Justice Institute
BRITISH COLUMBIA

PRIVACY IMPACT ASSESSMENT (PIA)
CLOSURE SUMMARY

Initiative	Chatitout
PIA Reference #	2024-002
PIA Completion Date	June 14, 2024
Project Sponsor	Junsong Zhang – Program Manager, Simulations, CTLI
Unit	CTLI

The purpose of a PIA is to determine whether an initiative complies with the *Freedom of Information and Protection of Privacy Act* ("**FIPPA**") and JIBC's policies and procedures. This document is to advise that the PIA review of this initiative has been completed. The following outlines the scope, issues, legal basis and conclusions associated with this PIA.

Initiative Description & Scope

Chatitout is an application that uses OpenAI's API to process and respond to user input. It is essentially an AI chat application.

Information Reviewed

Our review is based primarily on the PIA Questionnaire, completed by Junsong Zhang, which is attached at Schedule A. We also spoke with Technology Services to verify certain assumptions about the application, particularly the nature and scope of personal information that may be involved in its use, and where any such personal information, if provided, may be stored.

Legal Basis - Privacy

According to the PIA Questionnaire, the proposed tool does not collect any personal information for signup or otherwise. However, the nature of the proposed tool involves a high risk of accidental disclosure of personal information by the user.

Legal Basis - Security

Pursuant to section 30 of FIPPA, a public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized collection, use, disclosure or disposal. The proposed tool will not collect any personal information for signup. Information entered into the proposed tool will likely be stored outside of Canada.

Conclusions

Based on the information provided, our review has concluded that the proposed tool may be used for its intended purpose provided that users be instructed on safe use of the proposed tool, as the risk of accidentally entering personal information is high.

<u>Responsibilities</u>

CTLI is responsible for ensuring that users are informed of the risks of accidentally disclosing personal information while using the proposed tool.

Sample instructions to instructors for safe use of the proposed tool by students may take the following form:

> "Even though no personal information is required by the tool, students could accidentally enter personal information into the tool. Therefore, instructors must educate students on how to safely use the tool, prior to requiring its use. Instructors are encouraged to contract the Centre for Teaching, Learning and Innovation for guidance on how to educate students on the safe use of this tool. Given JIBC's lack of ability to monitor user activities, individual adherence to recommended practices is vital for security."

CTLI is responsible for ensuring that instructors are provided with guidance for the safe use of the proposed tool, which can be conveyed to students. We have attached as Schedule B to this PIA UBC's guidance with respect to the safe use of ChatGPT 3.5, which may be helpful in crafting such guidance.

If you have any questions or concerns about this PIA, please contact the General Counsel.

SCHEDULE A
PIA QUESTIONNAIRE

Please see attached.

PRIVACY IMPACT ASSESSMENT QUESTIONNAIRE

for

CHATITOUT

1. Purpose of the Privacy Impact Assessment Questionnaire

This form is used by JIBC to provide a high-level overview of the potential privacy risks of a current or proposed policy, system, project, program or activity. The results of these screening questions help judge the level of potential risk, the extent to which risk mitigation strategies may be needed and when completion of a privacy impact assessment is required under the *Freedom of Information and Protection of Privacy Act* (British Columbia) (the "**Act**").

2. Privacy Questions

Questions	Answers
Does the program involve personally identifiable information (PII) (as defined by the Act)? [Y/N]	This application does not require authentication or log in, hence it does not actively collect birthday, name, mailing address, etc. However, users might disclose certain personal information during the conversation. The application will record the chat history in order to generate a response to user's input.
Will the program involve the collection or creation of new information about individuals? [Y/N]	Same as above.
Will personal information about individuals be disclosed to organizations, programs, processes or people who have not previously had routine access to the information? [Y/N]	Yes. This application utilizes OpenAI's API to process user's input. Hence, users' chat history will be sent to the application which is currently hosted on render.com (we intend to move the hosting site to JI server), and then sent to OpenAI's server to generate a response. The response will be sent back and show up on user's screen. Please refer to OpenAI's privacy policy here.
Will personal information about individuals be used for a purpose it is not currently used for, or in a way it is not currently used? [Y/N]	No. This application only generates responses based on user's input.

