

Four Points for Your Artificial Intelligence Acceptable Use Policy

August 02, 2023

As technologies like ChatGPT and other artificial intelligence tools have entered the mainstream, billions of individuals have used such tools for assistance with everyday tasks, both personal and professional. These tools, however, are not without risks. To address such risks, an increasing number of companies have implemented an AI acceptable use policy. Here are four points to consider in implementing your company's acceptable use policy:

- **Establish expectations.** What are acceptable and unacceptable uses of AI? What data can be input into what types of AI tools? Under what circumstances? What are the consequences for failure to adhere to the AI acceptable use policy?
- **Address AI-specific issues.** An AI acceptable use policy can establish policies and procedures for addressing AI-specific issues (e.g., ensuring AI use does not offend any legal requirements or contractual commitments). While some aspects could potentially be folded into other policies (e.g., revising an incident response plan to address data incidents related to AI), drafting an AI acceptable use policy can be an efficient tool for comprehensively addressing AI.
- **Explain the “why” behind any restrictions or prohibitions.** Many companies restrict AI use to address concerns such as those related to privacy, intellectual property, ethics, and regulatory oversight concerns. Educating employees about the risks of such tools can help mitigate the risk of accidental legal violations and increase employee compliance with such policies.
- **Demonstrate diligence.** From employee acknowledgment and training to expanded incident response plans, an AI acceptable use policy can show company efforts to comply with legal requirements.

The precise restrictions and explanations to include in an AI acceptable use policy can vary significantly, but these four points should create a useful starting point.

Authored By



Irma Reboso Solares



Patricia M. Carreiro

Related Practices

[Cybersecurity and Privacy](#)

[Technology](#)

[Digital and E-Commerce Engagement and Innovation](#)

Related Industries

[Technology](#)

©2024 Carlton Fields, P.A. Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.