

COMPREHENSIVE

ANDROID PRIVACY GUIDE

Practical settings for stronger device,
account and communications security.

01	LOW IMPACT Secure the device and accounts.	03-04
02	MEDIUM IMPACT Reduce tracking, access and exposure.	05-08
03	HIGH IMPACT Apply stronger, risk-based controls.	09

Protection without guesswork

Choose settings that match how you use the phone and the risks you face.

This guide follows the same low-, medium- and high-impact approach as the Red.One iPhone guide. Start with the foundations, then add restrictions deliberately. More restriction is not automatically the right choice for every user.

01 Low impact

Pages 03-04

A sound starting point for nearly everyone. Keep updates, screen locks, account recovery and app security working.

02 Medium impact

Pages 05-08

Reduce account history, permissions, personalization and network exposure. Some conveniences will change.

03 High impact

Page 09

Consider stronger device protections and separation for higher-risk use. Test important functions before relying on them.

Before you change anything

Menu paths are examples. Pixel, Samsung, other Android devices and GrapheneOS differ. Use Settings search when a path does not match; do not force a setting your device does not offer.

Google-account sections apply where Google services are used. On Red.One-provisioned or employer-managed devices, retain the supplied security tools and ask before changing VPN, DNS or management controls.

This is a manual guide, not an automatically applied configuration. Verify calls, essential alerts, navigation, recovery and VPN operation after making changes.

Documentation: references 1-4, 21, 23, 33-35 on pages 11-12.

Secure the device first

Start with protections that preserve normal everyday use.

01 Keep Android and apps current

1. Open Settings > System > Software updates, or search Settings for "Software update." Install available updates and restart when prompted.
2. Check both the Android security update and Google Play system update, where present. The dates are normally under About phone > Android version.
3. In Play Store > profile > Settings > Network preferences > Auto-update apps, enable automatic updates. Also check profile > Manage apps & device for pending updates.

Use a device that still receives manufacturer security updates. A current app does not compensate for an unsupported operating system.

02 Strengthen the screen lock

1. Search Settings for "Screen lock." Use a unique PIN of at least six digits; choose a longer PIN or password for greater protection. Avoid dates and repeated digits.
2. Set a short screen timeout and require locking immediately after sleep, where available. Review any Extend Unlock or trusted-place exceptions.
3. Search for "Lock screen notifications" and hide sensitive content. For highly sensitive apps, hide their lock-screen notifications entirely.

Biometrics are convenient, but the underlying PIN or password still matters. Do not share it.

03 Prepare for loss or theft

1. Open Settings > Google > All services > Theft protection. Enable supported options such as Theft Detection Lock, Offline Device Lock and Remote Lock.
2. Review Identity Check if offered. It can require biometric authentication for sensitive changes outside trusted places.
3. Search Settings for "Find Hub." Enable it if device recovery is part of your plan, and review offline finding. Test account access elsewhere; store recovery codes separately.

Lost-device recovery involves location and account services. Do not disable them casually without choosing an alternative recovery plan.

Documentation: references 5-8, 39 on pages 11-12.

Protect accounts and apps

Reduce avoidable risk without disabling useful security controls.

04 Secure every Google account

1. Open Settings > Google > Manage your Google Account > Security & sign-in. Use a unique password and add a passkey or strong two-step verification.
2. Review recovery, signed-in devices and third-party access. Remove unfamiliar or unused access.
3. Repeat for every Google account on the device. Save recovery information in a secure place that does not depend only on this phone.

Keep personal and work accounts separate where practical. Ask your administrator before changing an employer-managed account or device.

05 Install fewer apps; retain Play Protect

1. Use trusted app sources and verify the developer. Read the permissions and Data safety information, but do not treat a store listing as a guarantee.
2. On devices with Google Play, open Play Store > profile > Play Protect > Settings. Keep "Scan apps with Play Protect" on.
3. Uninstall apps you no longer need. Avoid unknown APK links; if an approved installation requires "Install unknown apps," revoke that permission afterward.

