RGIS

AI POLICY

RGIS

2025

RGIS_MC_0072_01

TABLE OF CONTENTS

Dear Colleagues,

As we embrace the transformative power of Artificial Intelligence (AI) at RGIS, our success depends on using this technology ethically, responsibly, and collaboratively. AI should enhance our operations while aligning with our core values:

INTEGRITY

We use AI ethically and transparently, ensuring fairness, accountability, and compliance with all regulations.

EXCELLENCE

We strive for innovation while maintaining accuracy, reliability, and quality in all AI-driven solutions.

RESPECT

We prioritize human dignity, data privacy, and inclusivity in AI applications, ensuring fairness for our employees, customers, and stakeholders.

TEAMWORK

We integrate AI as a tool to support and empower our teams, fostering collaboration rather than replacing human expertise.

INNOVATION

We embrace AI to improve efficiency, decision-making, and customer service, while continuously assessing its impact and effectiveness.

These principles form the foundation of our AI Policy, guiding how we develop, implement, and use AI across RGIS. Every team member is responsible for ensuring AI aligns with our ethical standards and business goals.

If you have any questions or concerns about AI use within RGIS, please contact the Legal Department (legaleurope@rgis.com). Thank you for upholding our values and ensuring AI is used responsibly.

Sincerely,

Asaf Cohen
Chief Executive Officer

RGIS INTEGRITY EXCELLENCE RESPECT TEAMWORK INNOVATION

RGIS

AI Policy

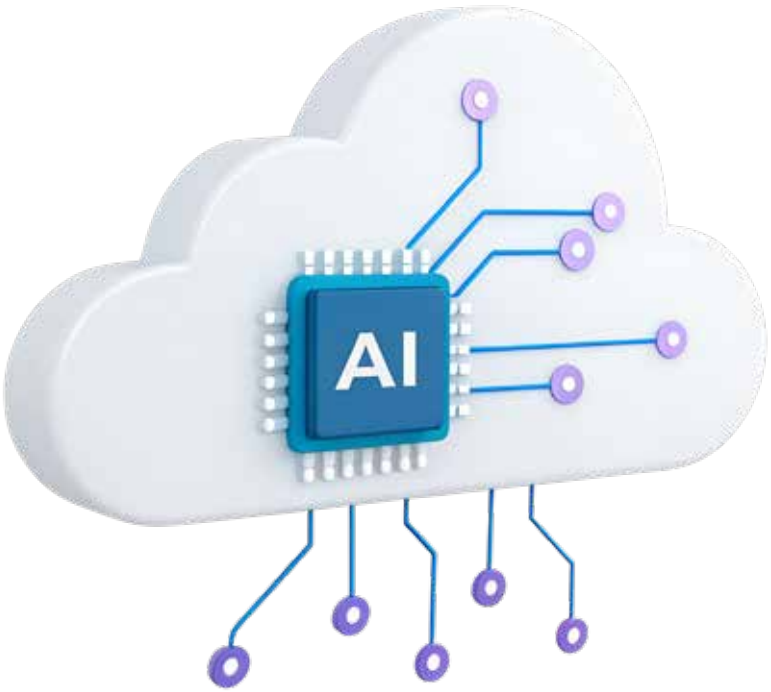
AI IN OUR WORKPLACE: WHY AN AI POLICY?

As AI continues to evolve, its potential to enhance productivity, streamline operations, and drive innovation is undeniable. However, with great potential comes inherent risks – ranging from data security and compliance concerns to ethical considerations and accuracy challenges. Our AI Policy is designed to strike the right balance between opportunity and risk, ensuring that AI is integrated securely, strategically, and in alignment with our business objectives.

Under the AI Director's leadership, AI integrations within our processes will be carefully assessed and implemented where they provide the greatest value, ensuring that AI supports – not replaces – human expertise. This policy serves as a framework to guide responsible AI use, ensuring clarity, security, and compliance across all departments.

Recent assessments highlight varying levels of AI adoption across our organization. While some teams have embraced AI for automation, analysis, and content generation, others remain hesitant due to concerns over security, compliance, and accuracy. Our approach acknowledges these concerns, prioritizing education, governance, and secure implementation to build confidence in AI's role within our business.

