Attachment B: Additional OpenAI information

Limitations



Potential risks for elections:

Misrepresenting electoral processes or the AEC Dependent on the data ChatGPT is 'trained' on, it could misrepresent the functions and responsibilities of the AEC, including hallucinatory responses.

This could include incorrect information about Australian electoral processes, including where 'presumptions' made by the AI are not based on Australian law. For example, asking ChatGPT "do I have to vote?" may provide an American-based response.

Misinformation/disinformation

ChatGPT and other AI can be used to produce deliberately generated disinformation based on relevant prompts. Despite certain parameters in ChatGPT that detects this breach in usage policy, framing or manipulating prompts in certain ways can allow users to bypass this.

Despite violating the content policy, DALL-E could be utilised to generate convincing images of a political nature, such as a political candidate being arrested or an election worker committing fraud.

• Taking AI response as fact:

Due to the technologically advanced and often unfamiliar nature of AI, the user may take the response from ChatGPT or other AI as factual. This can include the AI 'hallucinating' fake references or sources.



OFFICIAL:SENSITIVE