Net Friends

AI Policy Guidelines

A Guide to Safe and Responsible AI Use

This guide focuses on creating AI policy content. Each section of the policy is broken down, with questions about what to think about and examples.

Topics range from **authorized use cases**, **data handling** and **accountability**.

The goal is to create a clear, comprehensive, and accessible document that can be understood by all employees.

Company AI Policy

This policy applies to all employees, contractors, and any third parties who use, develop, or manage AI tools on behalf of **[Small Business Name]**.

This includes, but is not limited to:

01. Software-As-A-Service

AI-powered software-as-a-service for marketing, customer service, data analysis, etc.

02. AI Toolkit

Generative AI tools (e.g., ChatGPT, Midjourney) for content creation.

03. Automation Tools

AI-driven automation tools.

Permitted Uses

Step 1

Consider these questions:

- [ ] What specific business problem are we trying to solve with this AI tool or use case? Is it a core business function, a repetitive task, or a new opportunity?
- [ ] Is AI the best solution for this problem? Could a simpler, non-AI solution achieve the same result with less risk and complexity?
- [ ] How will this use of AI enhance our products, services, or internal processes without compromising quality or our brand?

Step 2

Determine what uses are acceptable to your business. Use the examples below as a guide when creating your own.

Ideation

Generating drafts of marketing copy, emails, or internal documents.

Time Saving

Automating routine and repetitive tasks.

AI Summary

Summarizing long articles or reports.

Analysis

Analyzing business data to identify trends and insights.

Automation Tools

Improving customer service with AI-powered chatbots for frequently asked questions.

Prohibited Uses

Step 1

Consider these questions:

- [ ] Who owns the output of the tool?
- [ ] Could using this tool compromise our own IP?
- [ ] Does the tool introduce new vulnerabilities to our network? For example, does it require access to our internal systems or data, creating a potential entry point for malicious actors?
- [ ] Does using this tool violate existing company policies?

Step 2

Determine what uses are prohibited to your business. Use the examples below as a guide when creating your own.

Critical Thinking

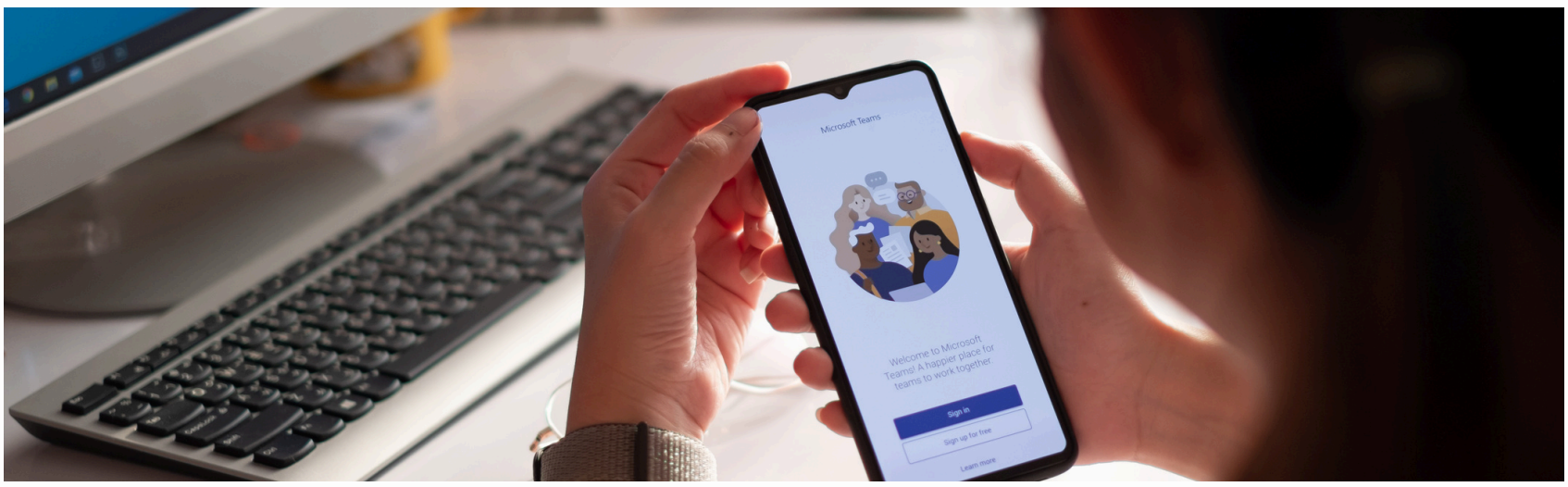
Using AI to make final decisions on hiring, promotions, or disciplinary actions without human review.

Privacy Concerns

Inputting confidential, sensitive data into public, and/or unapproved AI tools.

Copyright Violations

Using AI to create content that is plagiarized, misleading, or violates copyright.



Privacy and Data Protection

Step 1

Consider these questions:

- [ ] What kind of data will this AI use, and where does it come from? Is it confidential, proprietary, or personally identifiable information (PII)?
- [ ] Is our data clean, well-governed, and ready for AI? Do we have a robust data management and governance framework in place?
- [ ] Does our use of this AI comply with all relevant data privacy regulations?
- [ ] If we're using a third-party AI tool, what are their data retention and privacy policies? Do we know for certain that our data will not be used to train their public models or be accessible to other users?

Step 2

Determine what steps will be taken to protect the privacy and security of your data. Use the examples below as a guide to create your steps.

Approved Tools and Vendor Management

All AI tools used by the company must be approved by **[Name/Title, e.g., the Business Owner, the IT Manager]**.

Confidentiality of Inputs

Employees are strictly forbidden from entering any proprietary company data, trade secrets, or any other confidential information into third-party, publicly available AI tools.

Data Minimization

Only use the minimum amount of data necessary for a specific task.

Right to Be Forgotten/Erasure

It may be difficult or impossible to delete data once it has been submitted to a third-party AI system

Employee Responsibilities

Step 1

Consider these questions:

- [ ] What is the approval process? Who should an employee contact to request approval for a new AI tool or use case? What information do they need to provide in the request?
- [ ] Who is ultimately accountable for the AI's output?
- [ ] What are the requirements for human oversight? When must an AI-generated output be reviewed, edited, or verified by a human?
- [ ] What training will be provided? What topics will be covered in the training, and how often will it be updated?
- [ ] How can employees get help? Is there a dedicated channel for support?

Step 2

What does responsible AI use in your business look like? Use the examples below as a guide to define responsible AI for your business.

Due Diligence

Employees must review all AI-generated content or decisions for accuracy, fairness, and compliance with company policies.

Confidentiality

Do not input any proprietary, confidential, or sensitive company or customer data into external AI tools unless the tool has been explicitly vetted and approved for that purpose.

Attribution

When using AI to assist in creative work, employees must be aware of and adhere to copyright and intellectual property laws. Where appropriate, disclose the use of AI.

Use Only Approved Tools

AI tools will be evaluated and approved by the company.

Policy Review

Consider these questions:

- [ ] What is the standard cadence to review the policy?
- [ ] What are triggering events that require immediate review?
- [ ] Examples include new regulations, security event, or technology shifts.
- [ ] Who is involved in the review process?
- [ ] How will we communicate with employees?

Sample Wording

This policy will be reviewed and updated **[Frequency, e.g., annually]** or as new AI technologies and best practices emerge.

Contact Net Friends for expert guidance!

Our Contact Information

919-680-3763 contact@NetFriends.com NetFriends.com