**[Company Name]**

**Generative AI Company Use Policy[[1]](#footnote-0)**

### Definitions

| **Term** | **Definition** |
| --- | --- |
| GenAI Systems/ Tools/Generators, GenAI | any sophisticated artificial intelligence models that can understand and generate human-like text by leveraging vast amounts of training data and deep learning techniques. They excel in tasks such as natural language processing, content generation, and question answering, but their understanding is based on statistical patterns rather than true comprehension. |
| API | means Application Programming Interface. |
| BYOD | means Bring Your Own Device. |
| CISO | means Chief Information Security Officer. |
| Company Data | should be interpreted broadly for purposes of this Policy, and includes, but is not limited to, at least the following: all Company business information and all Personal Data (whether of employees, executives, contractors, consultants, Customers, consumers, users, or other persons) that is accessed, collected, used, processed, stored, shared, distributed, transferred, disclosed, destroyed, or disposed of by any of the Company systems; all proprietary information and intellectual property (including, but not limited to, source code, designs, schematics, product roadmaps, product plans, product specifications, market analyses, white papers, strategy documents, financial information, internal communications, Customer lists, Customer files, Customer contact information, Customer contracts, Customer’s proprietary data, and any non-public Company information. Company Data includes information in written, electronic, audio, video, or any other form or medium. Company Data can include any level of information covered by the Company’s policies. |
| Customer Data | any and all data that the third parties who contract as Customers with the Company provide to the Company to use, store, transmit, or process. |
| Customer(s) | any unique contracting entity listed within an active order form with the Company, including all individuals acting on the entity’s behalf. |
| DPO | means Data Protection Officer. |
| GDPR | Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). |
| IP (Intellectual Property) | any asset that is or may in future become the subject of intellectual property rights under the laws of any jurisdiction, including computer code and its protected elements, texts, graphics, logos, drawings, button icons, images, audio, video, audio-visual works, photographic works, fonts, musical works and sounds, data compilations (databases), any other works, performances, phonograms, videograms, inventions, utility models, industrial designs, designs, improvements, developments, scientific discoveries, trademarks, innovations, know-how and trade secrets and any other objects protected by the IP Rights. |
| IP Rights (Intellectual Property rights) | any and all patent rights, rights to inventions, trademark, trade names and domain names rights, know-how and trade secret rights, rights in get-up, rights in goodwill or to sue for passing off, rights in designs, copyright and related rights and any other intellectual property rights, including any moral rights and proprietary rights, rights of publicity or privacy and all similar or equivalent rights or forms of protection, in each case, whether registered or unregistered, granted, applied for or otherwise existing now or in the future under the laws of any jurisdiction (including all applications (or rights to apply) for, and renewals or extensions of, such rights and forms of protection). |
| Personal Data | within the meaning given in GDPR, any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. PII (Personally Identifiable Information) in the understanding of the U.S. laws is also encompassed by the term “Personal Data” used in the Policy. |
| SSO | means Single Sign-On. |
| Team Member(s) | all employees permanent, contract and temporary and those under a contract for services with the Company or an affiliate of the Company as an outsourced services supplier. |

## Introduction

## About GenAI

Generative AI (the “**GenAI**”) is a form of artificial intelligence that creates new content like text, images, or music by learning from existing data. Models like ChatGPT and Google’s Bard exemplify GenAI.

## Our Approach to GenAI

At [Company Name] (the “**Company**”), we value responsible and ethical use of GenAI as an assistant, not a replacement. We address legal and ethical concerns and establish decision-making principles for its workplace use.

This Generative AI Company Use Policy (the “**Policy**”) provides guidance and rules for responsible GenAI use by Team Members, aiming to leverage technology for good without causing harm.

## Purpose

As GenAI tools like ChatGPT and Google’s Bard gain popularity, it is essential to outline their proper use at the Company. We adopt new technologies while ensuring responsible application and risk awareness.

The Policy establishes ethical guidelines and best practices for GenAI use within the Company. It complies with laws and regulations and safeguards Team Members, suppliers, Customers, and the Company.

## Eligibility

This Policy applies to all Team Members using or interacting with GenAI, including language models, plugins, and data-enabled tools. It covers on/off-premises work using BYOD devices for work activities.

## Principles for GenAI Use

## Responsible Use

Team Members must employ GenAI responsibly, avoiding harm, privacy violations, and malicious activities. It should promote fairness, avoid bias and discrimination, and align with the Company’s values. GenAI can be used for work-related tasks like generating content for reports, emails, presentations, images, and Customer service, subject to Policy adherence.

