# Responsible AI Usage Policy for [Organization Name]

Artificial Intelligence (AI) is an increasingly important tool, offering unprecedented possibilities for content creation, customer engagement and automating workflows. However, with great power comes great responsibility. Therefore, this AI usage policy is designed to guide our team and organization in the responsible, transparent, and ethical use of AI in their work. The aim of this policy is not to hinder creativity or innovation, but rather to ensure that our use of AI aligns with our overall organizational identity and values and respects our customers' rights.

## Guidelines for Responsible AI Usage

### Transparency

It's crucial that we remain transparent about our use of AI. This includes acknowledging when AI has been used to create or modify content. This can be through a blanket statement on our website, a statement when asked or integrated into contracts with clients.

### Example Transparency Statement:

The following is an example of a transparency statement on your use of generative AI. Please edit to make it your own.

* We use AI to assist in some content development and processes at our organization. To ensure transparency, accountability, quality and privacy, we adhere to internal AI usage standards. These standards help us safeguard against biases, maintain data security, and uphold our commitment to ethical content and operating practices. One of these standards is that AI should be used to assist in content creation and streamlining our workflows, but never fully automating anything. We ensure that every piece of content and process we develop is shaped and reviewed by people who have an understanding of our organization, audience and AI’s limitations.

### Tool Selection

The following AI tools have been approved for use in our company. DO NOT use any tools outside of those on this list or approved in writing by our security team on company devices or to do company related work.

[Insert a bulleted list here]

### Accountability

Responsibility cannot be outsourced to a machine. Always remember that humans are ultimately accountable for the actions of the AI. AI is an assistant, not a replacement for good judgment. Our company policy is that we should NEVER publish or send something that has been written entirely by AI without human development or review for quality and accuracy. Additionally, in case of any negative outcomes from AI-assisted content, we must take responsibility and remediate as necessary.

### Use Cases That Should Not Leverage AI

While there are many positive use cases of AI assistance in our work, there are specific types of work in which we have decided as a company to restrict the use of AI. Do not use AI for the following:

[Insert any uses that your company would like to restrict based on your own standards. This will vary by company so have your own discussion internally about what scope you’d like to set. Limited use cases could - but don’t have to - include: performance evaluations, legal contracts, specific coding projects, etc. ]

## Addressing Specific Issues

### Bias

AI systems learn from the data they are fed, and thus can unintentionally perpetuate biases found in their training material. Many language models have filters to reduce the risk of bias or harmful outputs, but filters aren’t enough. It is our responsibility to ensure that content we produce is reviewed for potential bias and developed to be inclusive and accessible.

### Privacy

We must protect the privacy of our customers. See our list of approved tools with reliable privacy policies and do not submit customer data into AI tools or LLMs. In addition, we must protect the privacy of our own intellectual property (IP). Sticking with the approved list of tools above will help safeguard both and ensure our data and IP is not used to train publicly accessible language models.

### Consent

It is our policy that we must always obtain the explicit and informed consent of our clients or customers whenever their data is being used by our AI tools. Consent is paramount and its

violation will not be tolerated.

### Security

AI systems can be targets for cyber-attacks. Please review the approved list of AI tools and discuss any additional tools you subscribe to or use on company devices with the security team.

### Ethical Considerations

AI should not be used to mislead or manipulate customers. All content created using AI should be ethical and in line with our organizational values. AI content should go through a review process to check for bias, inaccuracies and other risks.

### Impersonation

It is our company policy that employees should not use AI to impersonate any person without their expressed permission. AI can allow you to create “in the style” of public figures; as a policy we do not do that in our company. Designated employees may, with permission and review, use AI to mimic the writing style of a current [Organization Name] employee for the purposes of ghostwriting or editing content from that individual.

## Training Employees on AI Usage

All employees involved in creating content with AI should receive appropriate training. This should cover both the technical aspects of using AI, and the ethical considerations outlined in this policy.

## Best Practices for Implementation

To practically implement this policy, always follow these steps:

1. Understand the AI system you're using, including how it works and its potential limitations.
2. Ensure that every new hire and existing employee you manage has read this policy.
3. For specific tools, document or use materials from the company to document its functionality, limitations, and our organization’s standards for using the technology.
4. Continually update your knowledge and training as AI technology evolves.

## Legal Compliance

Our use of AI system technology and any related data processing will always comply with all pertinent local, state, federal, and international laws and regulations. Non-compliance with these legal requirements will be viewed very seriously.

## Incident Response

In the event of any AI-related incidents or policy breaches, including harmful outputs, data breaches, bias-related issues, or other concerns arising from the use of AI, it is crucial to have a standardized and efficient incident response process in place. All incidents must be reported immediately to the designated contact or department, allowing us to swiftly mitigate risks, prevent further consequences, and be prepared to identify, manage, and mitigate any potential risks or liabilities associated with AI usage.

Example Incident Response Process:

1. **Identification**: If an AI-related incident is detected or suspected, immediately report it to the designated point of contact or department within our organization. This could be a supervisor, AI Ethics Officer, or a dedicated AI Incident Response Team.
2. **Notification**: The individual who identifies the incident should provide a brief but clear description of the issue, including a summary of any potentially affected data, AI-related workflows, or stakeholders.
3. **Assessment**: The designated incident response team or responsible department will evaluate the reported incident, determine its severity, and classify it accordingly (e.g., minor, major, or critical). This assessment should also consider the potential impact on our organization, clients, and any relevant legal, ethical, or compliance matters.
4. **Containment**: Once the severity of the incident has been established, the responsible team should take immediate action to confine its effects. This could include disabling specific AI functionalities, isolating data, or suspending any ongoing processes as needed.
5. **Investigation**: Concurrent with containment, investigate the root cause of the incident and gather any necessary data or evidence. This step is crucial for understanding and remediating the issue as well as preventing future occurrences.
6. **Remediation**: After investigating the root cause, develop and implement a strategy to resolve the incident. This may involve correcting any affected content or data, modifying AI configurations, or conducting additional training for employees, as appropriate.
7. **Communication**: Keep relevant stakeholders and personnel apprised of the incident, its status, and any updates. It is important to establish a reliable communication channel for effective collaboration and transparency.
8. **Review**: Once the incident has been resolved, conduct a thorough debrief with the responsible parties to review the lessons learned and make recommendations for improvements. Use this feedback to update and refine the incident response process and the AI Usage Policy as necessary.
9. **Documentation**: Document the entire incident response process, from initial detection to resolution, including any decisions made, actions taken, and the rationale behind them. This documentation will help improve future incident responses and can serve as a reference for legal or compliance purposes, if necessary.

## Enforcement

The effective enforcement of this policy requires everyone’s cooperation. Specifically, [enter responsible role/team] will be responsible for enforcing this policy. Violations of this policy can be grounds for disciplinary action up to and including termination of employment.

## Review and Updating of Policy

This policy will be reviewed on a [bi-annual/annual] basis, or more frequently as required, to ensure it continues to meet legal requirements and any advancements or changes in our AI capabilities. Amendments or modifications to this policy will be communicated to all stakeholders.

## Acceptance

By using AI in your work, you agree to comply with this policy. Non-compliance will be taken seriously and could lead to disciplinary action or employment termination. Remember, the goal of this policy is not to restrict creativity, but to ensure that we use AI responsibly and ethically. By following these guidelines, we can harness the power of AI while respecting our customers and upholding our company values.