# How to Protect Your Company from Legal Risks of Workplace AI Use

That artificial intelligence has direct ramifications on the workplace isn't exactly breaking news. But the newly launched ChatGPT app, which has gained over 100 million active users in less than 2 months of existence, has taken the AI threat to a completely different level. If you've ignored the issue in the past, you'll need to start taking action right now. Going through this analysis is a good first step because it will brief you on the ways workplace AI can hurt your company and what you must do to manage these risks.

### The Promise of AI and LLMs

ChatGPT (GPT stands for Generative Pretrained Transformer) is an example of an AI product referred to as Large Language Models (LLMs), aka, "chatbot." After being crammed with massive amounts of data, LLMs are trained, i.e., programmed via algorithms to interact with human users, follow instructions, identify and learn from their mistakes. An LLM is a real-world HAL, an AI language platform that users can converse with and instruct to perform certain tasks. And that can be extremely useful around the workplace.

### Potential Employee Uses of LLMs

> There are many ways that employees can use AI and LLMs to do their job better and more efficiently, including to:
>
> - Create and analyze code;
> - Translate languages;
> - Respond to customer or client calls;
> - Summarize messages and emails;
> - Analyze and explain lengthy, dense or technical materials;
> - Write content;
> - Perform calculations;
> - Answer technical questions;
> - Perform research.

But as science fiction has taught us, relying on AI can be dangerous. While HAL was too smart for humanity, LLMs remain imperfect and subject to limitations. So, even though the product undergoes rigorous performance testing, its data contains errors and gaps; its algorithms are essentially based on the programmer's guesses of what a user's questions and instructions will be. Another problem with LLMs and other "generative AI" language models is that they reflect the sudden and hidden biases of their human creators.

## The 2 Options

If your employees are using LLMs, bad things can happen. One way to protect your company from harm is to ban use of ChatGPT and other LLMs in the workplace. But while safe, that approach will also cost you the potential benefits of LLM use. Accordingly, you may be better served by allowing such use while implementing a policy that establishes guidelines to manage the potential dangers. Here are 10 risks to be on the lookout for and how to implement an LLMs use policy to protect yourself.

## 1. Confidentiality Breaches

**Problem:** Employees may share trade secrets, confidential or other proprietary information about your company, customers, clients and employees when engaging in work-related conversations with LLMs. Once entered into an LLM, this information may then leak onto the internet and into the public domain, laying it bare for all the world to see.

**Solution:** In your policy, ban employees from entering any confidential or proprietary information about the company or its business, operations, clients or personnel into an LLM. In addition, separately insert language banning the entry of such data into your confidentiality and proprietary information policies and contract clauses. You might also want to limit the access of employees entrusted with sensitive information to LLM platforms.

## 2. Personal Data Privacy Breaches

**Problem:** LLMs may collect personal information about their users, including social security numbers, IP addresses, browser types and settings and even health information protected by personal privacy laws. Thus, using or integrating information from an LLM may expose you to liability under these laws, especially if government regulators audit your databases.

**Solution:** Require employees to follow company data privacy and security protocols when using LLMs and use software or regular audits to monitor their usage. Also consider whether you need to update your company privacy rules to account for LLM usage.

## 3. Customer Data Privacy Breaches

**Problem:** LLM platforms "can't keep secrets." So, entering business information you collect from clients, customers, partners and business associates into an LLM may constitute a breach of your contractual obligation to keep that information confidential and not disclose it without express authorization.

**Solution:** Ban employees from entering confidential client data into LLMs unless and until you've completely vetted the product and the effectiveness of its data security controls and features. Alternatively, consider telling your clients and customers about and getting their written consent to these uses before engaging in them.

## 4. Original Work Contractual Breaches

**Problem:** It's becoming increasingly common for businesses to require creative services vendors, suppliers or contractors to expressly promise to use one or more particular employees—or, in some cases, any employees who are human—to generate the work product without the aid of AI. Use of LLMs could run afoul of such contractual obligations, especially if the application is for content generation.

**Solution:** Recognize that the relationship between an employee user and LLM isn’t like the relationship between an employee user and Microsoft Word or other word processing program or non-AI tool and ensure that employees aren’t using LLM and AI for unauthorized content creation.