## Ethical Use

GenAI must be used ethically, complying with laws and organisational policies. Team Members should not create discriminatory, offensive, or inappropriate content. If there are any uncertainties about the appropriateness of using GenAI in a particular situation, Team Members should consult with their supervisor or Information Governance Team.

## Compliance with Laws and Regulations

GenAI must comply with all applicable laws, including data protection, privacy, and IP laws.

## Transparency and Accountability

Team Members must be transparent about GenAI use in their work and utilise the Company’s system for governance and compliance. Team Members are accountable for outcomes generated by GenAI and should be prepared to explain and justify those outcomes.

## Data Privacy and Security

Adhere to the Company’s data privacy and security policies when using GenAI. Anonymise and securely store any Personal Data or sensitive data used.

## Bias and Fairness

Mitigate biases in GenAI to ensure fairness and inclusivity, avoiding discrimination.

## Human-GenAI Collaboration

Use judgement when interpreting and acting on GenAI-generated recommendations. GenAI is a tool to augment human decision-making, not replace it.

## Training and Education

Team Members must receive appropriate training for responsible GenAI use and stay informed about advancements and ethical concerns.

All managers will be trained on the proper use of GenAI in the workplace.

[*Optional: All Team Members using GenAI for work must attend training before doing so*.]

For inquiries, contact [*enter department and/or name and contact information*].

## Third-Party Services

When utilising third-party GenAI services or platforms, Team Members must ensure providers adhere to the same ethical standards and legal requirements outlined in this Policy.

## Governance

Before accessing GenAI technology, Team Members must notify the Information Governance Team of their intent, reasons, input information, generated output, and content distribution.

## Vendors

Any use of GenAI technology for work activities should acknowledge the policies, practices, terms, and conditions of developers/vendors.

## Copyright

Team Members must adhere to copyright laws when using GenAI. Using GenAI to generate content that infringes on others’ IP rights, including copyrighted material, is prohibited. If unsure, contact the legal advisor or Information Governance Team.

## Accuracy

All GenAI-generated information must be reviewed and edited for accuracy before use. Team Members are responsible for reviewing and ensuring accuracy. If in doubt, refrain from using GenAI.

## Confidentiality

Confidential information and Personal Data must not be entered into a GenAI Tool to avoid potential exposure. Follow data privacy laws and organisational policies. If uncertain, avoid using GenAI.

## Disclosure

Content produced via GenAI must be identified and disclosed as GenAI-generated.

Example footnote:

***Note:*** *This document contains content generated by Generative Artificial Intelligence (GenAI).* Gen*AI-generated content has been reviewed and edited by the author for accuracy. The author takes responsibility for this content.*

## Guidelines for GenAI Use

## Required Actions:

1. before using any GenAI Tool for any Company business, opt out of allowing GenAI Tools to use data for training their models;
2. consult the Company’s policies to classify data intended for GenAI use and ensure it is not too sensitive to share;
3. carefully review GenAI-generated material for accuracy, completeness, and protection of third-party rights and Company Data.

## Approved GenAI for Corporate Use:

1. access the list of approved GenAI for Company use at: [link to approved GenAI for corporate use];
2. the use of GenAI not included in the approved GenAI list is **strictly** **prohibited**;
3. submit a request to IT Procurement for using new GenAI not allowed by the Company, following provided instructions;
4. the Company shall evaluate the security of any GenAI Tool before allowing the use of it, including security features, terms of service, and privacy policy. Check the reputation of the GenAI Tool developer and any third-party services used by it and report concerns to the IT Procurement team.

## How You May Use GenAI:

1. comply with this Policy, other internal policies, rules, and confidentiality obligations in employment documentation;
2. use legally obtained data with GenAI Tools and obtain necessary permissions;
3. use only non-confidential, non-highly confidential, or non-restricted data, as per Company policies;
4. use vendor integrations or products featuring GenAI approved by the Legal and Security teams;
5. report security incidents or suspected breaches to [insert email address].

