Bitcoin Policy
UNITED KINGDOM

Privacy Toolkit: Simple Steps to Protect Your Freedom to Speak and Transact Online

Updated April 2026

Why Should I Care?

You might think privacy doesn't matter because you've got "nothing to hide." But privacy isn't about hiding — it's about control. Control over who knows what about you, and what they can do with that knowledge.

Here are three quick stories that might change your mind:

📱 **The face that wasn't his.** In 2026, a UK man was arrested after facial recognition cameras misidentified him as a burglary suspect — 100 miles from the crime. He spent hours in custody. The real suspect looked nothing like him. (The Guardian, Feb 2026)

📧 **The breach you don't know about.** Visit Have I Been Pwned. Type in your email. Chances are your name, password, phone number, and address have already been sold or leaked, and often multiple times. You just weren't told.

🔪 **The data that got people hurt.** When France's tax authority leaked the personal data of cryptocurrency holders, it triggered a wave of violent robberies targeting these people and their families. People were beaten and held at knifepoint, simply because a government database told criminals exactly who had assets worth stealing, and exactly where those people lived. Innocent people had their fingers cut off, were doused in petrol and threatened with being set alight, and in the most awful cases, actually murdered. **The only way to protect personal data is not to surrender it in the first place.**

Every card transaction, every app sign-up, every social media post creates a permanent record. Aggregated over years, this data paints a detailed picture of your health, politics, relationships, habits, and finances — available to insurers, employers, governments, and anyone who can steal or buy it.

Aldous Huxley wrote: *"Without freedom we cannot become fully human, and freedom is therefore supremely important."* Privacy is the foundation of that freedom. Without it, self-censorship creeps in — and a society that self-censors is not and cannot be free.

How Much Should I Care?

Not everyone faces the same risks, and not everyone needs the same tools. A privacy expert put it well: what some of us might consider a small tweak — like switching to a different app — **feels like a real sacrifice to most people.** They're giving up what's familiar and comfortable. That's why the WHY matters more than the WHAT.

But here's the thing: you don't need to do everything. You just need to do *something*. Every step you take is a step further from easy surveillance.

Think of privacy on a spectrum. Have a look at the tables below, see where you sit on that spectrum, and then read on to see the steps you might look to take, depending on your comfort and risk level.

Quick-Start Action Tables

This is the heart of the guide. Find your level, do those things. Each item refers to a detailed section further down if you want step-by-step instructions.

Table 1: How Much Should I Care? (The Spectrum)

Level	You are...	Your goal	Time commitment
🟢 Casual	A normal person who'd rather not be tracked	Reduce the easy data grabs	10 minutes
🟡 Aware	Someone who's seen the breaches and wants to act	Close the obvious gaps	An afternoon
🟠 Serious	A journalist, activist, or principled individual	Significantly reduce your digital footprint	A weekend
🔴 Committed	Someone facing real threats or living on principle	Near-zero trust in third parties	Ongoing practice

Table 2: 🟢 Casual — 10 Minutes That Actually Matter

Area	Action	Why
Passwords	Check Have I Been Pwned. Stop reusing passwords. Enable 2FA everywhere.	This alone stops most account takeovers
Search	Switch your default search engine to DuckDuckGo	Takes 30 seconds. Stops Google profiling your searches
Browser	Install Brave or Opera (built-in VPN)	Blocks trackers and ads automatically
Physical	Cover your laptop camera. Turn off location services and face recognition on your phone. Don't use iCloud.	Costs nothing, removes easy surveillance vectors
Data cleanup	Look into DeleteMe or Incogni	Subscription services that scrub your data from brokers
Shopping	Use cash when you can, especially for sensitive purchases	No digital trail. The oldest privacy tool there is

---

Table 3: 🟡 Aware — An Afternoon Well Spent

Everything from Casual, plus:

Area	Action	Why
Email	Create a Proton Mail account	Swiss jurisdiction, end-to-end encrypted, free plan
Email aliases	Set up SimpleLogin or DuckDuckGo Email Protection	Give every service a different email. When one leaks, you know who sold you out

