
The purpose of this policy is to ensure that all employees, athletes, and volunteers are informed about artificial intelligence tools and use third party and/or publicly available artificial intelligence (AI) tools in a secure, responsible, and confidential manner.

AI can be defined as the development of computer systems to perform tasks that would ordinarily require biological brainpower to accomplish, such as making sense of spoken language, learning behaviours, or solving problems.

Generative AI is a type of AI that produces content such as text, audio, code, videos, and images. This content is produced based on information that the user inputs into the AI system. Common AI tools include ChatGPT, ClickUp, Jasper and many more.

With the increased use of AI, cybercriminals can misuse AI tools to elevate and automate the quality and effectiveness of phishing scams. They are able to use AI tools to create realistic images that impersonate individuals and convince users to share confidential information. They can also automate the collection of personal information and produce highly personalized phishing messages. Additionally, chatbots can be used to initiate conversations that convince users to provide sensitive information or click on malicious links.

SOBC is committed to ensuring that the use of AI tools is safe and secure for all employees, athletes, and volunteers, as well as the organization itself. We believe that by following the guidelines outlined in this policy, we can maximize the benefits of AI tools while minimizing the potential risks associated with their use.

USE OF ARTIFICIAL INTELLIGENCE TOOLS

Protection of Confidential Information: Information and data that is confidential and/or proprietary must not be uploaded or shared with any AI tool. Any information shared or uploaded to an AI app has the potential to be made available to the public and would contravene SOBC's privacy policy.

Confidential Information can be described as Personal information of participants, athletes, coaches, and representatives including but not limited to home address, email address, personal phone numbers, date of birth, financial information, medical information, and background check information. Additionally, Confidential Information also includes information considered to be intellectual property of Special Olympics Canada or SOBC such as data, proprietary information, and trade secrets.

Use of reputable AI tools: Prior to use, AI tools should be evaluated based on their merits and reputation. Caution should be exercised when evaluating tools developed by individuals or companies without established reputations. Employees and volunteers should only use AI

applications that are approved by SOBC to ensure compliance with the organizations' security, data protection and privacy policies. Approved list can be accessed here.

Accountability: Users must take responsibility for the information generated by the AI tool. This includes ensuring the material is factual, free of bias, legal, ethical, and compliant with the tools' terms of use.

Transparency: Identify content that has been generated by AI tools and ensure they are not subject to copyright laws. Use generative AI as an additional resource to generate ideas not to create final content.

Cybersecurity: Users must be vigilant in their evaluation of emails and other communications that have external links or other suspicious content. Report all communications that garner suspicion and use an abundance of caution when opening any email attachments. If a user clicks on a malicious link or opens a suspicious attachment, they must notify the SOBC Systems and Data administrator immediately.

Compliance with security policies: Employees and volunteers must apply the same best practices that are used for all SOBC personal and confidential information. This includes using strong passwords, keeping software up to date, being vigilant about cybercrime and phishing attacks, and following SOBC's data protection policy.