

AI Usage Policy: one-page template

AI Administrator · Day 6 · Session 11 · Lab step 7

Participant handout

Organisation: _____ **Version:** 1.0 **Date:** _____ **Owner (role):** _____

Keep every heading to two or three sentences. Use real tool names, a real approver role and a real review date. Under 500 words.

1. Purpose and scope

What this policy covers (chat assistants, automations, agents) and who it applies to (staff, contractors, interns).

2. Approved tools

The named products and tiers staff may use (for example “Gemini through the company Workspace account, not the free app”), and how to request a new one (who decides, how long it takes).

3. Data rules

Public or internal: any approved tool. Personal data: redact or pseudonymise first; only business tiers with a data-processing agreement, in region _____. Confidential: only where the contract forbids training. Regulated or secret (card numbers, passwords, legal privilege): never sent to a model.

4. Human oversight

Actions that always need a named approver before they run (Tier 4 external and Tier 5 money, people, legal). Every gate writes an audit-log row: decision, approver, time.

5. Permissions

One service account per workflow with the narrowest scopes; tools allowlisted; permission mode set by the highest tier. No passwords or API keys in prompts, documents or shared sheets: they live in the tool’s credential store.

6. Components

Skills, templates, community nodes and connectors only from _____ (approved sources). An inventory per workflow: component, source, version, who installed it. Versions pinned; updates reviewed.

7. Monitoring and incidents

Who reviews the logs, and how often. The kill switch (who can unpublish a workflow, and how). Who to tell, within how many hours, when something goes wrong (and the data-protection notice duty that applies).

8. Ownership and review

Policy owner (role, not only a name). Approved by _____. Next review: _____ (every six months, or after any incident).

Signed: _____ (role) _____ Date _____