Area	Action	Why
Passwords	Use Proton Pass or another encrypted password manager	Unique strong passwords for everything, without memorising them
Messaging	Install Signal and move your important conversations there	End-to-end encryption. Disappearing messages. No tracking
VPN	Install Mullvad VPN	Encrypts your internet traffic. Your ISP can't see what you browse
Identity	Stop using your real name/credentials for online accounts unless legally required	Pseudonyms are lawful and significantly reduce your attack surface
Delivery	Use parcel lockers, collection points, or a PO box instead of home delivery.	Keeps your home address out of databases

---

Table 4: 🟠 Serious — A Weekend Project

Everything from Aware, plus:

Area	Action	Why
Phone	Buy a Google Pixel and install GrapheneOS	Privacy-hardened Android. Removes Google's surveillance while keeping app compatibility
SIM	Get a Silent Link eSIM, paid with Bitcoin	No KYC, no name, no email — just data
Browser	Use the Tor Browser for private browsing	Best-in-class anti-tracking. Routes traffic through multiple relays

Area	Action	Why
Social media	Create a Nostr identity	Censorship-resistant social media. No company can ban you or delete your posts
Bitcoin	Use Phoenix for Lightning payments	Fast, cheap, and far more private than card payments
Shopping	Buy gift cards with Bitcoin via Bitrefill	Shop at mainstream retailers without linking your identity
Transport	Don't call taxis to/from your front door — walk to the corner and order them to your external location	Simple habit that keeps your home address out of ride-hailing databases
Physical	Remove your name from your doorbell and letterbox	Reduces casual doxxing risk

---

Table 5: 🔴 Committed — An Ongoing Practice

Everything from Serious, plus:

Area	Action	Why
Computer	Switch to Linux Mint	Removes Microsoft/Apple telemetry. Won't comply with OS-level age-gating
Home server	Run Umbrel or Start9 for self-hosted files, Bitcoin node, Nostr relay	Your data stays on your hardware, in your house
Messaging	Explore Briar and Bitchat	Designed to work even when governments shut down the internet

Area	Action	Why
Bitcoin	Buy/sell via P2P: Vexl, Peach, Bisq, HodlHodl	No KYC. No reporting. No data to leak
Monero	Use Cake Wallet for Monero transactions	Privacy by default — every transaction is shielded
Physical	Look into Reflectacles	Glasses that defeat facial recognition cameras
AI	Run Ollama locally on Umbrel or Start9	Ask questions without training someone else's model on your thoughts

While this guide is up to date as of April 2026, be aware that the privacy landscape is continually changing, especially as governments attempt to gather more and more information on us. Make sure you stay up to date; monitor news for matters such as CARF and the evolving crypto/data reporting requirements. Know what governments are requiring — and plan accordingly.

A Note on Tools and Honesty

There is nothing worse than being motivated to try something new — and having it not work. We've been careful to recommend tools that are largely mature, functional, and genuinely useful today. Where we mention tools that are newer or rougher around the edges — like White Noise, Briar, or Bitchat — we flag them honestly: things to **be aware of and experiment with**, rather than immediate replacements for what you already use.

Our philosophy: **one clear recommendation per category.** Signal for messaging. Proton for email. Mullvad for VPN. Brave for browsing. Start with those. The alternatives are there when you're ready.

Bitcoin Policy
UNITED KINGDOM

Detailed Sections

Everything below expands on the Quick-Start Table with step-by-step instructions, honest assessments, video guides, and further reading.

Before We Get Started

Even without taking a single other step in this guide, you can easily and quickly:

1. **Check Have I Been Pwned** to see if your email has been found in any of the (very many) recent data breaches

2. Make sure you **don't re-use passwords**, change them regularly, and **use Two-Factor Authentication/2FA** on any account that offers it

3. **Cover your laptop camera** when not in use

4. **Don't use** features such as face recognition or iCloud

5. **Turn off location-based services** on your phone

6. **Use a variety of email addresses** for different services, each with a unique password

7. **Use cash** for everyday purchases — the simplest and oldest privacy tool there is

8. **Don't use your real credentials** unless absolutely necessary (banking, government). For everything else, a pseudonym is fine. Do this whenever you join pubic Wifi networks!

You may also want to investigate data deletion and data broker removal services such as DeleteMe or Incogni. These subscription services allow you to request large-scale deletion of your personal data that may have previously been sold, stolen, or both.