Through this policy, we emphasize that AI is not just a tool—it is a responsibility. Employees must use AI ethically, avoiding the sharing of confidential data, ensuring accuracy in outputs, and maintaining human oversight in decision-making. By following these guidelines, we can harness AI's full potential while safeguarding our operations, our people, and our future.



RGIS

AI Policy

1. INTRODUCTION

This policy establishes the guidelines and standards for the responsible use of Artificial Intelligence (AI) technologies, including Generative Artificial Intelligence (GenAI), within RGIS. AI tools are technologies designed to perform tasks that typically require human intelligence, while GenAI tools specifically generate new, previously undefined content based on user inputs or prompts. Examples of GenAI tools include ChatGPT, Gemini, Microsoft Co-Pilot, and other similar platforms. AI and GenAI technologies offer transformative potential across RGIS, enabling us to streamline operations, enhance productivity, and drive creativity in areas such as data analysis, content creation, and process automation.

2. PURPOSE

Whilst offering incredible potential, AI also introduces significant risks, including those related to data security, confidentiality, accuracy, intellectual property compliance, and ethical use. Finding the right balance between leveraging AI's transformative potential and mitigating its inherent risks is essential to ensuring responsible and effective implementation.

It requires a proactive approach, where innovation is encouraged while maintaining rigorous safeguards to protect data, ensure compliance, and uphold ethical standards. This policy outlines guidelines for the internal use, development, and deployment of Artificial Intelligence (AI) systems within RGIS.

The goal is to ensure that our AI use:

a. aligns with ethical standards;
b. respects data privacy in safeguarding RGIS's sensitive and confidential information,
c. customer data
d. adheres to regulatory frameworks AI introduces significant risks, including those related to data security, confidentiality, accuracy, intellectual property compliance, and ethical use.

The goal is to ensure that our AI use aligns with ethical standards, respects data privacy in safeguarding RGIS's sensitive and confidential information, and adheres to regulatory frameworks, including the EU AI Act.

3. SCOPE

This policy applies to all employees, including temporary staff and interns, contractors, affiliates, and third parties who work with or interact with AI tools and systems provided or approved by RGIS and accessing RGIS data. It covers AI applications, data handling, and compliance requirements associated with AI systems used within the organization.

4. DEFINITIONS

AI Tools: Any software, application, or hardware that utilizes artificial intelligence techniques (including machine learning, natural language processing, image recognition, and generative capabilities).

AI Governance Team: A group within an organization responsible for overseeing and managing the development, deployment, and ethical use of artificial intelligence (AI) technologies.

Confidential Information: Confidential Information refers to data that is proprietary or private to RGIS, including trade secrets, business strategies, financial information, and any other information that is not publicly available. All sensitive or non-public information, including but not limited to RGIS's proprietary RM technology, inventory management systems, RFID solutions, wireless technology implementations, client inventory data (including healthcare facility audit data), internal communications, and operational strategies.

RGIS

AI Policy

4. DEFINITIONS (continued)

Data: refers to any information collected, processed, or stored by AI systems, including user inputs, system outputs, metadata, and any structured or unstructured information used for training, inference, or decision-making.

Ethical Standards: Principles that guide the responsible use of AI, ensuring fairness, transparency, and respect for individual rights.

Generative AI: A category of artificial intelligence systems that are designed to generate new, previously undefined content based on user inputs or prompts. This content can include text, images, audio, video, or other forms of media.

Proprietary Systems: RGIS's RM technology, inventory management systems, RFID and wireless technology implementations, and associated digital infrastructure.

Sensitive Information: Sensitive Information encompasses data that requires protection due to its nature, including personal data, health records, and any information that could lead to identity theft or privacy breaches.

Unauthorized AI Systems: AI tools or platforms not explicitly reviewed and approved by the AI Governance Team.

5. ETHICS OF ARTIFICIAL INTELLIGENCE

5.1. Non-discrimination

We are committed to developing and using artificial intelligence algorithms fairly. We apply controls to detect and minimize bias in training data and AI models, ensuring no discrimination in terms of age, gender, ethnicity, creed, etc.