### 5. Cyber Attacks

**Problem:** One group of people that LLMs make life easier for is hackers. Vengeful former and current employees and other malicious users no longer need sophisticated programming skills to create malware to carry out cyber attacks against your company. LLMs also make it easier for bad actors with poor English-language skills to engage in phishing, disinformation and other schemes targeting English-speaking companies, employees and operations. While LLMs include user rules and safety mechanisms to guard against abuses, these controls can be circumvented.

**Solution:** Train employees on the cyber dangers of LLM platforms and require them to comply with all company data security policies, procedures and protocols when using them.

### 6. Copyright & Other Infringement

**Problem:** LLM developers use vast amounts of data to create and train their products, some of which may be protected by copyright, trademark, patent and other intellectual property laws. Employees who use that protected data for work may expose your company to risk of liability for infringement. In addition, using or integrating chatbot data for your own products might compromise your company’s ownership over the resulting product to the extent that the original source of the embedded information may be able to claim at least partial ownership in the output.

**Solution:** The IP issues involved in LLMs use are technical and complex and you should get advice from an experienced lawyer before sticking your neck out too far. For example, there’s currently uncertainty over whether IP created by AI is even protectable under copyright, patent and other laws designed to protect property created by a human “author” or “inventor.”

## 7. Discrimination

**Problem:** Discrimination isn’t always the product of racists, bigots, misogynists and other haters. Because of our history, culture and education, there’s some degree of hidden prejudice in just about all human beings, even those who earnestly accept and try to practice the principles of equal opportunity and nondiscrimination. That includes the people who generate the data used to train chatbots. Accordingly, Human rights commissioners in Canada and the US have warned against the danger of inherent bias posed by AI use.

**Example:** In 2018, Amazon pulled the plug on an AI-based recruitment program after discovering that the algorithm skewed against women. The model was programmed to vet candidates by observing patterns in resumes submitted to the company over a 10-year period. Most of the candidates in the training set had been men. As a result, the AI taught itself that male candidates were preferred over female candidates. In other cases, it’s been reported that LLMs generated code stating that only White and Asian men make for good scientists.

**Solution:** First and foremost, warn users that LLMs can be taught to discriminate and caution them to be sensitive to these risks when taking instructions from or using content these platforms generate. Rigorously test your LLM algorithms to ensure they don’t discriminate—either directly or in the form of seemingly neutral content or direction that has an indirect impact on a protected group as in the Amazon example above. Last but not least, include express language addressing discrimination by algorithm in your company nondiscrimination policies.

## 8. Deceptive Trade Practices

**Problem:** Using LLMs to produce content may violate fraud and deceptive trade practices laws when consumers believe or the product is marketed as being generated by a human. **Example:** The US government went after an adultery-based dating website for using an LLM to generate fake customer profiles designed to trick consumers into signing up and boost social media likes.

**Solution:** The best way to guard against potential liability for consumer fraud is to be transparent about your use of AI and LLMs. According to US regulatory guidance, “when using AI tools to interact with customers, be careful not to mislead consumers about the nature of the interaction.” Companies should also be transparent when collecting sensitive data to feed into an algorithm to power an AI tool, explain how an AI’s decisions impact a consumer and ensure that decisions are fair.

## 9. Inaccuracy & Quality Control

**Problem:** As impressive as LLMs are, they also have limitations. For example, language model AI platforms often struggle with computational tasks and give inaccurate results when asked to solve basic algebra problems. tendency to generate inaccurate results. LLMs also have knowledge gaps, for example, about world events that occur after they’re initially programmed. They also have tendency to “hallucinate,” that is, make statements that sound authoritative but are actually false.

**Solution:** Never take the accuracy of LLM-generated content for granted. Instruct employees to vet the material first before incorporating it into any work product or relying on it to make important business decisions.

## 10. Professional Ethics Violations

**Problem:** Use of AI may be problematic for lawyers, doctors, accountants and others governed by a professional code of ethics. For example, some ethical codes for lawyers define “legal representation” as a service rendered by a person who’s admitted to the bar. Accordingly, lawyers who rely on LLMs could be subject to charges of unauthorized practice of law.

**Solution:** If you’re in a regulated profession, beware of the ethical implications of AI use and ensure that your current practices are consistent with all professional and ethical codes.