Using AILMs at LTG

Version Number	1.2
Last Approved	Aug 8, 2023
Classification	PUBLIC

Learning Technologies Group plc – Proprietary and Confidential – This document contains confidential information, which is the property of Learning Technologies Group plc, and may not be distributed externally without explicit written permission.

Overview

Purpose

The purpose of this document is to provide guidelines for using **Artificial Intelligence Language Models (AILMs)** such as ChatGPT, Bard, Llama and similar tools. These guidelines are intended to allow for use of AILMs in a responsible and ethical manner. The guidelines will also ensure we meet our contractual obligations with our customers regarding the use of their data.

Scope

These guidelines apply to all LTG employees, contractors, products and processes with access to LTG Software or LTG customer data.

Guidelines

1. **Access**: Access to AILMs, leveraging sensitive or customer data. will be limited to authorized employees who have requested and received approval for specific use cases. Access to AILMs will be granted only for legitimate business purposes and will be subject to review and audit.
2. **Confidentiality**: Unless an AILM has been explicitly authorized for confidential use, only data that is publicly accessible or considered public should be used with AILMs. i.e. ***Treat sharing data with an AILM as if you are posting it publicly on the internet.***
3. **Data Privacy**: AILMs process large amounts of data to generate responses. To ensure the privacy of our customers and employees, we will use anonymized and aggregated data wherever possible. Any data used to train ChatGPT will be de-identified and anonymized.
4. **Accuracy and Transparency (Labeling)**: AILMs are designed to provide accurate and helpful responses. However, it is important to note that AILMs are not perfect, and their responses may sometimes be incorrect or incomplete. To ensure transparency, we will clearly communicate to our customers when they are interacting with AILMs and provide them with an option to speak with a human representative if needed.
5. **Security**: AILMs that process sensitive data must be protected from unauthorized access and misuse. We will implement appropriate security measures, including access controls, encryption, and regular security assessments, to ensure the confidentiality, integrity, and availability of an AILM in use.
6. **Compliance**: The use of AILMs must comply with all applicable laws, regulations, and company policies. We will ensure that AILM use does not violate any intellectual property rights, copyright laws, or any other legal requirements.
7. **Monitoring and Review**: We will monitor the use of AILMs and periodically review this policy to ensure that it is up-to-date and relevant. Any violations of this policy will be investigated, and appropriate corrective actions will be taken.

Additional Information

Additional information related to *Disciplinary Actions*, *Exceptions* and *Questions* can be found in the Security Documentation Overview .

Document control

This policy is only controlled in its live, digital format. Any other format or export of this policy is an uncontrolled version of this document

Document Owner	Managing Director - PeopleFluent	
Author(s)	@TJ Seabrooks @Tim Edwards (Deactivated) @Peter Brussard	
Required Approver(s) and Approval Date	@TJ Seabrooks Managing Director - PeopleFluent	Aug 8, 2023
	@Art Machado VP Information Security	Aug 8, 2023
Review cycle	ANNUAL	
Next review date	Aug 8, 2024	

Version History

Date	**Author(s)**	**Version**	**Changes**
Dec 10, 2024	@angelina.kilmer	1.2	Updated Policy classification from Confidential to Public
Jan 12, 2024	@Sarah Zwicker (Unlicensed)	1.1	Moved Confluence Spaces to GPR
Aug 8, 2023	@TJ Seabrooks @Tim Edwards (Deactivated) @Peter Brussard	1.0	Original version