5.2. Transparency

Decisions automated by our algorithms are explained in an accessible way to the relevant users, to ensure that they are understood. This allows users to better understand the logic behind automated decisions, especially when results influence professional or personal aspects.

5.3. Human Control

People remain at the heart of decision-making processes in operations that incorporate AI technologies. Human recourse is always possible for any important decision involving AI, allowing users or employees to question and clarify the results produced by AI.

6. APPROVED AI TOOLS AND USAGE

Employees may use AI tools that meet one of the following criteria:

Recognized Providers: Tools originating from well-known, reputable vendors – primarily from the United States – or those with a proven track record for compliance and security.

Internally Developed Tools: AI applications developed and maintained by the RGIS IT team.

All other AI tools or applications must undergo a formal review process and receive explicit authorization from the AI Governance Team prior to use.

RGIS

AI Policy

7. PROHIBITED PHYSICAL AND SOFTWARE PRACTICES

Employees MUST NOT:

Install or Use Unauthorized AI Tools:

- Install, download, or operate any AI software or hardware on RGIS-owned devices, or on personal devices connected to RGIS networks, without prior review and explicit written approval from the AI Governance Team.
- Introduce AI tools that integrate or interface with any proprietary RGIS systems (including RM technology, inventory management systems, RFID solutions, wireless technology implementations, tablet applications, and dashboard systems) unless specifically authorized.

Circumvent Security or Approval Protocols:

- Modify, bypass, or disable any security measures or approval processes designed to control the integration or use of AI systems within RGIS.

Integrate AI Tools with Core Systems:

- Connect or integrate any AI tools with RGIS's proprietary systems – including RM technology, inventory management systems, RFID solutions, wireless technology platforms, tablet applications, and dashboards – without explicit authorization from both the AI Governance Team and IT Security.

Misuse Customer Data:

- The use of unauthorized software, hardware, or external storage devices to collect, process, or store customer data is strictly prohibited. All AI systems must adhere to company-approved security protocols to prevent data breaches and unauthorized access.

8. CROSS-BORDER DATA TRANSFERS AND REGIONAL COMPLIANCE

Given RGIS's global presence, employees must:

- Ensure that any AI tool handling data complies with the data protection laws and regulations of the relevant jurisdictions (e.g., GDPR in the EU, CCPA in California, HIPAA for healthcare data, and other national standards).
- Not transfer any confidential or sensitive data across national borders via AI systems unless such transfers have been specifically reviewed, documented, and approved by the AI Governance Team.

9. ENVIRONMENTAL AND RESPONSIBLE DIGITAL CONSEQUENCES

Reducing the digital footprint:

- RGIS incorporates responsible practices to reduce the environmental impact of its digital activities. This includes optimized server utilization, proper equipment recycling, and energy-efficient technology choices.

Responsible digital awareness:

- We promote the responsible use of digital technologies and promote environmentally friendly behavior among employees, such as limiting paper printing and optimizing the use of IT resources.

RGIS

AI Policy

10. LIABILITY, COMPLIANCE, AND MONITORING

Liability for AI-Generated Errors:

- RGIS shall not be held liable for AI-generated errors in inventory counts, audits, or operational reports if the AI tool was used without proper approval or outside the bounds of this Policy. Any such error will be subject to internal review, and disciplinary action may be taken against employees found in violation.

Monitoring and Auditing:

- RGIS reserves the right to monitor and audit the use of AI tools on all company-owned or RGIS-connected devices. Non-compliance with this Policy may result in disciplinary measures, up to and including termination of employment.

Reporting Violations:

- Employees must immediately report any suspected violations of this Policy to their supervisor, IT Security, or the AI Governance Team.

