Working Draft
Open Source - Taking Contributions

Company GenAI Policy Considerations

Purpose of the Document

To provide in-house legal teams information and guidance on developing an internal Generative AI Policy for their company. This is open-sourced and I am actively soliciting examples. Email get@laurajg.com with your example.

Examples

Company AI Policy Example #1
Company AI Policy Example #2
How We Regulate AI Use at Ironclad

Table of Contents

Company Policy Considerations

Here are some questions to consider when developing an AI Policy. You can answer these questions and use them as a prompt in ChatGPT to have ChatGPT write the policy for you. Afterwhich, you can refine the output.

At a high level the policy should cover:

- Guidelines on when and where AI tools can be used
- Guidelines for use based on use case (e.g. development, marketing, legal, etc.)
- Restrictions on the types of data that can be input into the AI
- Advice for elevating output and using such output
- Procedures for reporting and addressing any issues or concerns that arise
- Training requirements for employees who use the AI
- Procedures for updating and revising the policy as the technology and its applications evolve

Check out my LinkedIn Post on 5 Considerations Before Using AI that can guide employees making decisions (it is based on UK Government Guidance to civil servants on use of generative AI).

Potential Prompt Template:

Specifically, the policy could address the following issues. You can provide answers to the following applicable questions and input it as a prompt into ChatGPT.

The purpose of the policy:

- What is the purpose of the policy?
- What are you trying to achieve by having a policy on AI use?
- Identify and describe the risks that are unique to your company. It's important to convey these risks to employees so they understand the rationale behind the policy.

The scope of the policy:

- What does the policy cover?
- Does it cover all AI tools, or just certain types of AI tools like specific subset, such as generative AI tools like GPT-3?

The applicable regulations

- What specific rules and regulations need to be addressed in the policy?
    - Check out Raymond Sun's AI Legislation Tracker
- How are you addressing data privacy regulations?
    - Consider the implications of data handling when using AI tools. If an AI tool is trained on sensitive company data, how is this data stored and processed? How is it shared with third parties? What measures are in place to protect this data?
    - See Privacy Considerations when Working with an an AI Vendor
- How are you addressing security concerns?

- How are addressing ethical concerns raised by AI use?
- If you are in Europe, how are you preparing for the AI Act?
    - It will require substantial documentation from developers similar to GDPR
    - Transparency and Explainability:
        - Depending on the context, you may need to be able to explain how the AI made a particular decision. Your policy should address how the company will ensure transparency and explainability in its AI system

The applicable internal rules:

- What constitutes acceptable use of the AI tool and what does not?
    - For instance, you may decide that using AI tools for certain types of work is acceptable, but using them with sensitive or proprietary data is not.
- What specific internal rules need to be addressed in the policy?
    - These could include things like how AI tools should be used, who is responsible for using them, and what happens if someone violates the policy.
- How are you addressing data inaccuracy?
- Intellectual Property Considerations
    - If your company develops its own AI systems, you should consider how intellectual property rights will be protected.
    - If you use third-party AI systems, you should understand the terms and conditions of their use to avoid infringing on others' intellectual property rights.

The enforcement of the policy:

- How will the policy be enforced?
- Will there be penalties for violating the policy?

The training and education of employees:

- How will employees be trained on the policy?
- Will there be any resources available to help them understand the policy and how to comply with it?
- Will you provide prompt engineering training?

The monitoring and review:

- How will the use of AI tools be monitored and how often will the policy be reviewed?
    - AI is a rapidly evolving field, so it's important that your policy is able to evolve with it.

Example Policies and Resources

Note, I have tried using ChatGPT-4 with Bing to find example of internal companies policies and have only found the resources listed below:

- Risk Management for Legal AI Solutions
- How We Regulate AI Use at Ironclad
- Resources for Employers AI Usage Policy
- Traverse Legal: AI ACCEPTABLE USAGE POLICY: EMPLOYEE HANDBOOK FOR RESPONSIBLE AI USAGE.

ChatGPT Drafted Generic AI Policy

[Your Company Name] Generative AI Usage Policy

1. Introduction

Artificial Intelligence (AI) is transforming the way we work, offering new possibilities for increasing efficiency and innovation. However, it is essential that we use AI tools responsibly and ethically, with respect for privacy and data security.

2. Purpose

Artificial intelligence (AI) has the potential to greatly enhance productivity and decision-making within our organization. However, it also introduces new risks and challenges, particularly in terms of data security and privacy. The use of generative AI tools must therefore be governed carefully to maximize their benefits while minimizing their risks.