"Improve harmful app detection" may send unknown apps to Google for analysis. This is a separate privacy-versus-detection choice.

06 Review powerful access and app locks

1. Search Settings for "Accessibility," "Device admin apps" and "Special app access." Check notification access, display-over-other-apps and unknown-app installation privileges.
2. Keep only access needed by trusted apps. Confirm with Red.One or your IT team before removing privileges used by provisioned security tools.
3. Enable an app's own lock where offered. If Red.One supplied Sophos App Protection, retain its additional authentication and follow your device-specific instructions.

App-lock features differ across devices and Sophos editions. An app lock supplements the screen lock; it does not make the app anonymous.

Documentation: references 2, 9-11, 36 on pages 11-12.

Reduce your Google data trail

Account controls are separate. Turning off one setting does not turn off all collection.

07 Limit saved activity and recommendations

1. Open your Google Account > Data & privacy. Review Web & App Activity and YouTube History. Turn off storage you do not need, or choose a short available auto-delete period.
2. If shown, review Search Services History and Personalized Recommendations separately. Google is rolling out these controls; older accounts may still use Web & App Activity.
3. Delete existing history separately when appropriate. Repeat for each account, and review optional audio or media saving where offered.

Turning history off is not the same as deleting it. These controls do not stop all service, security or transaction records.

08 Review Maps Timeline and old locations

1. In Google Maps, open profile > Your Timeline. Use its settings or Location & privacy settings to review whether Timeline is on, and turn it off if unnecessary.
2. Review and delete unwanted past Timeline data separately. Check every device where you use Maps and any Timeline backup shown under the cloud icon.
3. Review Google Maps Location sharing independently, and end access that is no longer needed.

Timeline, live location sharing and app location permission are different controls. Turning off Timeline does not hide your location from a mobile carrier.

09 Reduce advertising and Play personalization

1. Search Settings for "Ads." Review Ads privacy and turn off Ad topics, App-suggested ads and Ad measurement if shown. Delete the advertising ID where offered.
2. In your Google Account, open My Ad Center and turn off personalized ads if you do not need them.
3. In Play Store > profile > Personalization in Play, review personalization and Play History separately. Turn off unwanted history and delete existing entries as appropriate.

You will still see ads. These choices reduce specific forms of personalization; they do not erase purchases, downloads or every tracking identifier.

Documentation: references 1, 3, 12-16 on pages 11-12.

Control what apps can access

Give each app only the data and sensors needed for its purpose.

10 Audit permissions, app by app

1. Open Settings > Security & privacy > Privacy > Permission manager, or search "Permission manager." Review location, microphone, camera, contacts, photos and nearby devices.
2. For location, microphone and camera, prefer "While using" or "Ask every time" where available. Use approximate location unless precision is required.
3. Choose selected-photo access where supported. Review Privacy dashboard for unexpected use, and leave unused-app permission removal enabled where offered.

Permission choices vary. Contacts and other categories may only offer Allow or Don't allow. Test navigation, calling and essential alerts after changes.

11 Limit scanning and optional diagnostics

1. Under Location > Location services, review Wi-Fi scanning and Bluetooth scanning. Turn off scans you do not need; this can reduce location accuracy.
2. Search Settings for "Usage & diagnostics" and disable optional reporting if preferred. Review separate manufacturer analytics or personalization settings too.
3. End unneeded location sharing in apps. Preserve emergency functions and lost-device recovery.

Disabling diagnostics does not stop individual apps from collecting data. Location settings and a VPN do not prevent carrier-based location tracking.

12 Review Gemini and voice-assistant access

1. In Gemini, open the profile menu and activity controls. Review "Keep Activity," delete unwanted saved chats, and decline optional media-improvement sharing where offered.
2. Open Connected Apps and disconnect services Gemini does not need. Turning off Keep Activity does not, by itself, disable all connected apps.
3. Review "Hey Google," lock-screen access and personal results in the assistant settings available on your phone. Disable functions you do not use.