---

1. Browsing the Web Privately

Most websites track you through your browser. The fix is simple: switch to tools that collect far less.

Our recommendation: Brave — blocks ads and trackers automatically, right out of the box.

As an easy starting point, download and install Opera browser with its built-in VPN (free, works on phones, tablets and computers).

If you just want a quick win: change your default search engine to DuckDuckGo. It takes 30 seconds, even in Chrome.

For maximum privacy, use the Tor Browser. This is slower, but designed as the best-in-class means to defend against tracking, surveillance, and censorship. Available for desktop and mobile.

Pro tip: Combine any of these with a VPN (see Section 5). Start today by changing your default search engine — all it takes is 30 seconds.

---

2. Email and Organisation

Our recommendation: Proton Mail — Switzerland-based, end-to-end encrypted, generous free plan. With Proton, you get email, calendar, and cloud storage.

Another solid option is Tuta (fully open source), which also offers email, calendar, and storage.

How to switch (takes 2 minutes): 1. Go to proton.me/mail on your new browser 2. Create an account (pseudonym fine, no KYC needed) 3. Forward important emails, then phase out the old account

Beginner video guide: How to Create a Proton Mail Account (Full 2026 Guide)

Also consider:

· DuckDuckGo Email Protection — free @duck.com address that strips trackers and forwards to your personal inbox. You can create multiple unique private addresses for different websites

· SimpleLogin — excellent for burner/alias addresses

· Proton Pass — free password manager with identity protection

Going much further: Run your own small home server with self-sovereign options like Nextcloud on an Umbrel Pro or on any small PC using the Start9 system. This also lets you run Nostr relays (more in

Section 6) to back up your own social media posts and ensure no third party can delete them.

---

3. Your Phone: GrapheneOS + Anonymous SIMs

Your phone is the easiest method for governments and other bad actors to track you in the most invasive way possible. Reducing your attack surface here is one of the simplest but most effective privacy steps.

Bad news for Apple fans: the best privacy-focused options run predominantly on Android, specifically Google Pixel handsets.

GrapheneOS is a free, privacy-hardened version of Android that removes most tracking while still letting you run the apps you need. Good news for 2026: GrapheneOS works brilliantly on Google Pixel phones right now, and a partnership with Motorola was announced earlier this year — so official support for non-Pixel options is coming.

Setup (30-45 minutes): Use the official web installer.

Beginner video guide: GrapheneOS Install Guide (2026) — The Security Gold Standard

Stay anonymous with your SIM:

You can already buy cheap pay-as-you-go SIMs with cash in supermarkets (no ID is usually required for small top-ups).

For completely KYC-free mobile data: Silent Link sells data-only eSIMs (and some with a US number) that you can buy with Bitcoin (onchain or Lightning). No email, no ID, nothing. Plans start at $9 one-off for data (hotspot enabled).

Quick start: 1. Go to Silent Link, choose a plan (e.g. DATA.PLUS or US.PLUS) 2. Pay with Bitcoin/Lightning 3. Scan the QR code on your phone to install the eSIM

It works across most of Europe and the USA — ideal for GrapheneOS users who want zero personal data tied to their connection.

---

4. Private Messaging

Many end-to-end encrypted messaging apps such as WhatsApp do have better levels of privacy than SMS messages or emails, and allege that they are unable to scan your private messages. However, some are more secure than others, and crucially almost all of the commonly used apps will be reliant either on the internet or on the wireless network.

In extreme cases, where governments shut down the internet to prevent citizens communicating, what's the alternative? Mesh networks — running peer to peer between phones, using their Bluetooth connectivity to connect directly to each other. Such mesh networks remain in their infancy, but the more of us use them the greater the network effect.

Our primary recommendation: Signal. Simple, reliable, includes call functionality and disappearing messages. It's the one app you should get everyone you know onto.

⚠️ **An honest note:** Signal themselves DO run their servers, so hacking and government-action risks remain, and Signal do have a record of your username and copies of your data. For most people, Signal is still vastly better than WhatsApp, Telegram, or SMS — but it's important to be aware of the limitations.

