

Companion sheets

FREE WITH THE GUIDE

Five one-page sheets to go with **Take Back Your Phone**. Nothing here is **extra content** — four of these are chapters of the book reformatted onto a single side of A4, because you cannot hold a book open at the right page with one hand on a phone and the other on a laptop.

PRINT THESE TWO		THESE ARE OPTIONAL	
Install day — beside the laptop	Sheet 2	Which profile are you?	Sheet 1
Before you wipe — tick with a pen	Sheet 3	Recovery cards — cut-outs for 22.5	Sheet 4
		What it costs	Sheet 5

IF YOU CANNOT PRINT, YOU HAVE LOST NOTHING

Every sheet here exists in the book. Sheet 4 is the only one worth having on paper regardless — those cards are meant to be cut out and outlive the device, and the content behind them is Chapter 22.5 to 22.7.

Which profile are you?

SHEET 1 OF 5

Work down the page and **stop at your first yes**. That is your profile. If more than one applies, take the lowest-numbered — it already assumes the others.

1	Is there a specific person who might get their hands on your phone and wants in? An abusive or controlling partner, a stalker, a hostile relative, a contentious divorce.	Profile C TIER 1 + PARTS OF 3 Read 7.2, 10, 21.1
2	Could a state, or a well-funded organisation, want your data specifically? Journalist, activist, human-rights researcher, security researcher, a source handler.	Profile D TIERS 1, 2 AND 3 Read 21.4, 21.5, 21.6
3	Do you hold other people's confidential information as part of your job? Lawyer, doctor, therapist, accountant, HR. You owe a duty to someone else.	Profile B TIER 1, THEN TIER 2 Read 17.2, 20.2, 22
4	Do you regularly cross borders carrying this phone? Especially through jurisdictions with aggressive device-search powers.	Profile E TIER 1 + TIER 2 Read 10, 20.7, 21.6
5	None of the above — you simply want out of the surveillance pipeline. This is most readers, and it is a completely respectable place to be.	Profile A TIER 1, COMPLETE Read 12, 15, 22

BEFORE YOU SPEND A PENNY

Check that your bank, your work MFA app and any medical-device app work on GrapheneOS — search discuss.grapheneos.org for each by name. That is chapter 6.2, it costs nothing, and it is the one check that decides whether you should do this at all.

Keep this beside you. Do not press buttons on the phone unless a step tells you to. Full detail is chapter 8; troubleshooting is chapter 9.

A Update the stock OS

Settings > System > Software updates. Repeat until it says up to date — there may be two or three in a row.

☐ Phone reports it is up to date

B Enable OEM unlocking

Settings > About phone, tap Build number seven times. Then Settings > System > Developer options > OEM unlocking, on.

☐ Toggle is ON and not greyed out — if greyed out, stop: carrier-locked

C Prepare the computer

Chrome, Chromium, Edge or Brave. Not Incognito. 32 GB free. Type the address by hand: grapheneos.org/install/web

☐ Official installer open, address typed by you

D Boot into fastboot

Power off fully. Hold volume-down, then press and hold power. Keep holding volume-down until the text screen appears.

☐ Screen reads Fastboot Mode — and you have not pressed power again

E Unlock, download, flash

Connect direct to the computer. Unlock bootloader, confirming on the phone with volume + power. Download release. Flash release. Do not touch the phone while it flashes.

☐ Flashing reported complete

F Lock the bootloader

The most important step in the guide. Lock bootloader, confirm on the phone. The phone wipes a second time — this is correct.

☐ Device state: locked

G First boot and verify

Press power on Start. Set a strong lock — eight digits minimum. Leave the OEM unlocking checkbox ticked on the final setup screen.

☐ Boot hash matches Appendix E for your exact model

THE TWO THAT CATCH PEOPLE

At fastboot: the top menu item says *Start*. Pressing power selects it and boots the phone straight out of fastboot. Leave the phone alone.

Order is unlock, flash, lock. Locking before flashing leaves a stock-signed lock over non-stock images and the phone will not boot.

Before you wipe

SHEET 3 OF 5

Chapter 7 on one page. Everything here happens on your **current** phone. Do not start the install until every box is ticked.