With Keep Activity off, Google may still retain chats for up to 72 hours to provide the service. Do not submit confidential information without authorization.

Documentation: references 1, 11, 17-19, 40 on pages 11-12.

Protect network traffic

Use the Red.One configuration supplied for your device, then verify it works.

13 Use Red.One VPN consistently

1. For initial VPN setup, install and open the official WireGuard app. Tap + and import the supplied Red.One .conf file or scan its QR code. Activate the tunnel.
2. Open Settings > Network & internet > VPN, or search "VPN." Open WireGuard's settings and enable Always-on VPN and Block connections without VPN where supported.
3. Test both Wi-Fi and cellular data. Confirm a recent handshake or moving traffic counters and the expected VPN public IP. Keep the configuration private and device-specific.

Blocking without VPN can prevent internet access until the tunnel connects. Resolve failures with support rather than leaving protection disabled.

14 Keep DNS and VPN settings coordinated

1. Search Settings for "Private DNS." Keep the Red.One configuration; do not substitute providers.
2. A custom Private DNS service can override the VPN's DNS choice and bypass its intended filtering. Confirm the combination with Red.One, especially on GrapheneOS.
3. Do not enable competing VPN, firewall or DNS apps that use Android's VPN slot. Normally only one VPN can be active in a given profile.

DNS protection is not a VPN. A VPN protects traffic to its gateway; it does not remove malware or conceal who you are when you sign into an account.

15 Check Wi-Fi, sharing and VPN coverage

1. Forget unneeded Wi-Fi networks, disable unwanted auto-connect, and retain randomized MAC addressing where supported. Keep Quick Share visibility limited.
2. Do not assume a phone's VPN protects devices using its hotspot. Use a VPN on those devices or a properly configured VPN travel router.
3. Do not assume Private Space or other profiles share the main profile's VPN. Configure and test each required profile separately.

A hotel sign-in page may require a temporary connection exception. Complete only that sign-in, then restore and verify VPN protection before other activity.

Documentation: references 20-25, 34, 38 on pages 11-12.

Protect browsing and content

Reduce unnecessary exposure while keeping recovery and essential communications usable.

16 Review browser privacy and safety

1. In Chrome > Settings, run Safety check and keep Safe Browsing enabled. Review Privacy and security, including "Always use secure connections" where offered.
2. Under Site settings, review camera, microphone, location and notifications. Block third-party cookies if compatible with your sites; use narrow exceptions when needed.
3. Review browser sign-in, sync and saved data. Use an approved browser suited to your privacy needs.

Incognito mainly limits local browsing records after the session closes. Websites, signed-in accounts and network providers may still identify activity.

17 Choose backups and photo sharing deliberately

1. Search Settings for "Backup." Confirm the account and data categories. Keep a tested recovery option before disabling cloud backup or synchronization.
2. Review Google Photos backup separately. In the camera settings, turn off "Save location" if future photos do not need location tags.
3. Before sharing sensitive images, check the actual exported file for location metadata. Use a trusted export or metadata-removal process and verify the result.

Not every cloud item has the same encryption protection. Photos sharing controls do not necessarily strip camera-written location data from the original file.

18 Protect messages on the device

1. Use the encrypted communication apps approved for your work. Verify the recipient and, for sensitive exchanges, confirm identity through a separate trusted channel.
2. In Signal > profile > Privacy, enable Screen Lock and set a suitable timeout. Review Screen Security to conceal previews in the app switcher.
3. Review linked devices, notification previews and retention settings in each messaging app. Remove access that is no longer needed.

Signal's screen lock uses device authentication and is different from its account PIN. Screenshot controls cannot prevent the recipient from saving or photographing a message.

Documentation: references 26-32 on pages 11-12.