Beginner video guide: How to Use Signal App — Beginner Tutorial

For the more adventurous (be aware these tools are still maturing — try them as secondary options, not primary replacements):

· **White Noise** — leverages Nostr for decentralised identity and messaging, combined with Messaging Layer Security (MLS) for end-to-end encrypted group chats and DMs. No phone number or email needed. *Still new — keep an eye on it*

· **Briar** — intentionally designed to withstand attacks by authoritarian states. Free, open-source, peer-to-peer via Bluetooth, Wi-Fi, or Tor. Bypasses central servers to prevent surveillance and works offline. Android only. *Excellent for what it does, but requires others on the network*

· **Bitchat** — decentralised, open-source messaging created by Jack Dorsey in 2025. Works entirely without internet, cellular service, or servers. Uses Bluetooth Low Energy (BLE) for a local mesh network within 30-100 metres. Already seeing huge usage spikes in Uganda, Nepal, and Iran during government internet shutdowns. Recently banned from the Chinese app store — which is a stamp of approval in our book. *Think of it as emergency infrastructure*

Beginner video guides:

· White Noise — Private Messaging

· How to Use Briar App (2026 Guide)

· How to Use Bitchat — FULL TUTORIAL (Works 2026)

⚠️ **Honest assessment:** Like Nostr clients (more below), these alternative apps are improving rapidly but can still feel rough around the edges. The more people use them, the better they will get and the more the network effect will strengthen, but these should still be thought of as experimental at the time of writing.

---

5. VPNs and Protecting Your Internet Connection

If you are reading this from the UK or Australia, you probably already know about and use a VPN to circumvent the annoying but thankfully still ineffective attempts by those governments to age-gate the internet (thus collecting vast amounts of personal data which will assuredly soon be leaked). A VPN encrypts everything your device sends and hides your real location. It's advisable to use one everywhere — on your home Wi-Fi, especially on public networks, and on your phone.

Our top recommendation: Mullvad. No accounts, no logs of user data, and you can pay with Bitcoin or cash. You can pay completely anonymously and it just works. Famously, law enforcement once had to leave a raid of their offices empty-handed after it became clear there was no user data to confiscate. Install the app on your phone or computer, turn it on, and you're protected.

Opera's built-in VPN is a good free backup, especially if you're already using the Opera browser, but Mullvad is stronger for serious privacy.

Other good choices:

· Proton VPN — especially if you're already using Proton Mail. Has a free tier

· Orbot — open source and powered by Tor, but may need a higher level of technical ability to install and run

Beginner video guide: How to Download & Install Mullvad VPN

---

6. Uncensorable Social Media (Nostr)

If you live in the UK, you may currently be rather nervous about posting on social media, or apprehensive that the government may try to restrict certain things being said in public. If so, you should investigate Nostr.

With Nostr, you own your identity and can easily transfer between clients without losing your friend list, posts, or social graph. Your account is created and controlled not by an email and password, but by a private and public key pair — conceptually similar to a Bitcoin key pair for those familiar with that technology.

As the inimitable Alex Gladstein puts it: *"Nostr is a community-run digital network highly resistant to censorship and corruption. It has 40,000 weekly active users and a growing ecosystem of clients and applications ranging from social media to long-form publishing to payments."* His recent piece in Reason is highly recommended.

Getting started:

· **iOS:** Damus or Primal

· **Android:** Amethyst or Primal

· **Desktop:** Iris (web-based)

⚠️ **Honest assessment:** Nostr clients are improving rapidly but can still feel rough compared to Twitter or Instagram. Think of it as building the alternative — the more people join, the better it gets. The key point: your posts here can't be deleted by any company or government.

Beginner video guide: Create Your Nostr Account

---

7. Buying and Selling Privately with Bitcoin

(i) Buying and selling Bitcoin without surrendering your identity

The safest way to buy and sell Bitcoin in terms of your personal data is via P2P platforms, none of which require KYC (Know Your Customer identity checks). Centralised exchanges typically report purchases, sales, and holdings to domestic and — with the arrival of the Cryptoasset Reporting Framework (CARF) — to other tax authorities worldwide.

