

Memorandum

To: All Staff
From: Megan Chorlton, *CEO*
Maryam Sherkat, *General Counsel & CRO*
Claudia Chan, *Manager of Digital Strategy*
ChatGPT
Date: April 2023
Re: AIP Use Policy

I. Purpose

Many staff are familiar with or are using artificial intelligence programs ("AIPs") that can generate human-like responses to text-based questions. This policy establishes the guidelines for the appropriate and responsible use of AIPs by employees of the MIABC. The policy is intended to remain in place while we explore and experiment with potential business uses for AIPs at the MIABC. This policy sets out the acceptable uses - and mandatory requirements for use - of AIPs, which must be read in conjunction with the MIABC's IT, Internet, Email, & Social Media Policy, as contained in the Employee Handbook and available on the intranet (the "MIABC IT Policy").

As with any technology, AIPs can help expedite certain elements of our work at the MIABC; however, such tools cannot be relied upon without careful oversight and review. Staff are encouraged to explore and experiment with AIPs as agreed upon with their direct supervisors to understand how these tools might assist them. Employees are not permitted to use their MIABC email to sign up for or authenticate AIP accounts - all accounts must be created using a personal email and although existing personal emails may be used, employees are encouraged to create a new Gmail or other personal account for the purposes of adhering to this policy. Employees are permitted to use either paid or unpaid versions of AIPs but will not be reimbursed by the MIABC for paid subscriptions to an AIP unless approved by their supervisor.

II. Acceptable Use

Employees are permitted to use AIPs for work-related purposes, including but not limited to:

- Manually transferring information generated by AIPs (i.e. by copying and pasting information from AIPs into a Microsoft Word document or email) *without* enabling direct integration of the AIP into work applications, such as Microsoft Word.
- Providing support to members by answering their questions and providing information.
- Researching and analyzing data to help make better decisions.
- Creating and reviewing content such as articles, reports, and documents.
- Improving internal processes and workflows.
- Other legitimate business purposes as approved by each department head / your respective supervisor.

III. Mandatory Requirements

The following requirements must be met for those using AIPs for work related activities, subject to all relevant sections of the MIABC's IT Policy:

1. Using AIP for only work-related purposes or activities during an employee's regular business / working hours.
2. Carefully reviewing and amending, as necessary, all content– and in particular, images - obtained from AIPs. Using verbatim text from AIPs and images obtained from AIPs can lead to allegations of plagiarism and copyright infringement since AIPs generate text from training data that may be virtually identical to articles and images found on the internet.
3. Providing proper citations and references in any published article that used AIPs with, at a minimum, a notation that the article was prepared with the assistance of the AIP.
4. Abstaining from inputting confidential business information – including member local government names - or personally identifiable information on individuals (i.e. personal email, telephone number, home address, medical information etc.) into the AIP.

IV. Sample Responsible Uses

AIPs are best used to aid in a task rather than doing the task entirely; it is a creative collaborator - think starting point rather than final product. The following are examples of responsible uses:

- Ask the AIP for the top 10 things that are relevant to a topic you are researching or writing an article about to get some quick inspiration (then ask it for another five).
- Prepare a skeleton outline for a communication or generate a list of items to consider addressing.
- Obtain sample agreement clauses or pleadings to give you ideas on what you might include in a clause, without including any confidential information in the prompt and without directly using the content that is generated.
- Generate ideas on seminar topics.
- Generate purely administrative internal information (such as a list of ideas or agendas), as long as no confidential or personal information is input in the prompt.

V. Security

Employees are responsible for safeguarding the confidentiality, integrity, and availability of AIPs they use and the data processed by such AIPs. The following security measures must be implemented:

- Use of strong passwords as outlined in the "Security" section of the MIABC's IT Policy.
- Changing of passwords at least every three (3) months.
- Use of multi-factor authentication (MFA) if available.
- No sharing of access credentials.
- Protecting any AIP and the data processed by the AIP from unauthorized access, theft, loss, or damage.
- Reporting any security incidents or concerns to the CRO as soon as they are detected or suspected.

VI. Monitoring

The MIABC reserves the right to monitor the use of AIPs to ensure compliance with this policy and to protect the MIABC's data, reputation, and legal obligations. All activities conducted using AIPs may be logged and audited.

VII. Consequences of Violation

Violation of this policy carries with it the same disciplinary actions outlined for breach of the MIABC IT Policy.

VIII. Conclusion

This policy outlines the appropriate use of AIPs by employees of the MIABC. By using AIPs at work / for work related purposes, you are bound by this policy. By adhering to these guidelines, we can ensure AIPs are used responsibly and ethically to benefit the organization and its members.