LEGAL·IO

Policy Templates for Use of Generative AI

Templates for In-House Legal Departments to Encourage Responsible Use of Generative AI

About the Generative Artificial Intelligence Use Policy Templates

Legal.io, the leading on-demand legal talent network, is proud to present our community of legal professionals with resources to help them be more effective and efficient.

The Generative Artificial Intelligence Use Policy templates in this document are a resource for in-house legal departments that are looking to put in place generative AI guidelines for the first time, or are looking to benchmark their existing guidelines against a set of best practices.

You'll find several templates in this collection:

- A Sample Policy for Internal Use of Generative AI Tools by Developers
- A Sample Policy for Internal Use of Generative AI Tools by Employees
- A Sample Generative AI Use Policy for Employees and Contractors

The templates outline a framework for the sourcing and use of generative AI technologies, ensuring that they are leveraged to enhance productivity and quality of work, while minimizing risks such as data security vulnerabilities and intellectual property infringement.

The templates were co-developed with a publicly listed company with a mature legal operations function that is very active in the field of Artificial Intelligence. They are provided by way of example and reference only, and not as legal advice. Make sure to adapt these guidelines to your company's specific needs and requirements.

Explore other resources to streamline your legal department, such as our Salary Insights tool, used by legal departments in top tech and Fortune 500 firms across the U.S. to benchmark in-house legal compensation and assist with budgeting.

Sample Policy for Internal Use of Generative AI Tools by Developers

Purpose

This policy establishes guidelines for the safe and responsible use of generative AI tools for code completion within our company, with the goal of ensuring the security and integrity of our codebase.

Scope

This policy applies to all developers who use generative AI tools for code completion within our company.

Responsible Use

Developers who use generative AI tools for code completion must use the tools responsibly, to assist in coding. Generative AI tools are not a replacement for critical thinking and coding expertise. You are responsible for the code you write with the help of AI tools, and you must follow the same policies and practices you would use for any other type of code that you did not originate. Use of the tools must be consistent with any agreements or policies or practices that apply to your project.

Intellectual Property

Developers who use AI tools must ensure that any features designed to highlight and/or block outputs that match public code are active at all times.

Output Validation

Developers must use the same internal processes required for any code they did not independently originate, to validate the output generated by the tool before incorporating it into the codebase. This includes verifying that it meets the company’s general coding standards and does not introduce security vulnerabilities or other issues.

Performance Monitoring

Developers must monitor the tool's performance and identify any issues or limitations, and address them as needed. This includes monitoring the quality and accuracy of the generated code and assessing the tool's impact on productivity and efficiency.

Documentation

As part of standard software documentation requirements, developers should keep a record of how the tool is being used, by whom, and for what purpose. This can help identify issues or limitations, and ensure that the tool is being used appropriately and effectively.

Training

Developers who will use an AI tool must take *[list an internal onboarding training or link to documentation that will cover these principles]* training support to ensure that they understand its capabilities and limitations, and can use it effectively and responsibly.

Policy Review

This policy will be reviewed and updated periodically to ensure that it remains relevant and effective.

By following this policy, we can ensure that our company's adoption of generative AI tools for coding is done safely and responsibly, and that our codebase remains secure and protected.

Sample Policy for Internal Use of Generative AI Tools by Employees

Purpose

This policy establishes guidelines for the safe and responsible use of generative AI tools across our company, with the goal of ensuring the security, integrity and efficiency of our operations.

Scope

This policy applies to all employees who use generative AI tools within our company, regardless of their department or role.

Responsible Use

Employees must use generative AI tools responsibly, to assist in their respective tasks. These tools are not a replacement for critical thinking and professional expertise. You are responsible for the output you generate with the help of AI tools, and you must follow the same policies and practices you would for any other type of work. Use of the tools must be consistent with any agreements, policies, or practices that apply to your project or department.

Intellectual Property

Employees must ensure that any features designed to highlight and/or block outputs that match proprietary or public information are active at all times to protect intellectual property.

Output Validation

Employees are required to use the same internal processes required for any work they did not independently originate, to validate the output generated by the tool before it is finalized or incorporated into any project. This includes verifying that it meets the company’s standards and does not introduce security vulnerabilities, legal issues, or other concerns.