Recent data leaks by the tax authority in France have led to a spate of violent crimes and robberies, many involving grievous bodily harm, targeting cryptocurrency holders whose details were leaked. **The only way to protect personal data — and in this case, yourself — is not to surrender that data at all.**

Buy and sell Bitcoin privately using these established and reputable services:

- **Vexl** — peer-to-peer, in-person trades
- **Peach** — mobile P2P trading
- **HodlHodl** — non-custodial P2P marketplace
- **Bisq** — decentralised desktop exchange

For Bitcoin purchases, ideally use a self-custody Lightning wallet. Recommended: Aqua Wallet and Phoenix Wallet. Also notable: Cake Wallet are doing interesting things with Bitcoin Silent Payments.

Beginner video guides:

- Buy Bitcoin Without ID (Vexl)
- Peach Bitcoin: Buy BTC Without KYC via P2P
- HodlHodl: How to Buy Bitcoin Without ID
- How to Use Bisq (Full Tutorial)

(ii) Spending Bitcoin on real goods anonymously

Using Bitrefill, you can buy gift cards (Amazon, supermarkets, Uber, etc.), phone top-ups, and eSIMs instantly with Bitcoin. No KYC required for most purchases. You can even purchase a prepaid virtual Visa card, enabling you to pay anywhere Visa is accepted.

Beginner video guide: How to Buy Anything with Bitcoin | Bitrefill Tutorial

Other similar no-KYC services:

· **SpendCrypto** — often prices at face value with tight rates

· **CryptoRefills** — wide brand coverage, good for international use

· **CoinsBee** — excellent if you hold altcoins

All of the above let you turn Bitcoin or crypto into vouchers or top-ups without handing over ID.

---

8. Your Computer: Privacy-Focused Operating Systems

We're now moving further up the difficulty ladder, though even this step will not be overly challenging for those who have set up a computer from scratch. With increasingly common rumours that various governments may be considering the implementation of **operating-system-level age verification** — essentially meaning no one will be able to use an age-gated computer without surrendering their ID — you may want to consider software that is unlikely to comply (as it is free and open source).

Our recommendation: Linux Mint — free, familiar Windows-like interface, no built-in age-gating or tracking.

Beginner video guide: How to Install Linux Mint on ANY PC or Laptop (2026 Complete Guide)

For more options: The Most Secure Linux Distributions for Privacy & Security (2025).

Self-hosted AI: If you want to run AI large language models locally and privately, both Umbrel and Start9 will let you run Ollama simply (though be aware you'll need higher levels of RAM and CPU power than many mini computers offer). Your questions never leave your home.

Beginner video guide for Ollama: Running LLMs Locally Just Got Way Better — Ollama + MCP

---

9. Blocking Facial Recognition (Physical Privacy in Public)

Facial recognition cameras are increasingly used across the UK and the world. They have already been linked to cases of mistaken identity and wrongful arrest — and none of us have consented to being photographed, with our personal data stored and used, in this way.

Is it possible to block them? It's still an open question, but products like Reflectacles are coming to market. These claim to defeat facial recognition cameras with infrared-blocking lenses and reflective frames. No apps or batteries needed — wear them like normal glasses for instant analogue protection.

More here: Can Reflectacles Glasses Defeat Facial Recognition?

Final Thoughts

This is not a guide intended to help you become a ghost, or to have any chance of really scrubbing yourself from the internet. But it's a list of some simple steps that anyone can take — even if you're not technically minded — to protect your data, to make yourself a little less obvious, and to be a little less apparent to a surveillance state than your neighbour.

Remember: **privacy isn't about hiding wrongdoing. Privacy is a human right** — the ability to selectively reveal oneself to the world. It is about keeping control of your own life in whatever way you choose. The fact that governments around the world are desperate to undermine our privacy is their failure, not ours.

Eric Hughes wrote in the Cypherpunk Manifesto:

"We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence… We must defend our own privacy if we expect to have any. We must come together and create systems which allow anonymous transactions to take place… We know that someone has to write software to defend privacy, and since we can't get privacy unless we all do, we're going to write it."

You've got this. One small step at a time, we keep the ability to speak and transact freely. And only when we are truly free are we truly human. Here's to a future of free humans, despite all the efforts of governments to overcome us.

Start with one change this week. Official websites as listed in this guide are always best — bookmark them and stay safe.
