



User Profile Plan

Which app lives where · belongs with Chapters 14 and 15 · Device: _____ · Date: _____

Three tools, three degrees of separation. The work profile (Shelter) is a room in the house: separated, but within the same user account. The Private space is a hidden room: its own keys, and once locked it is invisible. The user profile is a separate house: fully separated, but every switch costs time and a PIN. Rule of thumb for Google: as few instances of Sandboxed Google Play as possible, ideally one, with all Google-dependent apps bundled there. If you need no such app, do not install it at all.

1 · THE THREE LAYERS COMPARED

Criterion	Work profile (Shelter)	Private space	User profile
Separation	Real, but not complete. Own container within the same user account, Auto-freeze per app.	Nested profile within the main profile with its own encryption keys. Locking stops all apps inside immediately.	Complete. Own keys, own app list, no shared clipboard.
Notifications	Without switching profiles.	Directly in the main profile while unlocked.	Only via forwarding, without content, no replying.
Visible when locked	Apps remain visible, identifiable by the work profile icon.	Apps disappear from the app drawer, the main profile looks normal.	Other profiles cannot see the app list.
Own VPN path	Yes, own VPN configuration. A VPN installed there applies only to the work apps.	Yes, own VPN configuration: a different VPN, no VPN, or the same provider with its own tunnel.	Yes, own VPN configuration per profile.
Best for	Freezing individual apps on demand, dual accounts, risk apps.	Simple isolation, second app instance, Google on demand (Android Auto, for example), separate network path.	Financial apps, separate identities, maximum separation.

2 · MY PLAN

Profile / area	Purpose	Apps (keywords)	Sandboxed Google Play	VPN (provider / none / Tor)	Notifications (direct / forwarded / none)	After use: End session
Main profile						not applicable, always active
Private space						instead: lock it

Rows 3 to 7 are meant for user profiles. Enter only profile names and purposes, no PINs, no account names. At the end, check the Sandboxed Google Play column: more than one “yes” is a reason to rethink the plan.

3 · FOUR TEMPLATES FROM THE BOOK (CHAPTER 15)

Setup	Main profile	Private space	User profiles
Beginner	Open-source apps and the base system. Sandboxed Google Play here if you need Google-dependent apps.	Everything you want to separate from the open-source apps: social media, WhatsApp, banking app (with Sandboxed Google Play).	None.
Pragmatist	Only apps from open-source sources, no Sandboxed Google Play.	Sandboxed Google Play plus everything that depends on it: banking, broker, WhatsApp, Maps. Own VPN path.	None.
Advanced	Open-source apps only, no Google. Notifications direct.	Sandboxed Google Play for push apps: home camera, car app, smart home. Notifications while unlocked.	Banking and broker with Sandboxed Google Play. Notifications via forwarding, switch with PIN to check.
Naked Owner	Owner profile: system maintenance and updates only. No accounts, no data, no third-party apps.	Not used.	Daily (communication, open source, no Google), Google (only when needed, then End session), Banking (financial apps only, own VPN path, End session after each use).

⚠ **Forwarded notifications are deliberately content-free.** You only see that something is waiting in another profile. No replying, no accepting calls: an app through which you expect calls belongs in the main profile or the Private space. ⚠ **“End session” means silence.** The profile is then encrypted and dormant, no app is running, no notification comes through until you unlock it again. ⚠ **Private DNS applies to all profiles, VPN to only one.** The DNS setting is system-wide, whereas every profile needs its own VPN configuration (Chapter 20).