How to Protect Your Privacy When Using AI (Step by Step)

AI Safety & Privacy · about 19 minutes · 2026-11-11

A fully illustrated 28-step guide to protecting your privacy when using AI: audit what you share, lock down accounts and data settings, handle sensitive material, then review, delete and build lasting habits.

Phase 1 — Audit What You Actually Share

1. **List every AI tool you use**
   List every AI tool you use.
2. **Classify the data each one sees**
   Classify the data each one sees.
3. **Check what is stored and for how long**
   Check what is stored and for how long.
4. **Locate the delete and export controls**
   Locate the delete and export controls.
5. **Trim each prompt to the minimum needed**
   Trim each prompt to the minimum needed.
6. **Redact identifiers before pasting**
   Redact identifiers before pasting.
7. **Prefer local or no-retention modes**
   Prefer local or no-retention modes.

Phase 2 — Lock Down Accounts and Settings

8. **Use a distinct, strong password**
   Use a distinct, strong password.
9. **Turn on two-factor authentication**
   Turn on two-factor authentication.
10. **Review connected apps and permissions**
    Review connected apps and permissions.
11. **Separate work from personal use**
    Separate work from personal use.
12. **Disable training on your content**
    Disable training on your content.
13. **Choose the shortest retention period**
    Choose the shortest retention period.
14. **Check where your data is processed**
    Check where your data is processed.

Phase 3 — Handle Sensitive Material Safely

15. Keep regulated and secret data out entirely

Keep regulated and secret data out entirely.

16. Anonymise case studies and examples

Anonymise case studies and examples.

17. Get consent before uploading others' data

Get consent before uploading others' data.

18. Write a no-go list for your team

Write a no-go list for your team.

19. Scan answers for leaked fragments

Scan answers for leaked fragments.

20. Verify facts before you rely on them

Verify facts before you rely on them.

21. Store AI outputs at the right sensitivity

Store AI outputs at the right sensitivity.

Phase 4 — Review, Delete and Build Lasting Habits

22. Delete old conversations monthly

Delete old conversations monthly.

23. Revoke access when a project ends

Revoke access when a project ends.

24. Audit sign-ins and activity logs

Audit sign-ins and activity logs.

25. Close accounts you no longer use

Close accounts you no longer use.

26. Write a one-page personal rule

Write a one-page personal rule.

27. Share results without permanent links

Share results without permanent links.

28. Recheck settings after tool updates

Recheck settings after tool updates.

Sources

1. Mozilla — web and browser resources
   https://www.mozilla.org/
2. NIST — AI Risk Management Framework
   https://www.nist.gov/
3. Anthropic — AI research and documentation
   https://www.anthropic.com/
4. USA.gov — official U.S. government services
   https://www.usa.gov/

Written as a checklist from https://www.howcompass.com/how-to/How-to-Protect-Privacy-When-Using-AI. Corrections: https://www.howcompas