**Generative AI in the Workplace**

**Employer Considerations when creating a AI Usage Policy**

By creating a comprehensive policy around the use of AI in the workplace, Employers can help to ensure that the technology is used effectively and ethically and that employees are trained on how to use it safely and responsibly. The policy should be formulated with guidance and governance in mind. Already we have seen some of the risks and opportunities that Generative AI can bring however it is not without it’s limitations;

* The difficulty with generating an AI policy for a business is that it’s impossible to define policy without knowing for what purpose AI will be used.
* It is advisable that any business in a regulated space - tax, accounting, law/HR, transport, pharma, food, etc to be extremely cautious about use of AI tools, and not to presume that any output is compliant.
* Involve all necessary stakeholders in the process. They may include end users, community members, partners, funders, policy makers, regulators, researchers, and others. You need to identify who they are, what their needs and expectations are, how they will interact with your AI solution, and how they will benefit or may be harmed by it.
* AI is only as good as the data it is set
* The output is only as good as input.

**How are businesses using ChatGPT?**

Examples include:

* Writing templates for online content.
* Customer service correspondence (Chat Bots)
* Writing code.
* Writing sales pitches.
* Summarising long reports.
* Analyse business trends.

Supporters of the system maintain that it doesn’t signal a replacement of traditional workers, but it does give traditional workers a time-saving tool, the likes of which they have never seen before. In other words, it’s opening new doors.

**Food for thought**

* Set guidance based principles. Most if not all employees will be using these tools in the next few years so forbidding is not an option.
* Data Security needs to be at the forefront of all guidelines
* Be mindful of bias
* Experiment with the tools – knowledge is key and again it may be a workplace opportunity.
* Think Strategically – can value be added in your company using this tool?

**Why the need for a policy for ChatGPT?**

Because as good as ChatGPT looks on first viewing, the system also has its share of limitations that could cause problems if left unchecked. Much of these limitations stem from the information bank available to it.

* That bank does not keep up with any news cycle. The most recent information could be months, if not years, old. This means any ChatGPT-produced content could ignore the most recent relevant events.
* The information bank can include biased sources. ChatGPT could misinterpret these as hard facts and present them as such.
* The bank *may*contain sensitive data, which ChatGPT could deem fair game for widespread publishing. If organisations use ChatGPT for published content, they become liable.

In addition, the system (like any other technology) can make simple errors that might be challenging to spot.

Limitations are just one factor in why companies should create a policy for Chat GPT. The other is the pace of its popularity. Many will undoubtedly feel they need help to keep up and make sound decisions about its use. Policies help correct this imbalance.

**What should a ChatGPT or AI usage policy contain?**

Here are some areas that Employers should consider when creating an AI policy for their workplace:

1. **Data privacy and security:** A policy should be put in place that outlines how the company will collect, store, and protect the data used by AI systems. This includes ensuring that only authorised personnel access data and that it is stored securely.
2. **Bias and discrimination:** AI systems can reflect and amplify human biases and prejudices. The policy should address how the company will ensure that AI systems do not discriminate against individuals or groups based on protected characteristics such as race, gender, or age.
3. **Transparency and fact checking**: The policy should require that AI systems used in the workplace are transparent and explainable. This means that employees should be able to understand how AI decisions are made and why specific outcomes are generated.
4. **Employee training:** The policy should require that all employees who work with AI systems are trained on how to use them effectively and ethically. This includes understanding the limitations of the technology and the potential impact on their work.
5. **Accountability and responsibility:** The policy should clearly define who is responsible for AI systems’ decisions in the workplace. This includes holding individuals and departments accountable for the outcomes generated by AI systems.
6. **Ethical considerations:** The policy should address ethical concerns surrounding the use of AI in the workplace, such as the potential impact on employment and the ethical use of AI in decision-making.
7. **Continuous monitoring and improvement:** The policy should require ongoing monitoring and modification of AI systems used in the workplace to ensure that they are functioning as intended and are not causing unintended consequences.

