



Employee AI Usage Policy

Artificial Intelligence (AI) Tools and Platforms

Governing the Responsible Use of AI Tools Across All Business and Academic Functions

Document Owner:	Vista Group, Group Technology and Operations
Applies To:	All Employees: Administration, Finance, Management, Operations, and Academic & Education Staff
Scope:	All Vista Group entities and business units (UAE & Africa)
Version:	1.0, March 2026
Classification:	Internal Use Only. Not for External Distribution.

1. Purpose & Scope

This policy governs the use of all Artificial Intelligence (AI) tools and platforms by Vista Group employees. It applies to tools such as Google Workspace Gemini Pro, Microsoft Copilot, ChatGPT, Claude, Perplexity, DeepSeek, Kimi (Moonshot AI), Doubao (ByteDance), and any other AI assistant or generative AI platform used for work purposes. This policy covers all business and academic functions, including Administration, Finance, Management, Operations, HR, Legal, IT, Business Development, and Academic & Education.

The intent of this policy is to empower employees to use AI tools to the maximum extent possible while establishing clear boundaries around sensitive data, with a focus on financial and banking information, to protect Vista Group, its clients, and its partners.

This policy applies to every Vista Group employee or representative who uses any AI tool for work-related tasks, whether the tool is company-provided or accessed independently.

2. What is Artificial Intelligence (AI) Tools?

Vista Group employees may be provided with, or may use, a range of AI tools to support their work. The most common platforms include Google Workspace Gemini Pro (built into Gmail, Docs, Sheets, Slides, Drive and Meet), Microsoft Copilot (built into Microsoft 365 apps), ChatGPT (OpenAI), Claude (Anthropic),

Perplexity AI, DeepSeek, Kimi (Moonshot AI), and Doubao (ByteDance). Employees may also encounter other AI tools integrated into specific software used by their department. Regardless of which platform is used, this policy and its restrictions apply in full.

Key facts that apply to all AI platforms:

- Data submitted to company-managed AI tools (such as Gemini Pro within Google Workspace or Copilot within Microsoft 365) stays within your organisation domain. Employees may also use other company-approved AI platforms such as Claude (Anthropic) or similar tools. Regardless of the platform, always follow the data restrictions in Section 4 and use only company-approved or business accounts for any AI tool used for work purposes.
- Company-managed AI platforms are configured to restrict use of your data for AI training. External AI platforms may use submitted content for model improvement unless enterprise accounts with data protection agreements are in place.
- AI tools integrated into your work platforms can only access files and data you already have permission to view. Standalone tools such as ChatGPT have no access to internal Vista Group systems unless you manually paste content into them.
- All existing Data Loss Prevention (DLP), Information Rights Management (IRM), and information security policies apply to all AI-generated content regardless of which tool produced it.
- AI sessions are private to you on company-managed platforms. On external platforms, sessions may be stored by the service provider and should be treated accordingly.

3. Permitted Uses: Maximum Access Granted

Vista Group grants employees the broadest possible permissions to use AI tools in their day-to-day work. The following categories are fully permitted across all departments, regardless of which AI platform is being used:

3.1 Administration & Office Operations

- Drafting, editing, and responding to internal and external emails in Gmail
- Summarising long email threads, documents, and meeting notes
- Creating internal reports, memos, briefing notes, and business correspondence
- Formatting and proofreading documents for professional quality
- Translating content into other languages for cross-border communications
- Building templates for recurring administrative tasks

3.2 Finance Team: Permitted Uses

Finance team members may use AI tools for the tasks listed below. Section 4 defines what financial data must NEVER be entered into any AI prompt, on any platform.

- Drafting financial commentary, summaries, and narrative sections of reports using anonymised figures
- Creating presentation slides and dashboards that display aggregated financial data

- Using AI tools to build formulas, pivot logic, and data models in spreadsheets using anonymised test data
- Drafting finance-related emails, proposals, and budget justification documents
- Researching market benchmarks, industry data, and general financial concepts
- Building financial report templates, tracker layouts, and budget frameworks

3.3 Management & Leadership

- Drafting board reports, executive summaries, business plans, and strategy documents
- Preparing presentations for internal reviews, investor briefings, and partner meetings
- Summarising research, market intelligence, and industry reports
- Creating KPI dashboards and performance reporting frameworks in Sheets and Slides
- Assisting with decision-making by generating structured analysis and options papers
- Drafting leadership communications, all-staff messages, and announcements

3.4 Human Resources

- Drafting job descriptions, offer letters, and onboarding documentation
- Writing HR policies, guidelines, and internal handbooks
- Creating training materials, learning guides, and staff development content
- Summarising performance review frameworks and goal-setting templates
- Drafting staff communications, engagement surveys, and announcements

3.5 Business Development & Marketing

- Generating proposals, pitch decks, and capability statements
- Writing marketing copy, website content, newsletters, and social media posts
- Conducting research on markets, sectors, and competitor landscape
- Brainstorming campaign ideas, product launches, and event plans
- Creating client-facing presentations and company profile documents