GET YOUR DATA OUT

- ☐ DCIM and Pictures folders copied to a computer
- ☐ Google Takeout requested AND downloaded — links expire
- ☐ Contacts exported as .vcf
- ☐ Calendar exported as .ics
- ☐ Signal backup on, 30-digit passphrase on paper
- ☐ WhatsApp folder copied off the phone
- ☐ Wi-Fi passwords recorded for networks you rarely visit
- ☐ Notes, fitness and journal apps individually exported
- ☐ IMEI, phone number and APN settings written down
- ☐ A second copy exists somewhere else
- ☐ You opened a photo from five years ago and it displayed

KEEP YOUR ACCOUNTS

- ☐ Every 2FA account listed on paper
- ☐ Recovery codes downloaded for email, bank, work, registrar
- ☐ Recovery codes PRINTED and in a drawer
- ☐ Authenticator moved to Aegis or Ente Auth
- ☐ A real login tested with a code from the new app
- ☐ Encrypted authenticator export saved in two places
- ☐ Passkeys moved out of the device keystore
- ☐ Password manager master password known from memory
- ☐ Emergency kit printed
- ☐ Chrome passwords exported, imported, CSV deleted
- ☐ SMS-2FA accounts switched to app-based where possible

THE LOCKOUT DRILL — SAY THESE OUT LOUD

Reading them silently lets you hand-wave. Saying them does not.

- ☐ If my phone vanished right now, how would I log into my primary email?
- ☐ How would I log into my bank?
- ☐ How would I get into my password manager?
- ☐ Where, physically, are my printed recovery codes?

STOP

If you cannot log into your email, your bank and your password manager **without this phone**, nothing else on this sheet matters. Go back to chapter 7.2 and fix that first.

NEVER WRITE A SECRET ON THESE

They record **where things are**, not what they say. Keep them with your recovery codes, in a safe or a locked drawer — not in your wallet. Cut along the dashed lines.

WHERE MY KEYS ARE

Locations only. Update whenever one of them moves.

Printed 2FA recovery codes

Seedvault 12-word key

Aegis / Ente encrypted export

Signal 30-digit passphrase

Password manager emergency kit

Off-site backup drive

THIS PHONE

Fill in on install day. Useful for a police report and for proving the install is still genuine.

Model and codename

IMEI

Installed (date)

Build number at install

First 8 characters of boot hash

Support ends

IF IT IS LOST OR STOLEN

- Assume the keys were in memory unless it was powered off or had rebooted.
- Change your primary email password **first** — everything else recovers through it.
- Then the password manager, then the bank, then anything holding money.
- Revoke the device at each service — sessions, connected devices, active logins.
- Report the IMEI to your carrier to blacklist the handset.
- Re-issue the eSIM or move the physical SIM.
- There is no remote wipe. Your protection was the lock secret and the encryption, and they are already doing their job.

IF I AM NOT ABLE TO

For whoever handles my affairs. Leave with your will or a trusted person.

Who to contact

Where the password manager kit is

Where the printed codes are

- The phone is encrypted. Without the lock secret its contents cannot be recovered by anyone, including the manufacturer.
- Photos and documents are backed up separately — see the “Where my keys are” card.
- Do not attempt PIN guesses. The device throttles and may be set to erase.

What it costs

SHEET 5 OF 5

In money and in hours, before you commit. **The operating system is free and always will be** — everything below is hardware and the services replacing the ones you are leaving. Prices approximate.

ONE-OFF

GrapheneOS itself	Free
Pixel 10a or 9a, new	£400–500
Pixel 8a, discounted or used	£200–300
A cable that carries data	£10
External drive for backups	£50–80
Two hardware keys (B, D, E)	£80–100

EVERY YEAR

Your own domain name	£12
Mail — Posteo, cheapest credible	£12
Mail suite — Proton Unlimited	£80–110
Photos — Ente	£35–90
VPN — Mullvad, flat rate	£50
Password manager — Bitwarden	Free–£10
Typical realistic total	£60–150

THE NEARLY-FREE PATH

If budget is the constraint: **Posteo** mail at about £12 a year, **Syncthing** for photos and files, **Bitwarden** free, **Aegis** free, **Organic Maps** free, no VPN. A complete migration for roughly the price of one takeaway — and not a worse configuration, only a less convenient one.

YOUR HOURS

40 minutes	Read Part One and write your threat model
1 hour	Check your critical apps — before spending anything
3–5 hours	Back up, sort out 2FA, print recovery codes
2 hours	The installation itself, most of it waiting
2–3 hours	First-hour setup and your essential apps
1 hour × 6 weeks	Service migration, one per week
An afternoon	Tier 2 hardening, optional
15 min / month	Ongoing maintenance, forever