By setting clear guidelines for the use of these tools, we can ensure that they are used in a way that aligns with our company's values and goals, and that respects the privacy and security of our data. This policy is an important part of our broader commitment to responsible AI usage and governance.

This policy provides guidelines for the responsible and ethical use of generative AI tools, such as ChatGPT, within [Your Company Name]. It seeks to protect our organization, our employees, and our stakeholders by preventing unauthorized disclosure of sensitive information and ensuring that these tools are used appropriately and responsibly.

3. Scope

This policy applies to all employees, contractors, and third parties working on behalf of [Your Company Name] who use generative AI tools in the course of their duties.

4. Definitions

Generative AI: A type of artificial intelligence that is capable of creating content, such as text, images, or music, that is novel or not directly based on provided data.

5. Guidelines

a) Authorized Usage: Generative AI tools should only be used for purposes directly related to your duties at [Your Company Name]. Unauthorized uses include but are not limited to generating inappropriate or offensive content, and any use that violates laws, regulations, or company policies.

b) Data Security: Generative AI tools should not be used with sensitive or confidential information, including but not limited to customer data, proprietary code, and internal communications.

c) Prompt Engineering: Employees using generative AI tools should be trained on prompt engineering to ensure that the information used as prompts does not compromise the security or privacy of company data.

d) Reporting Concerns: Any concerns about the use of generative AI tools, including potential data breaches or misuse, should be reported to [appropriate department/individual] immediately.

6. Roles and Responsibilities

a) Senior Management: Responsible for overseeing the implementation of this policy and providing necessary resources.

b) IT Department: Responsible for providing training, managing access to AI tools, and responding to reported concerns.

c) Employees and Contractors: Responsible for following this policy and reporting any concerns.

7. Training

All users of generative AI tools are required to complete a training course provided by the IT Department on safe and effective use of these tools. This training will cover topics such as data security, prompt engineering, and how to report concerns.

8. Non-compliance

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contractual agreements.

9. Policy Review

This policy will be reviewed annually, or as needed, by the senior management team in consultation with the IT Department and other relevant stakeholders, to reflect changes in technology, laws, business practices, or company needs. All revisions will be communicated to the relevant parties.

10. Approval and Implementation

This policy is approved by [Name, Title] and will be implemented from [Date].

Company Approaches

Companies Embracing ChatGPT

- **Bain & Company**: Bain & Company is a global management consulting firm that is using ChatGPT to help its employees with research and analysis.
- **Quizlet**: Quizlet is an educational technology company that is using ChatGPT to create personalized learning experiences for its users.
- **Instacart**: Instacart is a grocery delivery company that is using ChatGPT to answer customer questions and provide recommendations.
- **Shopify**: Shopify is an e-commerce platform that is using ChatGPT to help its merchants with customer service and marketing.
- **Duolingo**: Duolingo is a language learning platform that is using ChatGPT to create personalized learning experiences for its users.
- **Snapchat**: Snapchat is using ChatGPT to create a more personalized experience for its users.
- **Coca-Cola**: Coca-Cola is using ChatGPT to help it with its marketing and product development.
- Insurance: Zurich Insurance is using ChatGPT to help it with its claims processing and customer service.
- **Mattel**: Mattel is using ChatGPT to help it with its product design and marketing.
- **Absci**: Absci is using ChatGPT to help it with its drug discovery research.

Companies Banning or Restricting AI Tools and ChatGPT

These companies have banned ChatGPT because they are concerned about the potential for the tool to be used for malicious purposes. ChatGPT is a powerful tool that can be used to generate text, translate languages, write different kinds of creative content, and answer your questions in an informative way. However, it is also a tool that can be used to generate fake news articles, phishing emails, and other malicious content.The companies that have banned ChatGPT are taking a proactive approach to security. They are recognizing that AI tools can be

used for both good and bad, and they are taking steps to mitigate the risks associated with using these tools.

