

# Acceptable use policy

|                |                                                                        |
|----------------|------------------------------------------------------------------------|
| Version        | 1.0                                                                    |
| Effective date | 27 October 2026                                                        |
| Owner          | Robin Ashford                                                          |
| Applies to     | Everyone with access to Final Frame systems, accounts or customer data |
| Review         | 27 October 2027                                                        |
| MPA CSBP       | OR-1.1, OP-2.0, TS-1.4                                                 |

**Approved by Robin Ashford, Founder, 27 October 2026**

---

## Systems this covers

- Google Cloud project and the Google account that administers it
- GitHub organisation
- WorkOS, Postmark, Resend, fal, TMDb, fanart.tv, EIDR and every other account in the Vendor management policy
- Google Workspace mail for final-frame.com
- The Macs used for development (see the Workstation security policy)
- The Final Frame platform itself, including the platform admin plane

## You must

- Use these systems only for Final Frame work.
- Use your own named account. Never share a login, a session or a recovery code.
- Keep a second factor on every account that has one available.
- Keep secrets in Secret Manager or the password manager. Nowhere else.
- Lock your screen when you step away.
- Report anything that looks wrong at once, to security@final-frame.com or to Robin (see the Incident response policy).
- Complete the security awareness module before access, every 12 months, and when its version changes.

## You must not

- Download customer content to a workstation unless the task needs it. If it does, delete it when the task ends. Never copy it to removable media, personal cloud storage or a personal device.
- Open customer content on a phone or tablet.
- Paste customer content, secrets or production data into any AI tool, chat or search engine that is not listed in the AI use policy.
- Give an AI coding assistant production credentials beyond what a supervised session needs, or customer content at all.

- Use the platform admin "View as" feature except to answer a support request from that Org, or to investigate an incident. Each use is in that Org's audit trail.
- Use production data in local development or tests. Use the seed data and factories.
- Turn off a security control (CI check, MFA, logging, RLS, rate limit) to save time.
- Install software from sources you do not trust.

## **Customer content on screen**

Work with customer content where nobody else can see the screen. No screenshots or screen recordings of customer content except to fix a bug, and delete them after.

## **Monitoring**

Activity on company systems is logged (see the Logging and monitoring policy). Logs may be reviewed to investigate an incident.

## **Breaches of this policy**

A breach is handled as an incident. It can lead to loss of access and, for contractors, ending the contract.

---

Final Frame Ltd · Registered in England and Wales · Company number 17413345 · [www.final-frame.com/trust](http://www.final-frame.com/trust)