Performance Monitoring

Employees must monitor the tool's performance and identify any issues or limitations, addressing them as needed. This includes monitoring the quality and accuracy of the generated output and assessing the tool's impact on productivity and efficiency.

Documentation

As part of standard documentation requirements, employees should keep a record of how the tool is being used, by whom, and for what purpose. This can help identify issues or limitations and ensure that the tool is being used appropriately and effectively.

Training

Employees who will use an AI tool must take *[list an internal onboarding training or link to documentation that will cover these principles]* training support to ensure that they understand its capabilities and limitations, and can use it effectively and responsibly.

Policy Review

This policy will be reviewed and updated periodically to ensure that it remains relevant and effective.

By following this policy, we can ensure that our company's adoption of generative AI tools is done safely and responsibly, enhancing our operations while keeping our data and intellectual property secure and protected.

Sample Generative AI Use Policy for Employees and Contractors

This policy establishes the guidelines and standards for sourcing and use of generative AI technologies to conduct company business. It applies to all employees and contractors.

Generative AI Defined
“Generative AI” is a category of algorithms that are trained on data sets and can generate text, images, video, sound or other work product (output) in response to prompts (input). Examples include ChatGPT (text-to-text/image), GitHub CoPilot (text-to-code), Midjourney (text-to-image), and ModelScope (text-to-video). Generative AI can also appear as a feature in another application, such as “Compose with AI” in Front.

Our Policy: Balancing of Benefits and Risks
Generative AI can deliver significant benefits by enhancing idea generation and creativity, increasing productivity, uncovering patterns and insights, and improving quality of work product. Simultaneously, generative AI carries significant risks, including factually untrue outputs (“hallucinations”), biased outputs, data security vulnerabilities, IP infringement, privacy risks, and unacceptable license terms.

We will adopt generative AI responsibly: only if we anticipate clear, articulated benefits and we have concluded in this policy or via the approval process below that the risks are acceptable in light of the anticipated benefits.

Guidelines for Sourcing and Adoption
As a general rule, we will use generative AI only via company-provided accounts. Use of generative AI for business purposes via a personal account (for example, a personal ChatGPT account) is permissible only if all of these conditions are met: (1) the use is unrestricted (see below), (2) the user has taken all available steps to opt-out of sharing input and output data into the training data set, (3) the user has enabled all optional safety features, and (4) the user is familiar and complies at all times with the terms and conditions for use of personal account.

Prior to implementation of any generative AI in a company account – either as a standalone application or as a feature of another system – we will follow this process:

1. The requester must explain the anticipated benefits from the generative AI's adoption and obtain the informed approval of [(1_______, (2) _________, and (3) _______].
2. The technology must undergo security and legal review. Important findings of this review will be:
   - **a**. Whether there are known data security vulnerabilities and their severity
   - **b**. How the data training set was sourced. We will not use generative AI trained on illegally or unethically sourced data sets
   - **c**. Whether inputs and outputs go into the training data set. As a general rule, we will not use generative AI that takes our inputs and outputs and adds them to the training data set. Exceptions require strong justification and express, informed approval by the Legal team
   - **d**. Whether the technology has safety features designed to minimize the risks of its use (hallucinations, bias, IP infringement, etc.). We will closely review the safety features of each proposed generative AI technology and, where available, compare them to those of alternatives
   - **e**. Whether the technology is licensed under non-standard or unacceptable terms
3. If this is a new purchase, our Purchasing Policy and process apply
4. The results of the security and legal reviews are presented to the [Department Executive, __________and ________], and they reapprove the adoption of the technology after review of the findings

The implementer of the generative AI is responsible for enabling opt-out of training data set contributions and all available safety features. After implementation, the implementer must periodically check whether new safety features have become available. During the first year of adoption, checks for new safety features should be quarterly, then annual or upon a major release, whichever is sooner.

Guidelines for Use

There are three categories of use: prohibited, controlled and unrestricted.