Add stronger controls deliberately

For higher-risk use. Expect compatibility, notification or convenience trade-offs.

19 Consider Android Advanced Protection

1. Search Settings for "Advanced Protection." On supported devices, review Device protection, enable it when appropriate, and restart if prompted.
2. Review the listed restrictions and test essential apps, websites and accessories. Supported USB safeguards can block new data connections while the device is locked.
3. Consider Google Account Advanced Protection separately, with recovery methods ready.

Device protection and account protection are separate. Availability depends on hardware and software; Android does not use the iPhone Lockdown Mode feature.

20 Use Private Space with its limits in mind

1. On supporting Android 15+ devices, open Settings > Security & privacy > Private space. Set a separate lock and automatic locking; use a dedicated account if needed.
2. Keep critical background alerts outside it. Apps stop while the space is locked, and its local app data is not included in standard device backups.
3. Verify VPN protection inside the space. Google warns that Private Space apps bypass the main profile's VPN. Do not treat hidden apps as undetectable.

Reusing the same cloud account can reconnect data across spaces. A separate space is useful separation, not a separate identity or a guaranteed secret compartment.

21 Preserve the Red.One device configuration

1. On a Red.One GrapheneOS device, retain its provisioned profile separation, exploit protections and USB controls. Google Play may be intentionally limited to a separate profile.
2. Add only necessary apps. Check permissions and VPN behavior in each profile you use; do not move sensitive work into a convenience profile by default.
3. Do not root, unlock the bootloader or disable security controls to work around an app problem. Ask Red.One to review the compatibility issue.

GrapheneOS controls are not universal Android settings. Test banking, work access, calling, navigation and emergency functions before relying on a stricter setup.

Documentation: references 21, 23, 33-35, 37 on pages 11-12.

Keep the protection working

A short review is more useful than settings you never check again.

Weekly or after a major update

Confirm Android and apps are current, inspect security alerts and remove apps you no longer use.

Review new permissions, linked devices and location sharing. Check that your Red.One VPN still reconnects on Wi-Fi and cellular data.

Before travel or sensitive activity

Carry only the accounts, files and apps needed. Confirm you can recover important accounts without relying on the phone alone.

Use trusted charging equipment, review Wi-Fi auto-connect and sharing visibility, and test the communication and navigation tools you will rely on.

For a hotspot, Private Space or a separate user profile, verify VPN coverage at that endpoint instead of assuming it is inherited.

After changing privacy settings

Check ordinary calls and messages, essential notifications, maps, work sign-in and your chosen lost-device recovery method.

Confirm the VPN endpoint and DNS behavior. Where block-without-VPN is enabled, verify that internet traffic is blocked when the tunnel is unavailable.

Document an approved exception rather than broadly turning off protection. Do not place essential background alerts inside a locked Private Space.

When something looks wrong

Stop the suspicious activity and contact Red.One or your designated security team through a trusted channel. Record the alert and what happened immediately beforehand.

Do not approve unexpected sign-ins, install a suggested "fix," or factory-reset the phone before getting guidance. A configuration issue and a compromised device require different responses.

Support and device-specific guidance

red-one.info/support | info@red-one.info

Documentation: references 1-3, 7-11, 20-24, 34-35, 38 on pages 11-12.

Sources and further reading

First-party guidance reviewed 8 October 2026. Settings may change after publication.