Questions	Answers
Will the program require contacting individuals in ways that they may find intrusive? [Y/N]	No
Does the program have a collection notice or use policy? [Y/N]	Not yet. We are in the process of forming privacy statement, as well as terms of use.

3. Technology Questions

Questions	Answers
Does this program involve the implementation of a new electronic system or use of a new application or software to support the creation, collection, updating or storing, backing-up or disposition of personal information? [Y/N]	OpenAI's API is used in this application in order to generate responses.
Does this program require any modifications to existing information technology (IT) systems (e.g., integration with or consolidation of other IT systems)? [Y/N]	TBD by TS
Will a new or modified electronic system change the existing business workflow? [Y/N]	I don't think it is going to change business flow. We intend to use in conflict resolution courses as a teaching and learning tool.
Does the program involve the use of new technology that might be perceived as being privacy intrusive? [Y/N]	No.

4. Impact Questions

Questions	Answers
What are the purpose of collection, use and/or disclosure of the personal information? [Internal/External/Both]	If users chose to disclose their personal information during the chat, this application will record the chat in order to generate a response. The purpose is to coach users' through a conflict conversation.
Will personal information about the same individual that was previously maintained separately now be aggregated and stored together? [Y/N]	This application does not aggregate personal information per se. It only collects users' input in order to respond to it… No algorithm created to aggregate user information or generate user profile.. Users may leave the chat session open on their browser and then came back to continue

	the conversation. Is this considered "aggregated?"
How would you describe the information classification level of the personal information? (Select all that apply) • Highly Confidential • Confidential • Public	confidential
What are the type(s) of personal information? (Select all that apply) • Bio/demographic information • Academic/education Information • Employment information • Medical/health Information • Financial Information • Criminal information • Images • Opinions about individuals • Individuals' personal views and opinions • Business contact information • Personal contact information • Other	Users will most likely disclose their opinions about others and self during their interaction when conversing with the AI-based coach. However, depending on users' choice of topics, users may disclose other information in the list. We don't have control over what users might say, it could be anything.
What are the type(s) of individuals? (Select all that apply) • Prospects • Applicants • Students • Employees • Donors/alumni/other 3rd parties • Volunteers • Service providers • Other	We intend to use this tool in conflict resolution courses. Student, faculty, and staff may have access to this application.
How many records documenting individuals will be stored, accessed, used or disclosed? [1-1000], [1001-5000], [5,001-50,000], [50,001-100,000], [100,000+]	1-1000 Depends on user's input. Note we did NOT create admin access to this application.
How many JIBC employees, volunteers and service provider employees will be able to access, collect, use or disclose the information?	That there is no administrator role in this application. No login needed for users, and no

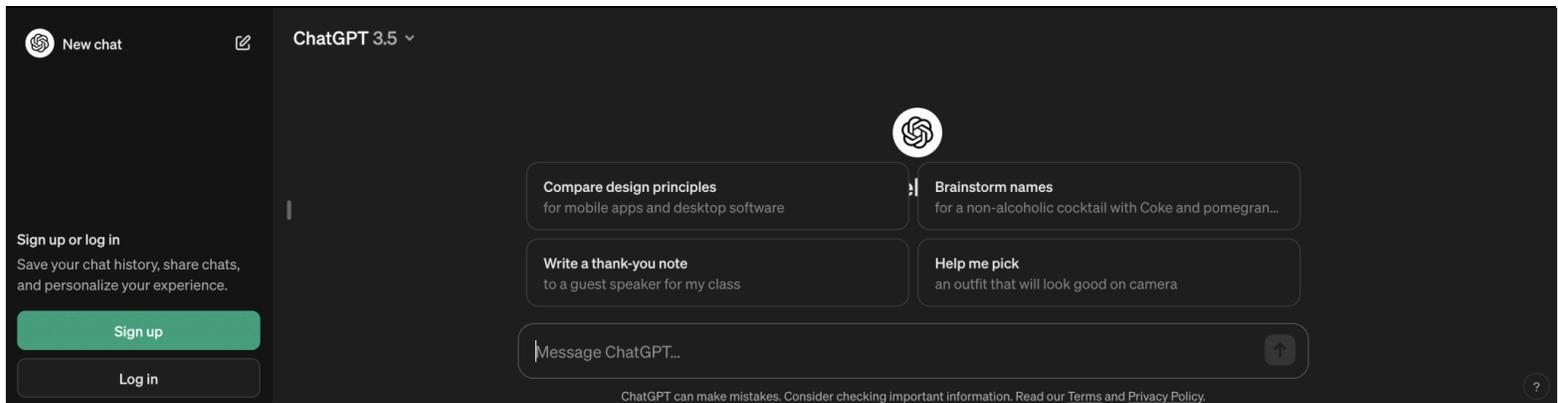|	
[1-10], [11-50], [51-100], [101-250], [251-500], [501-1,000], [1,000+]	admin login. The only way to access, use, or disclose information is probably through hacking the application and access the code base itself.
Is any of the information owned by another organization? [Y/N]	No Please refer to OpenAI's privacy policy here.