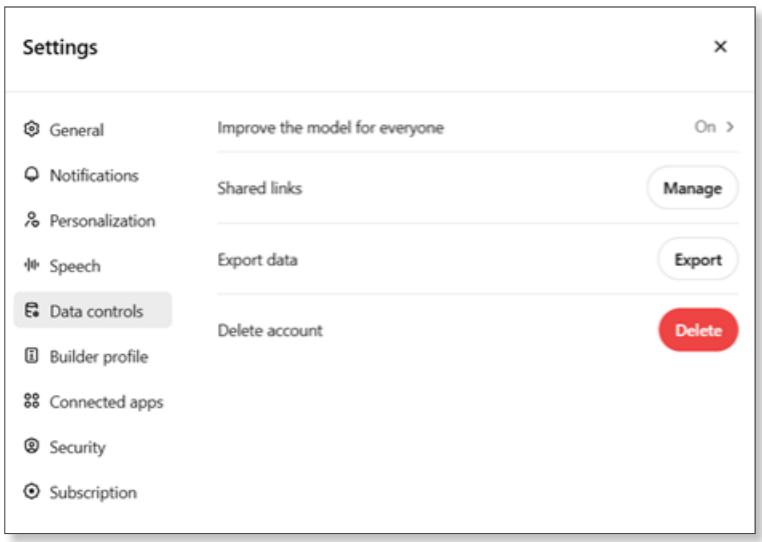
11. POLICY AMENDMENTS

RGIS reserves the right to amend or update this Policy at any time. Any changes will be communicated through official channels and will take effect immediately upon release.