**SAMPLE POLICY: WHEN GENERATIVE AI IS MOSTLY FORBIDDEN**

Employees are not allowed to use ChatGPT and other third-party generative AI services to conduct business. This includes using such services to generate computer code or any kind of customer communication, even as a starting point. You are also prohibited from using the services to generate internal communications, policies or documentation, or any other materials that are intended to be used in connection with the running of businesses.

You *are* allowed to use such services for the purpose of educating yourself about how these services work, subject to the limitations stated below. As of today, all teams are approved to use the ChatGPT or any other AI Generative tools for experimental and testing purposes only, provided that you do not use any company or third-party or confidential information, any personal information, or any customer or third-party data as an input.

**SAMPLE POLICY TEMPLATE: SETTING GUIDELINES**

**AI tool usage policy**

This AI tool usage policy template can help you draft an AI tool usage policy to ensure responsible and secure use of artificial intelligence (AI) tools in your organization. Modify it based on your needs.

**Policy brief & purpose**

Our company AI tool usage policy outlines best practices for use of artificial intelligence tools in the workplace, especially as it pertains to using sensitive data and proprietary company and customer information in these tools. We’ll explain how and how not to use AI tools especially as they become more prevalent in day-to-day work.

**Scope**

Artificial Intelligence (AI) tools are transforming the way we work. They have the potential to automate tasks, improve decision-making, and provide valuable insights into our operations.

However, the use of AI tools also presents new challenges in terms of information security and data protection. This policy is a guide for employees on how to be safe and secure when using AI tools, especially when it involves the sharing of potentially sensitive company and customer information.

**Purpose**

The purpose of this policy is to ensure that all employees use AI tools in a secure, responsible and confidential manner. The policy outlines the requirements that employees must follow when using AI tools, including the evaluation of security risks and the protection of confidential data.

**Policy statement**

Our organization recognizes that the use of AI tools can pose risks to our operations and customers. Therefore, we are committed to protecting the confidentiality, integrity, and availability of all company and customer data. This policy requires all employees to use AI tools in a manner consistent with our security best practices.

**Security best practices**

All employees are expected to adhere to the following security best practices when using AI tools:

a. Evaluation of AI tools: Employees must evaluate the security of any AI tool before using it. This includes reviewing the tool’s security features, terms of service, and privacy policy. Employees must also check the reputation of the tool developer and any third-party services used by the tool.

b. Protection of confidential data: Employees must not upload or share any data that is confidential, proprietary, or protected by regulation without prior approval from the appropriate department. This includes data related to customers, employees, or partners.

c. Access control: Employees must not give access to AI tools outside the company without prior approval from the appropriate department or manager and subsequent processes as required to meet security compliance requirements. This includes sharing login credentials or other sensitive information with third parties.

d. Use of reputable AI tools: Employees should use only reputable AI tools and be cautious when using tools developed by individuals or companies without established reputations. Any AI tool used by employees must meet our security and data protection standards.

e. Compliance with security policies: Employees must apply the same security best practices we use for all company and customer data. This includes using strong passwords, keeping software up-to-date, and following our data retention and disposal policies.

f. Data privacy: Employees must exercise discretion when sharing information publicly. As a first step, employees must ask themselves the question, “Would I be comfortable sharing this information outside of the company? Would we be okay with this information being leaked publicly?” before uploading or sharing any data into AI tools. Second would be to follow b) above.

**Review and revision**

This policy will be reviewed and updated on a regular basis to ensure that it remains current and effective. Any revisions to the policy will be communicated to all employees.

**Conclusion**

Our organization is committed to ensuring that the use of AI tools is safe and secure for all employees and customers, 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.

**Acknowledgement and compliance**

All employees must read and sign this policy before using any AI tools in the organization. Failure to comply with this policy may result in disciplinary action, up to and including termination.

By signing this policy, I acknowledge that I have read and understand the requirements outlined in this policy. I agree to use AI tools in a manner consistent with the security best practices outlined above and to report any security incidents or concerns to the appropriate department or manager.

Employee Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_