## Rules for Acceptable Use Must Be Followed:

1. sign up for GenAI System using a corporate account and the Company’s corporate SSO (if available);
2. use GenAI solely for work-related purposes aligned with respective tasks;
3. consider GenAI outputs as preliminary and verify for accuracy and potential bias before publication or decision-making;
4. exercise caution as anything entered into a GenAI Generator may become publicly accessible;
5. use only drafts of source code during interaction with GenAI (applicable for ChatGPT);
6. review and edit any public-facing creatives generated by GenAI prior to publication to protect copyright;
7. use only drafts of documents without identifying Company Group information during interaction with GenAI;
8. disable chat history and training in GenAI System (applicable for ChatGPT);
9. obtain approval from the manager and Security Team before training GenAI on Team Member data;
10. report any potential data breaches, unauthorised access, or suspicious activities to the Security Team at [insert email address];
11. apply standard security practices for all Company and Customer Data, including strong passwords, up-to-date software, and data retention and disposal procedures.

## Prohibited GenAI Use:

1. do not use personal accounts with GenAI Tools for Company-related purposes;
2. do not use Customer Data with GenAI Tools;
3. do not use any Company Data classified as confidential, highly confidential, or restricted (as defined in our policies);
4. do not use GenAI Tools for Company-related purposes without opting out of letting them use data you feed to train their models.

## Restrictions on GenAI Tools Usage

At all times, each Team Member must:

1. avoid sharing non-public information with GenAI, including confidential and sensitive corporate information, Personal Data, Company IP, and regulatory protected information;
2. consider the sensitivity of information before uploading it to GenAI Tools and consult managers if unsure;
3. ensure compliance with GDPR and other data protection laws by refraining from entering Personal Data or protected/confidential information into GenAI Tools or search engines powered by GenAI;
4. avoid using ‘Browse with Bing’ and third-party plugins for GenAI Tools;
5. refrain from using GenAI Tools for unethical, illegal, or malicious activities that may harm the Company, its Group, Customers, Team Members, or third parties;
6. avoid installing unauthorised third-party GenAI-based browser plugins for video call voice transcripts, even with ChatGPT;
7. not use unauthorised Slack bots with GenAI features;
8. not use code that has already been committed to corporate repositories (GitLab, GitHub) for interaction with GenAI (applicable for ChatGPT);
9. not share access to GenAI Tools.

The Company reserves the right to monitor and audit GenAI Tool usage by Team Members to ensure strict compliance with this Policy and investigate concerns regarding inappropriate use. This includes verifying the use of approved GenAI Tools, their correct usage, and proper data access and storage.

## Enforcement

The [CISO, DPO] and Security Team will ensure compliance with this Policy through various methods, including business tool reports and internal/external audits. Any exceptions must be pre-approved by the [CISO, DPO] and General Counsel, or their designees. Violation of this Policy may result in disciplinary action, up to termination of employment or legal action if warranted.

## Implementation and Monitoring

## GenAI Governance Board

A multidisciplinary GenAI risk management team (the “**GenAI Governance Board**”), comprising data scientists, legal and compliance professionals, and ethics specialists, will oversee responsible GenAI development and deployment. They will define roles for designated committees critical to GenAI oversight.

## Designated GenAI Officer

A designated GenAI Officer will oversee Policy implementation, guide Team Members, and ensure compliance with laws. The Officer will periodically review GenAI use, identify risks, and recommend Policy updates.

## Incident Reporting

Team Members must report suspected violations of this Policy or ethical, legal, or regulatory concerns to the GenAI Officer or established reporting channels.

## Monitoring

The Company’s existing monitoring and internal policies apply when using GenAI with Company equipment.

## Document Control

## Document Owner

[CISO, DPO]

## Revision History

| **Effective date** | **Version** | **Contributors** | **Notes** |
| --- | --- | --- | --- |
| [Date] | 1.0 | CISO, DPO, Info Sec, Legal, IT | Created |

## Policy Review

This Policy will undergo periodic review and updates as needed to remain compliant with evolving AI technology and regulations. Team Members will be informed of any changes to the Policy.

## Acknowledgement and Compliance

All Team Members must read and sign this Policy before using any GenAI Tools at the Company. Non-compliance may result in disciplinary action, including termination.

By signing this Policy, I acknowledge that I have read and understood the requirements. I agree to use GenAI Tools following the security best practices and report any incidents or concerns to the appropriate department or manager.

| Team Member’s name: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| --- | --- |
| Signature: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Date: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

1. This document is a draft and provided to you for information purposes only. **It is not legal advice.** Before using it, make sure it is in line with the applicable law. Please consult a lawyer before using it.

   © 2023 Legal Nodes LTD. You are allowed to modify and use this template for your company and for information and education purposes. The use for any other purpose and/or distribution of this or a modified version of this document is only allowed with our prior written consent. [↑](#footnote-ref-0)