Prohibited Uses

We will not use generative AI:

1. To create images, videos or sounds for company use[1]
2. Where the input is sensitive personal data[2] or the output affects fundamental rights of individuals, such as the rights to be free from discrimination, to participate in employment, to obtain credit or be eligible for government assistance, etc.
3. Where the input is system access credentials (for our systems or those of any third party)
4. Any use that violates any law, company policy or the technology's terms and conditions for use

Controlled Uses

These uses require special precautions:

1. We may use generative AI to write code only if:
    a. The generative AI has an enabled safety feature to minimize the risk of copying or license infringement of known software
    b. The file header of each file contains the following notice: "This file was created in whole or in part by generative AI."
    c. The code is scanned for vulnerabilities and IP infringement by a specialized tool (for example, Black Duck) prior to being committed
2. Any use where the input is our leads/prospects/customers list (in whole or in part). This requires the prior review and approval of the [Department Executive] in consultation with Legal and InfoSec.
3. Any use where the output is directly presented to customers or third parties without human review. We must present additional information to aid the recipient in evaluating the output.
4. Any new category of use that is neither prohibited nor unrestricted. Each new category of use must be approved by the Department Executive in consultation with Legal and InfoSec. Legal will be responsible for updating this policy to record the use as prohibited, controlled or unrestricted.

Unrestricted Uses

The following use of generative AI is unrestricted (all conditions must be met): (1) the input is not confidential information (of our company, a customer or any third party) or personal information, (2) the output will be used only internally or externally[1] in marketing materials after human review, (3) the output will not affect the[2] rights or obligations of any person, and (4) the output will not be incorporated in company technology.

Any controlled or unrestricted use must comply with applicable law, company policies and the terms and conditions for use of the generative AI.

Users' Responsibilities

It is critical that each of us uses generative AI responsibly and sensibly. Below are several examples of responsible use, but these are not exclusive:

1. If the output is a statement of fact, the user is responsible for checking it for accuracy

2. If the output is about people, the user is responsible for checking it for detectable bias

3. If the user generates code or other additions to our technology, the user must label them as such by including the notice: "This file was created in whole or in part by generative AI."

4. Consistent with our "golden rule"[3] the user must have a lawful and ethical intent when using AI. Examples of unlawful and/or unethical intent are: disinformation, manipulation, discrimination, defamation, invasion of privacy.

[1] There is ongoing litigation involving generative AI that uses image data sets to generate images. Given the legal uncertainty and our limited need for images, vides and sounds, currently the legal risks outweigh the benefits to us from generating images, videos and sounds via AI. If the balance of risks and benefits changes, this section will be updated.

[2] Our Data Classification and Protection Policy defined sensitive personal data as:

- An individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (i) Social security number; (ii) driver's license number, identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data
- An individual's precise geolocation
- An individual's racial or ethnic origin, religious or philosophical beliefs, or union membership
- The contents of an individual's mail, email, and text messages unless is the intended recipient of the communication
- Genetic information

[3] The golden rule is in our Employee Handbook and states that we must act at all times lawfully, ethically and with integrity.

Enforcement

We will investigate any complaint or alleged violation of the law or this policy and, if necessary, take appropriate corrective action and/or disciplinary action (up to and including termination of employment).

Review

We will review this policy periodically and update it as necessary to reflect technological advancements, changes in the law or company policy, or changes in our risk appetite. Because of the ongoing rapid development of generative AI and its evolving risks, initially we will review this policy quarterly. We will announce any updates to all.

Date of Adoption	
Revision Date	
Author	
Approver	
Approver	
Approver	

Legal.io – The Leading On-Demand Legal Talent Network

With more than 40,000 legal professionals in the U.S. and beyond, Legal.io is one of the world's largest legal services networks, serving US legal departments with local and international needs.

Hire top in-house legal talent for contract, part-time and full-time legal roles quickly and efficiently. Ramp up and down as business needs require.

Quality Candidates
Our team conducts a tech-enabled, targeted search for each role, presenting a shortlist of highly qualified candidates to our clients.

Faster Speed-to-Fill
Our sourcing precision and expertise of our trained lawyer-recruiters enable a faster, more efficient talent acquisition process.

Transparent Pricing
We offer transparent, cost-plus pricing that allows us to charge our clients a fair market price for our services.

For more information about Legal.io, please visit www.legal.io or email hiring@legal.io to learn more about our staffing solutions