- 01 LaSorsa & Associates - Android privacy setup**
<https://www.lasorsa.com/android-privacy-a-step-by-step-setup/>
- 02 LaSorsa & Associates - Google Play privacy and security**
<https://www.lasorsa.com/google-play-store-settings-for-privacy-and-security/>
- 03 LaSorsa & Associates - Google Account privacy**
<https://www.lasorsa.com/google-account-privacy-settings/>
- 04 LaSorsa & Associates - iPhone guide / impact-level structure**
<https://www.lasorsa.com/iphone-privacy-guide/>
- 05 Google - Check and update Android**
<https://support.google.com/android/answer/7680439>
- 06 Google - Set a screen lock**
<https://support.google.com/android/answer/9079129>
- 07 Google - Theft protection and Identity Check**
<https://support.google.com/android/answer/15146908>
- 08 Google - Prepare to find a lost Android device**
<https://support.google.com/android/answer/3265955>
- 09 Google - Make your account more secure**
<https://support.google.com/accounts/answer/46526>
- 10 Google - Play Protect**
<https://support.google.com/googleplay/answer/2812853>
- 11 Google - Change app permissions**
<https://support.google.com/android/answer/9431959>
- 12 Google - Web & App Activity**
<https://support.google.com/accounts/answer/54068>
- 13 Google - Search Services History and Personalized Recommendations**
<https://support.google.com/websearch/answer/17025248>
- 14 Google - Manage Maps Timeline**
<https://support.google.com/maps/answer/6258979>
- 15 Google - Android advertising privacy**
<https://support.google.com/android/answer/13720755>
- 16 Google - Personalization and history on Google Play**
<https://support.google.com/googleplay/answer/16693200>
- 17 Google - Manage Android location settings**
<https://support.google.com/android/answer/3467281>
- 18 Google - Gemini activity and privacy**
<https://support.google.com/gemini/answer/13278892>
- 19 Google - Gemini Connected Apps**
<https://support.google.com/gemini/answer/13695044>
- 20 Red.One - WireGuard VPN quick setup**
<https://www.red-one.info/assets/docs/vpn-quick-setup.pdf>

Sources and further reading

First-party guidance reviewed 8 October 2026. Settings may change after publication.

- 21 Android Developers - VPN behavior, always-on and blocking**
<https://developer.android.com/develop/connectivity/vpn>
- 22 Google - Advanced network settings and Private DNS**
<https://support.google.com/android/answer/9654714>
- 23 GrapheneOS - FAQ: VPN, DNS and profile considerations**
<https://grapheneos.org/faq>
- 24 Proton VPN - Android hotspot VPN limitation**
<https://protonvpn.com/support/share-vpn-connection-android-hotspot>
- 25 Google - Quick Share visibility and sharing**
<https://support.google.com/android/answer/9286773>
- 26 Google - Chrome safety and security settings**
<https://support.google.com/chrome/answer/10468685>
- 27 Google - Chrome cookies and third-party cookies**
<https://support.google.com/chrome/answer/95647>
- 28 Google - Incognito mode and its limits**
<https://support.google.com/chrome/answer/95464>
- 29 Google - Android backups and restoration**
<https://support.google.com/android/answer/2819582>
- 30 Google - Photos location information and sharing**
<https://support.google.com/photos/answer/6153599>
- 31 Signal - Screen Lock**
<https://support.signal.org/hc/en-us/articles/360007059572-Screen-Lock>
- 32 Signal - Screen Security**
<https://support.signal.org/hc/en-us/articles/360043469312-Screen-Security>
- 33 Google - Android Advanced Protection**
<https://support.google.com/android/answer/16339980>
- 34 Google - Private Space setup and limitations**
<https://support.google.com/android/answer/15341885>
- 35 GrapheneOS - Usage guide and security controls**
<https://grapheneos.org/usage>
- 36 Sophos - Intercept X for Mobile App Protection**
<https://docs.sophos.com/esg/sixm-android/help/en-us/Features/AppProtection/>
- 37 Google - Advanced Protection USB safeguards**
<https://support.google.com/android/answer/16778864>
- 38 LaSorsa & Associates - Privacy habits and practical limitations**
<https://www.lasorsa.com/private-phones-dont-exist-private-habits-do/>
- 39 Google - Lock-screen notifications**
<https://support.google.com/android/answer/9079661>
- 40 Google - Usage and diagnostics reporting**
<https://support.google.com/android/answer/6078260>