



Misuses of artificial intelligence (AI) based Chatbots Across Industries





Al-based chatbots are generative Al tools that allow users to input text prompts and see natural sounding text as outputs.

Many misuses have put businesses and professionals in quite tricky situations since the release of ChatGPT.

See the timeline for misuses across industries.

ChatGPT is released by OpenAl



Kairoi Summaries



January 2023

Non-profit mental health service bases responses to patients on ChatGPT without patients' informed consent¹

8th Feb

6th Jan

CNET publishes article written by "Al engine" that explains compound interest incorrectly²

12th Jan

a factual error⁵

advertises Al-

based chatbot

Bard generating

Google

1st Feb

CNET publishes article written by "AI engine" that explains compound interest incorrectly³ (3/6)

Survey: 70% of workers using ChatGPT at work are not telling their boss; overall usage among professionals jumps to 43%⁴



Kairoi Summaries



Samsung runs internal seminar to advise executives on ChatGPT after staff input proprietary source code⁶

22nd Mar 4th May 12th Apr 4th Apr

Lawyer references fake court cases cited by ChatGPT9

Student asks The Guardian's archives team about a fake article mentioned in an output from ChatGPT⁷

Record daily attempts of pasting corporate data into ChatGPT detected by Cyberhaven⁸





The brief and incomplete timeline shows AI-based chatbots being used incorrectly across different industries:



- Mental health services
- Journalism
- Computer software
- Electronics
- Education
- Law

The risks are social in nature and include spreading misinformation, exposing sensitive data and harming people directly.





At Kairoi, we believe that social concerns raised by AI tools can be mitigated through robust workplace policies, and that employers can play a critical role in educating the public about AI systems.

With the help of AI and governance experts, we've developed a *Template ChatGPT Use Policy* to ensure its responsible usage in the workplace.

The template is freely available at: https://tinyurl.com/kairoi





Developing your Generative Al Use Policy



Strategic communications: Articulate your organisation's values in a way that makes them practical to enact



Policy review: Understand how internal policies interrelate and how a Generative AI Use Policy best integrates



Staff engagement: Refine value definitions through internal workshops and develop personas for each department



Implementation and monitoring: Ensure continuous reviews of AI-related policies as new tools and use cases emerge





Contact us to safeguard your organisation from misuses of generative AI tools

hello@kairoi.uk

Contribute to, adapt and share our Template ChatGPT Use Policy

https://tinyurl.com/kairoi

References

- ¹ Biron (2023) Online mental health company uses ChatGPT to help respond to users in experiment raising ethical concerns around healthcare and AI technology, *Business Insider*, online [accessed 05 June 2023]
- ² Christian (2023) CNET's Article-Writing AI Is Already Publishing Very Dumb Errors, *Futurism*, online [accessed 05 June 2023]
- ³ Christian (2023) CNET's Al Journalist Appears to Have Committed Extensive Plagiarism, Futurism, online [accessed 05 June 2023]
- ⁴ Fishbowl (2023) 70% Of Workers Using ChatGPT At Work Are Not Telling Their Boss; Overall Usage Among Professionals Jumps To 43%, *Fishbowl Insights*, online [accessed 05 June 2023]
- ⁵ Coulter & Bensinger (2023) Alphabet shares dive after Google Al chatbot Bard flubs answer in ad, *Reuters*, online [accessed 05 June 2023]
- ⁶ Jeong Doo-yong (2023) Concerns turned into reality: As soon as Samsung Electronics unlocks ChatGPT, 'misuse and abuse' appears one after another, *The Economist*, online [accessed 05 June 2023]
- ⁷ Moran (2023) ChatGPT is making up fake Guardian articles. Here's how we're responding, *The Guardian*, online [accessed 05 June 2023]
- ⁸ Coles (2023) 11% of data employees paste into ChatGPT is confidential, *Cyberhaven*, online [accessed 05 June 2023]
- ⁹ Maruf (2023) Lawyer apologizes for fake court citations from ChatGPT, *CNN*, online [accessed 05 June 2023]

Citing this slide deck

This slide deck is made available under the <u>Creative Commons</u>
Attribution 4.0 International licence. Please cite as follows:

Kairoi Ltd (2023) Misuses of artificial intelligence (AI) based Chatbots Across Industries, linkedin.com/company/kairoi