AI GOVERNANCE GUIDE

# Writing Your AI Acceptable Use Policy

The sections a practical AI policy needs, what to include in each and the decisions your leadership team has to make.

Most organizations already have people using AI tools at work, often without clear rules. A short, practical policy sets expectations, protects information and gives people the confidence to use approved tools well. This guide sets out a practical structure. Use it as a checklist while you write a policy in your own words.

### Important: read before using this guide

- **General guidance only.** This guide is provided for general information. It is not legal, privacy, employment, regulatory or other professional advice, and it does not create an advisory, client or other relationship with ilene.ai.
- **Not written for your organization.** It may not reflect the laws, regulations, collective agreements, contracts or public sector directives that apply to you. These vary by jurisdiction and sector and change over time.
- **You are responsible for your policy.** Your organization is solely responsible for the policy it writes, approves, implements and enforces, and for confirming that it complies with all applicable laws. Have it reviewed by qualified legal counsel and your privacy and security advisors before adoption.
- **No warranty or liability.** ilene.ai makes no representation that this guide is complete, accurate, current or suitable for any purpose and, to the fullest extent permitted by law, accepts no liability for any loss or claim arising from its use. Current as of October 2026.

## The structure at a glance

**PART A**
**Foundations**
Purpose, scope, definitions and principles

**PART B**
**Rules of use**
Approved tools, information, acceptable and prohibited uses

**PART C**
**Safeguards**
Review, transparency, intellectual property, security, incidents

**PART D**
**Governance**
Roles, training, exceptions, compliance and review

## PART A Foundations

Set the intent and the boundaries.

### 1 Purpose

Why the policy exists, and the balance it strikes between productive use of AI and protecting information, people and reputation.

**DECIDE** Is the tone enabling, cautious, or deliberately both?

### 2 Scope

Who it covers (employees, contractors, volunteers), which tools (standalone generative AI, AI features in existing software, tools you build) and personal devices used for work.

**DECIDE** How it relates to existing policies. State that the stricter rule applies.

### 3 Definitions

Plain definitions of AI tool, generative AI, approved tool, output, personal information and confidential information.

**DECIDE** Reuse terms from your privacy and security policies so they match.

### 4 Guiding principles

Five or six short principles: people stay accountable, protect information, verify output, be transparent, treat people fairly, use approved tools.

**DECIDE** Which principles reflect your values and your sector.

© 2026 **ilene.ai** · General guidance only. Not legal advice.

# Rules and safeguards

## PART B Rules of use

The sections people will read most. Make them concrete.

### 5 Approved tools

Where the approved list lives, what each tool may be used for, the highest level of information it may receive, and how to request a new tool.

**DECIDE** Who assesses tools, and what you check in vendor terms: data retention, training on your data, data location and security.

### 6 Information you may use with AI tools

A simple table that matches each information classification to approved and unapproved tools, plus a default rule for when someone is unsure, such as treating the information as confidential and asking.

| Example classification | Approved AI tools | Unapproved or public AI tools |
|---|---|---|
| **Public** | Permitted | Permitted |
| **Internal** | Permitted | Not permitted |
| **Confidential** | Only in tools approved for it | Not permitted |
| **Personal information** | Only in approved tools, after a privacy review | Not permitted |
| **Restricted** | Only with written approval | Not permitted |

**DECIDE** Align with your existing classification scheme, and confirm privacy, records and data location obligations with counsel.

### 7 Acceptable uses

Practical examples such as drafting, summarizing, brainstorming, research starting points and code assistance, each with its review condition.

**DECIDE** Which uses are open to everyone and which need approval.

### 8 Prohibited uses

Clear examples: entering information above the permitted level; making or materially influencing decisions about individuals, such as hiring, discipline or eligibility, without an approved process and meaningful human review; impersonation and deceptive synthetic media; presenting unchecked output as fact; bypassing security controls.

**DECIDE** Which additional prohibitions your sector or regulators require.

## PART C Safeguards

Keep people accountable and risks visible.

### 9 Human review and accountability

Who is responsible for output, what to check (errors, invented citations, bias, outdated or sensitive content) and which uses need a second reviewer.

**DECIDE** Your threshold for higher-impact review.

### 10 Transparency and disclosure

When to disclose AI use in external content, how AI systems that talk to clients or the public identify themselves, and labelling of synthetic media.

**DECIDE** Your disclosure threshold.

### 11 Intellectual property

Respecting tool licence terms, checking external content before publication, and who owns work created with AI tools.

**DECIDE** Which agreements govern ownership.

### 12 Security

Company accounts and single sign-on, required privacy settings, approval before connecting AI to systems, and awareness of AI-enabled phishing and deepfakes.

**DECIDE** Which settings are mandatory for each tool.

### 13 Reporting incidents and concerns

What to report (information entered that the policy does not permit, harmful or materially wrong output, unexpected tool behaviour, suspected AI-enabled fraud), where to report it, how quickly, and protection against retaliation.

**DECIDE** The reporting channel and who owns the response.

© 2026 **ilene.ai** · General guidance only. Not legal advice.

# Governance and rollout

ilene.ai

## PART D Governance

Make the policy owned, maintained and enforceable.

### 14 Roles and responsibilities

A short table of who does what: policy owner, IT and security, privacy, legal, people leaders and everyone in scope.

**DECIDE** Who owns the policy and reports on AI use to leadership.

### 15 Training

The training required before using approved tools, and how often it is refreshed.

**DECIDE** Whether higher-impact uses need additional training.

### 16 Exceptions

How to request an exception, who approves it, and that approvals are documented and time-limited.

**DECIDE** The approver and the maximum duration.

### 17 Compliance

How breaches are handled, by reference to existing disciplinary processes, contracts and any collective agreements.

**DECIDE** Whether access can be suspended during a review.

### 18 Review

How often the policy is reviewed, at least annually is common, and the triggers for an earlier review: a change in law, the tools in use, or the way the organization uses AI.

## Document control

Put this at the top of the final policy.

| | | |
|---|---|---|
| **Policy owner** | **Approved by** | **Effective date** |
| **Next review date** | **Version** | **Related policies** |

## Rollout checklist

- [ ] A policy owner is named and accountable.
- [ ] Current AI use across teams is mapped, including tools staff already use.
- [ ] Data rules match your information classification scheme.
- [ ] Legal, privacy and security reviews are complete.
- [ ] The approved tool list is published, with uses and limits.
- [ ] Related policies are cross-referenced and conflicts resolved.
- [ ] The policy is communicated with practical team examples.
- [ ] Training is available and completion is tracked.
- [ ] The incident reporting route is tested.
- [ ] The first review date is set.

### Keep it short

A policy people read is worth more than a complete one they skip. Aim for a few pages, plain language and real examples, and move detail such as the approved tool list into a separate page you can update without re-approving the policy.

### Want help writing and rolling it out?

Through AI Governance, ilene.ai works with your leadership, legal and privacy advisors to set AI policy, approved tools and oversight that fit how your organization operates.

**Book a strategy call**

© 2026 **ilene.ai** · hello@ilene.ai · General guidance only. Not legal advice.