Acceptable use policy

Version 2 · Approved 18 November 2026 · Next review 18 November 2027
Owned by the Founder & CEO · Approved by the Founder & CEO
Latest version: https://gdpr.complydog.com/documents/policies/acceptable-use

Why we have this policy

Most security problems start with an everyday slip. These are the simple rules everyone at ComplyDog follows to avoid them.

Who it applies to

Everyone who works for us or on our behalf, on any device they use for work, including their own.

Devices

- Keep devices up to date and let updates install promptly.
- Keep the disk encrypted and the screen locking after 5 minutes.
- Never leave a device unlocked or unattended in public.
- Report a lost or stolen device straight away.

Accounts and passwords

- Use your own accounts only, and never share them.
- Use a different strong password for each account, kept in NordPass.
- Turn on two-step sign-in wherever it's offered.

Information and tools

- Use company information only for your work.
- Store it only in the tools we've approved. New tools, including AI tools, need approval from the Founder & CEO first.
- Don't paste customer or confidential information into tools we haven't approved.
- Be careful with links and attachments, and check unexpected requests for money or passwords another way.

Working away from the office

Work only on networks you trust, or use the company VPN if there is one. Keep screens and calls private in public places.

Leaving

When you leave, return company devices and delete company information from your own devices.

Problems and questions

Report anything suspicious to support@complydog.com. The Founder & CEO owns this policy and looks at it again at least every 12 months. The Founder & CEO approved it. When we review this policy, we also check it's being followed: we look at the records it asks for and fix any gaps we find. If something in this policy can't be followed, the Founder & CEO can agree an exception. It's written down with the reason, what we do instead and an end date.