15. Staff training and awareness record

> **Template.** Part of the open-source AI App Policy Kit, version 1.0. Replace everything in [square brackets], delete what does not apply, and have the person who runs the business approve it. A starting point, not legal advice.

Business	[Business name]
Document owner	[Name and role]
Approved by, and date	[Name], [date]
Next review	[Date, at most 12 months on]

Why this matters

A policy nobody has read protects nobody. A regulator, an insurer or a large customer will also ask for evidence that staff were told. Training does not need to be a course: half an hour with the policies and a few real examples is enough for most small teams.

Who it covers

Everyone who works for [Business name], contractors included, from their first week.

The rules

1. **New starters are trained in their first week,** before they get access to customer data.
2. **Everyone repeats it every 12 months,** and when a policy changes in a way that affects their work.
3. **Training covers the topics below,** with examples from this business.
4. **People with more access get more.** Anyone who writes or releases code, or administers systems, also covers documents 03, 04, 05, 12 and 14.
5. **Everyone confirms** they have read the policies that apply to them. Record it below.
6. **Practise.** Once a year, walk through a made-up incident as a team (document 06). Send a harmless test phishing email if you can.
7. **Nobody is punished for reporting.** People who report their own mistake quickly are thanked. A business that hears about problems early has fewer bad ones.

What everyone covers

- ☐ Which AI tools are approved, and what must never go into them (document 01).
- ☐ What personal data is, and what we hold (document 02).
- ☐ Passwords, the password manager and two-step sign-in (document 03).
- ☐ Spotting phishing, fake invoices and voice or video impersonation, including AI-made fakes.
- ☐ Checking AI output before using it.
- ☐ What an incident is, and who to phone (document 06).

- ☐ What to do when a customer asks for their data or asks for it to be deleted (document 10).
- ☐ Locking devices, and reporting a lost one the same day.

Training record

Name	Role	Date trained	Topics	Policies read and confirmed	Trained by	Next due
[Name]	[Role]	[Date]	[All staff topics]	[01, 02, 03, 06, 10]	[Name]	[Date]
[Name]	[Developer]	[ ]	[All, plus technical]	[All]	[ ]	[ ]

Practice record

Date	Exercise	Who took part	What we learned	Changes made
[Date]	[Incident walk-through: a leaked API key]	[Names]	[ ]	[ ]

Policy acknowledgement

I have read the policies listed against my name, I understand them, and I know who to ask if I am unsure.

Name	Signature or email confirmation	Date
[ ]	[ ]	[ ]

Checklist

- ☐ Every current member of staff has a row in the training record, dated within 12 months.
- ☐ Every starter in the last 12 months was trained in their first week.
- ☐ One practice exercise was held in the last 12 months.
- ☐ Contractors with access are included.

References

- NCSC, free cyber security training for staff, and *Exercise in a Box*.
- ICO, *Training and awareness* (accountability framework).

AI App Policy Kit, version 1.0. © 2026 PugliseWeb LTD, licensed under CC BY 4.0: use it, change it and share it, with credit. The whole kit, and a free Software Health Check of your app against it: https://www.pugliseweb.com/ai-policy-kit