5. Probability Questions

Questions	Answers
Where will the information be stored? (Select all that apply) • <mark>On campus – JIBC servers</mark> • On campus – other • Off-campus – inside Canada • Off-campus – outside Canada	Ideally we'd like to host it on JIBC server. To be confirmed by TS regarding if it is on campus – JIBC servers.
Is any of the information accessed from outside of Canada? [Y/N]	No admin account or access in this application. However, we use OpenAI's API which is a U.S. company.
Will personal information be transmitted? (Select only one) • Personal information is used in a closed system (i.e., no connections to the Internet, Intranet or any other system and the circulation of hardcopy documents is controlled) • <mark>Personal information is used in a system that has connections to at least one other system</mark> • Personal information is transferred to a portable device (i.e., USB key, diskette, laptop computer), transferred to a different medium or is printed • Personal information is transmitted using wireless technologies	Users' chat history with the AI coach can be downloaded to users' own desktop. Users may also email it to whoever they feel appropriate. The system does not actively transmit users' chat history. However, OpenAI's API is used so it is connected to other system I guess?
Will a third party (e.g., vendor or service provider) have access to the information? [Y/N]	Potentially OpenAI
Will the program result in different record keeping systems converging? [Y/N]	No

SCHEDULE B
UBC GUIDANCE RE: USE OF CHAPGPT 3.5

Please see attached.

A.I. In Teaching and Learning

ChatGPT 3.5

Tool Name	Does it require personal information for signup?	Does it protect personal information?	Can it be recommended or required for use by students in your course?
⚠ ChatGPT 3.5 by OpenAI	⊘ **No**, not for ChatGPT Version 3.5	⚠ No, it will share information entered into the tool outside Canada. Some device data such as IP Address <u>may be stored (https://openai.com/policies/privacy-policy)</u> .	⚠ **Yes, with caution**. Students should be instructed on safe use of this tool, because the risk of accidentally entering personal information or intellectual property is high.

⚠ **INSTRUCT STUDENTS IN SAFE USE:** Even though no personal information is required by the tool, students could accidentally enter personal information or intellectual property into the tool. Therefore, **instructors must educate students on how to safely use the tool, prior to requiring its use**. Instructors can convey the guidance in the "Detailed Guidance" section below to educate about safe use of this tool. **Given UBC's lack of ability to monitor user activities, individual adherence to recommended practices is vital for security.**

About This Tool

OpenAI's **ChatGPT** is available from https://chat.openai.com/ (https://chat.openai.com/) as a free version that, as of April 2024, can be accessed without an account. The version available without an account can be referred to as ChatGPT 3.5. OpenAI also offer another version of ChatGPT called ChatGPT 4 which requires a paid account which collects private information, and thus should not be recommended for use within a course. **The information on this page is specifically about ChatGPT 3.5**.

🖹 Sample Syllabus Language

Usage of ChatGPT in this Course

In this course, you will use OpenAI's generative AI tool, ChatGPT version 3.5.

Because ChatGPT uses global data centres there is a high likelihood of data being shared or stored outside of Canada. To better protect your data and privacy, please follow these practices:

- **Do not log in to ChatGPT.** Ignore the login/signup buttons in the sidebar. ChatGPT version 3.5 does not require login.

