-sensitive-data rules.
Incident responder	Coordinates response to account compromise, doxxing, or spyware suspicion.	Should know when to refer to Access Now or other experts.

10. The “do not do” list

- Do not assume a tool makes you safe.
- Do not introduce a new tool during a crisis without prior training.
- Do not upload sensitive names, addresses, witness testimony, or internal plans to AI tools.
- Do not centralize all communications, funds, or evidence in one account or one person.
- Do not store wallet seed phrases in screenshots, email, or cloud notes.
- Do not publish public keys, wallet information, or technical details that create targeting risk unless there is a clear reason.
- Do not shame members who cannot use advanced tools. Good security must be teachable.

11. A 30-day implementation plan

Week	Goal	Action
Week 1	Assess	Map current tools, account risks, member skill levels, and top digital threats.
Week 2	Train basics	Run a 90-minute session on passwords, 2FA, phishing, secure channels, and redaction.
Week 3	Pilot tools	Test one tool in a small low-risk group: Nostr publishing, Bitcoin learning stipend, or Bitchat local test.
Week 4	Review and scale carefully	Document lessons, fix mistakes, decide whether to expand, and create a help channel.

Selected practical resources

Use these resources as starting points. Always adapt them to local risk, language, and legal context. Do not upload sensitive case material to any platform unless the security protocol has been approved.

- **Nostr protocol repository:** Technical reference for the decentralized Nostr protocol. Link
- **Nostr information site:** Plain-language introduction to Nostr as an open social protocol. Link
- **Bitcoin.org:** Basic explanation of Bitcoin as open-source peer-to-peer money. Link
- **HRF Bitcoin Development Fund:** Supports Bitcoin and related freedom technologies for human rights defenders. Link
- **Bitchat:** Peer-to-peer Bluetooth mesh messaging app. Link
- **Bitchat GitHub:** Open-source repository and technical information. Link
- **Access Now Digital Security Helpline:** Help for digital emergencies and technical support. Link
- **Security in-a-Box:** Digital security guide for activists and human rights defenders. Link

Final reminder

Remember: Freedom technology is not magic. The right sequence is always: threat model first, then training, then small pilot, then review, then careful scaling.