- **Amazon:** Amazon has banned ChatGPT from being used by its employees after it was discovered that some employees had used the tool to generate code that could be used to exploit security vulnerabilities.
- **Verizon**: Verizon has banned ChatGPT from being used by its employees after it was discovered that some employees had used the tool to generate fake news articles.
- **JPMorgan Chase**: JPMorgan Chase has banned ChatGPT from being used by its employees after it was discovered that some employees had used the tool to generate phishing emails.
- **Northrop Grumman**: Northrop Grumman has banned ChatGPT from being used by its employees after it was discovered that some employees had used the tool to generate sensitive company information.
- **Samsung**: Samsung has banned the use of ChatGPT by its employees. The ban was issued after it was discovered that some employees had used ChatGPT to leak sensitive company information. ChatGPT is a large language model chatbot developed by OpenAI. It is trained on a massive dataset of text and code, and can generate text, translate languages, write different kinds of creative content, and answer your questions in an informative way. However, ChatGPT has also been criticized for its potential to be used for malicious purposes, such as leaking sensitive information. Samsung's ban on ChatGPT is a sign that the company is taking the security of its intellectual property seriously. It is also a reminder that AI tools can be used for both good and bad, and that it is important to use them responsibly.
- **Apple:** Apple restricts workers from using ChatGPT and other third-party AI tools, citing concerns about confidential data leaks. They have also told employees not to use the automated software code-writing program Copilot. Apple is reportedly developing its own AI tools.
- **Bank of America**: Bank of America added ChatGPT to its list of unauthorized apps that employees are prohibited from using for business. This was part of stricter compliance measures around internal communications following fines for the firm’s failure to monitor employee use of unauthorized messaging apps like WhatsApp.
- **Calix**: Calix banned ChatGPT across all business functions and devices. The CEO cited a recent data leak at Samsung as the driving reason for the ban, highlighting the potential for ChatGPT to expose sensitive information like confidential internal memos or customer contracts under NDA to outsiders.
- **Citigroup:** Citigroup added ChatGPT to its standard firm-wide controls for third-party software, where certain categories of websites are automatically restricted. The company is actively exploring the benefits and potential associated risks of using this technology.
- **Deutsche Bank**: Deutsche Bank disabled access to ChatGPT for its staff as a standard practice for third-party websites. The restriction is aimed at protecting the bank from data leakage. In the meantime, the bank says it will evaluate how to best use the platform while protecting its own and client’s data. The bank is also developing AI chatbots1.

- **Goldman Sachs**: Goldman Sachs blocked access to ChatGPT for employees through an automatic restriction on third-party software. However, Goldman is in the process of developing its own generative AI tools.
- **Verizon**: Verizon informed employees that ChatGPT is not accessible via corporate systems due to the risk of losing control of sensitive information like customer data and source code. They are also concerned about privacy and security with ChatGPT1.

Choosing an AI Vendor

Vendor Management Considerations

If you're purchasing AI solutions from vendors, your policy should also cover how these relationships will be managed, including vetting vendors for their own data privacy, security, and ethical use policies.

Here are some steps you can follow:

1. Identify the AI tools that your employees will be using.
2. Evaluate the security risks associated with each tool.
3. Create a policy that outlines the requirements that employees must follow when using AI tools.
4. Ensure that all employees use AI tools in a secure, responsible and confidential manner.
5. Prohibit employees from using AI tools not on the list for company-related activities.

Privacy Considerations when working with an AI Vendor

Using AI means privacy responsibilities if you are inputting personal data.

You need:

- To have a DPA in place: because your company is the controller
- Vet the AI provider: because they are your data processor
- You'll likely transfer data to the US. So you need SCCs, a TIA, additional security measures and more (not easy after the Meta decision)
- Get security documents from the AI provider: because you might incorporate it into your product / platform / services / support - and its required pursuant to the GDPR,
- Do a DPIA (see DPIA on a Page for more information)
- If your company starts incorporating the AI into your product / platform / services, you need to update your own DPA (sub processor list) and/or your privacy policy
- Make sure that you have the right to the data and that data deletion & retention is outlined in your policy.

- Train your organisation on how to use the AI, so they know they can and cant do, eg don't upload personal data (as outlined in your policy).
- And remember data accuracy can be a problem.

Thanks to Stine Mangor Tornmark for the overview.

High Level Risk and Benefits of Gen AI Use:

Risks

- Generate incorrect or misleading information.
- Generate confidential information.
- Generate offensive or harmful content.
- Generate bias and discriminatory content and results.

Benefits

- Automate tasks.
- Generate creative content.
- Answer questions in an informative way.

Legal Specific

- Contract negotiation and drafting assistance (see Chatting with Contracts with ChatGPT)
- Other uses by in-house counsel (see Real-life stories of generative AI for in-house legal: Laura Jeffords Greenberg)