- **Do not enter personal or private information**, or information you do not own such as PDFs of others' public work. Do not share any information that you would not publish on the internet. Anything you enter may be shared as results to other users.

- **Opt out of the 'Improve the model for everyone'** setting by clicking the small grey question mark in the lower right hand corner and then select settings from the menu that pops up. Un-select "improve model for everyone" such that it is shown as grey.

- **Enable the 'Temporary Chat' option** by clicking 'ChatGPT 3.5' towards the top left, and then enabling the 'Temporary Chat' toggle. With this option, prompts won't be part of the chat history or used to train OpenAI's future models.

- **Do not click the "Bad Response" and "Read Aloud" icons** at the bottom of a response. Clicking either icon risks unintentionally sharing the chat session data with OpenAI.

- **Start a new topic to clear the chat history** when you are done with a chat. Click "New Chat" in the sidebar to start a new topic. Starting a new topic ensures that all temporarily stored prompts and responses from the current chat session are discarded from the cache.

- **To ask OpenAI to remove any sensitive data you have accidentally provided**, see the OpenAI policies page (https://openai.com/policies/privacy-policy) to determine who to contact.

Detailed Guidance for ChatGPT   −

- **Instruct students not to log in to ChatGPT**. ChatGPT 3.5 does not require login. Students should not be instructed to ignore the "log in/sign up" buttons in the sidebar.

- **Do not require sharing sensitive data with the tool**: Information entered into the tool will be used for AI training purposes, and may be returned as results to other users. You should not require students to enter any sensitive information, personal information, or intellectual property into the tool.

- **What students can be instructed to share with the tool:** Limit data sharing to information that is "Low Risk" according to UBC's Information Security Standard U1 (https://cio.ubc.ca/information-security-standards/U1) .
  - This information may be freely disclosed or would cause minimal harm if disclosed. Examples include names and work contact information of UBC faculty and staff members; information that is posted on a public UBC website; and research of a non-personal, non-proprietary nature.

- **Instruct Students to Avoid using the feedback buttons**: Once you receive a response, ChatGPT may show you "Bad Response" and "Read Aloud" icons to give feedback on the response. Clicking either icon risks unintentionally sharing the chat session data with OpenAI. As such, it is best to avoid providing this feedback.

- **Instruct Students to opt out of the 'Improve the model for everyone' setting each time they use the tool**: By default, ChatGPT 3.5 will use any information submitted by students to help train their models. This means anything entered as part of all conversations, by default, can – and likely will – be stored and used by OpenAI in the future. By clicking the question mark icon in the lower right, and then selecting settings, students will have the option to opt out of this meaning less information is shared directly with OpenAI.

- **Instruct students to enable the 'Temporary Chat' Option**. This helps reduce the chat history within the student's browser as well as preventing the chat from being used as part of future model training. They can do this by clicking 'ChatGPT 3.5' towards the top left, and then enabling the 'Temporary Chat' toggle.

- **Remind students of the the critical limits to the tool's responses**: As with any generative AI tool, ChatGPT may give inaccurate or misleading responses known as "hallucinations". Also, ChatGPT may include ads in its responses. Keep a sharp eye out for errors or questionable responses, and externally validate the accuracy of any responses that will be broadly disseminated or relied on for decision-making.

- **Inform students that some of their information is shared automatically** with the use of the tool: Similar to most websites, a user's IP Address is shared with the service provider. Students can use the UBC VPN (https://it.ubc.ca/services/email-voice-internet/myvpn/how-access-myvpn) in order to help mask their IP address and location.

Centre for Teaching, Learning and Technology
Irving K. Barber Learning Centre

214 – 1961 East Mall
Vancouver, BC Canada V6T 1Z1
Tel 604 827 0360
Fax 604 822 9826
Website ai.ctlt.ubc.ca (https://ai.ctlt.ubc.ca)
Email ctlt.info@ubc.ca (mailto:ctlt.info@ubc.ca)

Find us on

(http://facebook.com/UBC.CTLT)   (http://twitter.com/UBC_CTLT)   (https://www.youtube.com/user/ctltresources)

(https://www.flickr.com/photos/olt/)