

# Privacy Best Practices

## Position Privacy

By default, Meshtastic nodes broadcast GPS coordinates to the entire channel at regular intervals. Your approximate location is visible to all channel participants. If your node is on the Default public channel *and* your node (or a node that hears it) uplinks to the public Meshtastic MQTT server with map reporting / "OK to MQTT" enabled, your position also appears on aggregation sites such as [meshmap.net](https://meshmap.net). Being on the Default channel alone, with no MQTT path, does not publish you to those maps.

## Mitigations

- **Use a private channel:** Position broadcasts on a private channel are only visible to nodes with the key - *but only if* no gateway on that channel uplinks to MQTT. By default the MQTT uplink sends packets to the broker **unencrypted** (unless `mqtt.encryption_enabled` is set true), which publishes positions to the internet. The protection also fails if the node is simultaneously broadcasting position on a public channel. A private PSK alone does not stop MQTT exposure.
- **Disable the position module:** Navigate to *Config → Position → GPS Mode → DISABLED*. The node will not broadcast any location data.
- **Set a fixed imprecise location:** Instead of live GPS, configure a fixed position - use the center of your neighborhood or a nearby landmark rather than your exact address. This allows you to appear on mesh maps without revealing your precise location.
- **Reduce position precision:** Meshtastic lets you broadcast a coarsened position. Position precision is configured **per channel** (in the app: Channel settings → Position precision), so it must be set on the channel you broadcast on, then verified. This reduces - but does not eliminate - location disclosure; an approximate fix (e.g. nearest kilometer) can still identify a small town or a single rural site. Note: position is **not** used for mesh routing (Meshtastic uses managed-flood routing, not GPS-based routing), so coarsening or disabling it does not affect message delivery.

## Node Naming

Your node's long name is broadcast to everyone on the channel and appears on public mesh maps. Use a callsign, handle, or alias rather than your full real name if privacy is a concern. Your node's short name (4 characters) is used in the mesh and is also public.

# Telemetry Data

If you enable device telemetry or environmental sensors, data such as battery voltage, temperature, humidity, and pressure are broadcast on the channel. This data can reveal:

- Whether your device is plugged in or on battery (usage patterns)
- Environmental conditions at your location (indirectly revealing location details)
- When the device is active or idle

Disable telemetry modules you do not need, especially on nodes deployed in sensitive locations.

# Public Mesh Visibility

If your node is on the Default channel *and* is bridged to the public Meshtastic MQTT server (map reporting / "OK to MQTT" enabled), sites like [meshmap.net](https://meshmap.net) aggregate and display:

- Node long name and short name
- GPS position
- Last-heard timestamp (this is derived by the map, not part of the report payload)
- Hardware model
- Firmware version

This information is public and indexed. Consider the public mesh as a zero-privacy environment.

# Sensitive Use Cases

For deployments where participant safety depends on privacy (e.g., domestic violence shelters, witness protection situations, activist networks operating in hostile environments), apply all of the following:

- Use a private channel with a strong random PSK generated by the app.
- Disable GPS entirely (Config → Position → GPS Mode → DISABLED).
- Use an alias or callsign as the node name - never a real name.
- Consider **Meshtastic** instead of Meshtastic (see below): its routing may expose less network-wide identity data, because it follows discovered paths rather than flooding the

whole network. Evaluate this carefully against current MeshCore documentation - neither platform provides anonymity.

- Disable all telemetry modules.

# Meshtastic vs. MeshCore Privacy Profile

The two platforms have meaningfully different privacy characteristics as a consequence of their routing architectures:

## Meshtastic (Flood Routing)

Meshtastic uses a managed-flood routing model. NodeInfo packets - advertising each node's ID, name, and position - are flooded outward up to the hop limit (default 3 hops), reaching nodes within that hop-limited radius rather than literally the entire mesh. Within the reachable area, nodes typically learn about all other nodes they can reach. This is high-transparency by design and enables features like mesh maps, but it means even passive observers within range on the channel receive location and identity data for nearby nodes.

## MeshCore (Path-Based Routing)

MeshCore uses a path-based (source-routed) architecture in which messages follow discovered paths rather than flooding the entire network. According to MeshCore's own description, nodes primarily exchange routing information along discovered paths rather than broadcasting advertisements to the whole mesh; confirm the exact default advertisement behavior against current MeshCore documentation before relying on it for a sensitive deployment. In dense networks this can mean a node's existence and location may not be known to distant nodes that have no route to it, which can be more privacy-preserving where blanket network-wide NodeInfo broadcasting is undesirable.

Neither platform should be considered a complete anonymity solution - LoRa transmissions are detectable and direction-findable by anyone with appropriate radio hardware, regardless of the software layer's privacy features. For genuine life-safety deployments, seek professional operational-security guidance rather than relying on radio-software settings alone.

---

Revision #3

Created 2026-05-03 04:15:59 UTC by Mesh America Admin

Updated 2026-06-09 12:08:46 UTC by Mesh America Admin