RGIS AI POLICY

Appendix

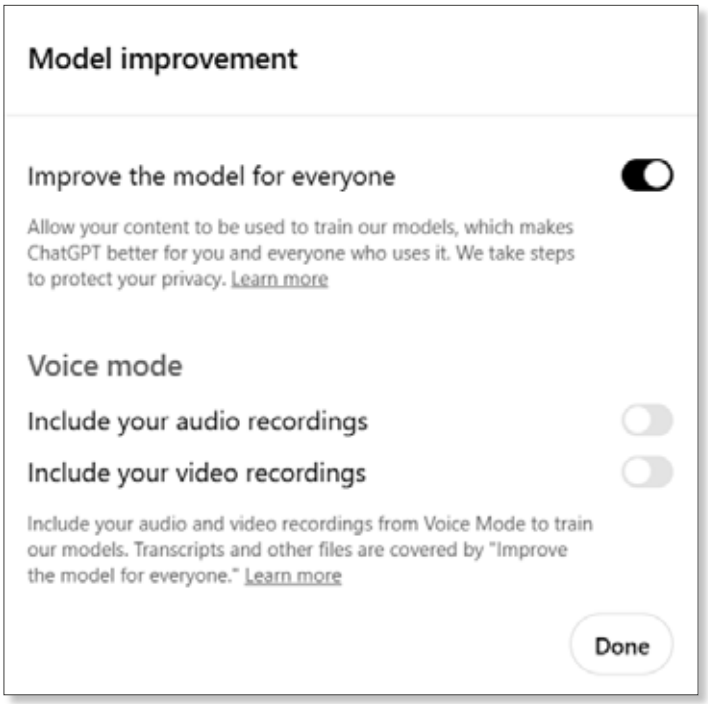
CHATGPT

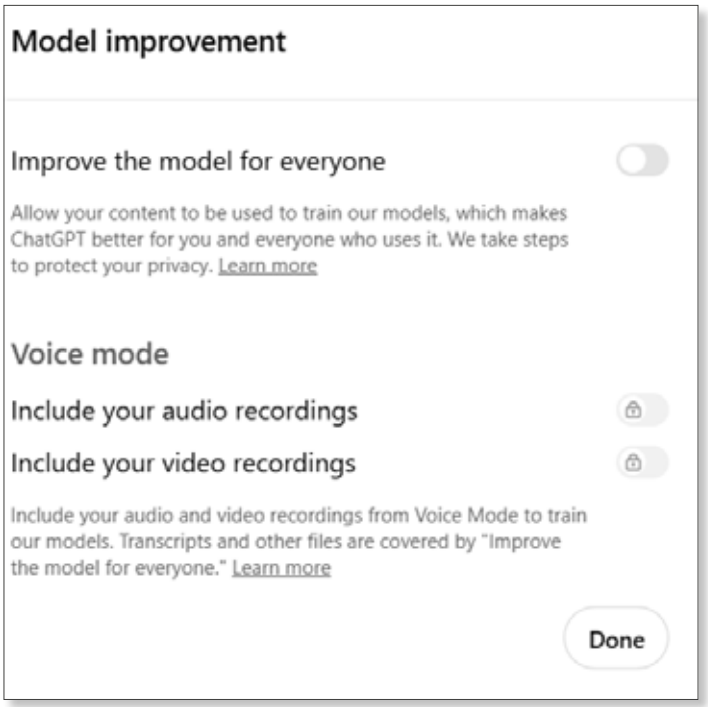


RGIS AI POLICY

Appendix

CHATGPT

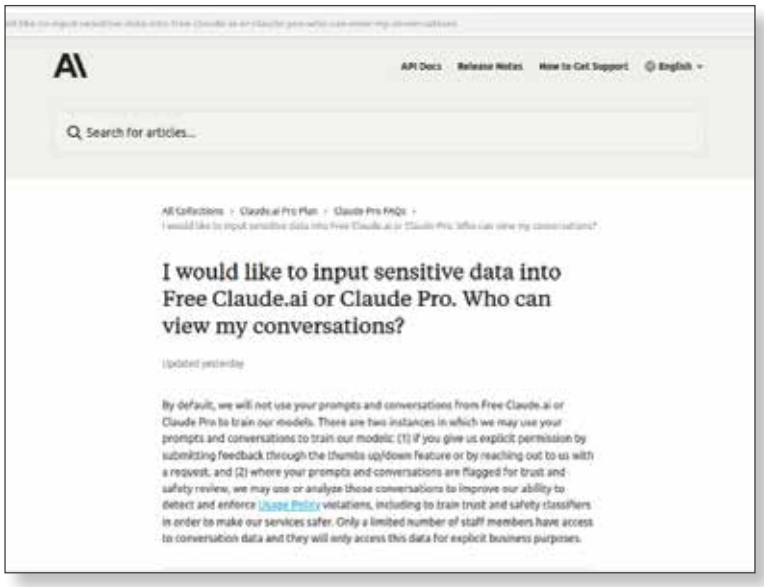




RGIS AI POLICY

Appendix

CLAUDE



I would like to input sensitive data into Free Claude.ai or Claude Pro. Who can view my conversations?

Updated yesterday

By default, we will not use your prompts and conversations from Free Claude.ai or Claude Pro to train our models. There are two instances in which we may use your prompts and conversations to train our models: (1) if you give us explicit permission by submitting feedback through the thumbs up/down feature or by reaching out to us with a request, and (2) where your prompts and conversations are flagged for trust and safety review, we may use or analyze those conversations to improve our ability to detect and enforce Usage Policy violations, including to train trust and safety classifiers in order to make our services safer. Only a limited number of staff members have access to conversation data and they will only access this data for explicit business purposes.

MICROSOFT CO-PILOT

How does Microsoft 365 Copilot use your proprietary organizational data?

Microsoft 365 Copilot provides value by connecting LLMs to your organizational data. Microsoft 365 Copilot accesses content and context through Microsoft Graph. It can generate responses anchored in your organizational data, such as user documents, emails, calendar, chats, meetings, and contacts. Microsoft 365 Copilot combines this content with the user's working context, such as the meeting a user is in now, the email exchanges the user had on a topic, or the chat conversations the user had last week. Microsoft 365 Copilot uses this combination of content and context to help provide accurate, relevant, and contextual responses.

Important

Prompts, responses, and data accessed through Microsoft Graph aren't used to train foundation LLMs, including those used by Microsoft 365 Copilot.

Microsoft 365 Copilot only surfaces organizational data to which individual users have at least view permissions. It's important that you're using the permission models available in Microsoft 365 services, such as SharePoint, to help ensure the right users or groups have the right access to the right content within your organization. This includes permissions you give to users outside your organization through inter-tenant collaboration solutions, such as shared channels in Microsoft Teams.

When you enter prompts using Microsoft 365 Copilot, the information contained within your prompts, the data they retrieve, and the generated responses remain within the Microsoft 365 service boundary, in keeping with our current privacy, security, and compliance commitments. Microsoft 365 Copilot uses Azure OpenAI services for processing, not OpenAI's publicly available services. Azure OpenAI doesn't cache customer content and Copilot modified prompts for Microsoft 365 Copilot. For more information, see the Data stored about user interactions with Microsoft 365 Copilot section later in this article.