3.6 IT & Technical Operations

- Drafting IT policies, user guides, and technical documentation
- Assisting with troubleshooting documentation and knowledge base articles
- Creating training content for system rollouts and technology adoption
- Summarising technical specifications and vendor documentation

3.7 Academic & Education Institutions

- Drafting course outlines, programme handbooks, module guides, and academic calendars
- Creating lecture notes, lesson plans, presentation slides, and supplementary learning materials
- Writing student communications, admission letters, enrolment notifications, and event announcements
- Summarising academic research, journal articles, and institutional reports for internal use
- Designing assessment frameworks, rubrics, and grading templates (not individual student results)

- Producing marketing and recruitment content for programmes, open days, webinars, and events
- Translating institutional content and correspondence for multilingual student and partner communities
- Drafting accreditation documentation, institutional review submissions, and quality assurance reports

Vista Group policy is to provide maximum AI tool usage permissions to all employees. If you are uncertain whether a task is permitted, the answer is almost always YES, unless it falls under Section 4 below.

4. Restricted & Prohibited Uses

Certain categories of data must never be entered into any AI tool prompt, on any platform. This applies regardless of your seniority, department, or intent. These restrictions exist to protect Vista Group from financial fraud risk, regulatory breaches, and data exposure.

4.1 Data Permissions: Quick Reference

Data Type / Use Case	Status	Guidance
General business documents & drafts	ALLOWED	Fully permitted for all staff
Internal emails & communications	ALLOWED	Fully permitted for all staff
Presentations and reports (general)	ALLOWED	Fully permitted for all staff
Anonymised / aggregated financial figures	ALLOWED	No account or party identifiers
HR documents (templates, policies)	ALLOWED	Non-personal, template-based only
Individual employee salary or compensation data	RESTRICTED	HR Director authorised use only
Individual performance review records	RESTRICTED	Authorised HR/Manager use only
Client or vendor contact lists (raw data)	RESTRICTED	Use in aggregate; no full databases
Bank account numbers / IBANs / SWIFT codes	NOT ALLOWED	Strictly prohibited at all times
Raw bank statements or transaction logs	NOT ALLOWED	Strictly prohibited at all times
Payroll processing data	NOT ALLOWED	Never enter into any AI tool
Credit card or payment card details	NOT ALLOWED	PCI-DSS protected, prohibited
Passwords, API keys, or system credentials	NOT ALLOWED	Never enter credentials of any kind
Confidential investor or deal data (M&A, funding)	NOT ALLOWED	Prohibited until publicly disclosed

Legal contracts or privileged legal documents	NOT ALLOWED	Seek Group Legal approval first
Passport, visa, or national ID data	NOT ALLOWED	Personal identity data, never enter

4.2 Financial and Banking Data: Critical Restrictions

STRICTLY PROHIBITED: Under no circumstances should banking, payment, or raw financial transaction data be entered into any AI tool or platform. This applies to ALL employees including Finance, Management, and C-Suite.

The following financial data types are absolutely prohibited in prompts to any AI tool or platform:

- Bank account numbers, sort codes, IBANs, or SWIFT/BIC codes
- Full bank statements, transaction histories, or reconciliation files
- Payroll data including individual salaries, deductions, or net pay figures
- Credit card numbers, CVVs, or cardholder data of any kind
- Confidential financial projections linked to undisclosed business activities
- Vendor payment details including account numbers or payment references
- Group treasury, cash flow, or liquidity data in raw or identifiable form

What Finance teams ARE permitted to do with AI tools:

- Drafting narrative commentary using anonymised figures (e.g. 'Revenue grew by 12%' with no account or party names)
- Building report templates and presentation layouts in Docs and Slides
- Creating formula logic and financial models in Sheets using dummy or test data
- Drafting finance-related emails, proposals, and budget summaries

4.3 HR & Employee Personal Data

HR teams must exercise particular care given the sensitivity of employee data:

- Never paste employee ID numbers, passport details, or visa information into any AI tool
- Never input individual salary figures, compensation packages, or bonus details in bulk
- Do not use any AI tool to process disciplinary records or grievance case notes
- Performance review templates and frameworks are permitted; individual assessments with named employees are restricted to authorised HR or manager use only

4.4 Absolutely Prohibited Activities

The following are prohibited for all employees regardless of context or justification:

- Using any personal or unmanaged AI account for Vista Group work tasks
- Sharing AI-generated confidential outputs with unauthorised external parties
- Using any AI tool to generate content that misrepresents Vista Group's position, finances, or official communications
- Attempting to extract or reconstruct data belonging to other users via any AI tool
- Using any AI tool to produce deceptive, harassing, or discriminatory content of any kind

5. How AI Platforms Handle Vista Group Data

Employees should understand how different AI platforms handle data, and apply the appropriate level of care:

Company Managed AI Tools: Your prompts and outputs on company approved and company managed AI platforms remain within Vista Group's controlled environment. No data leaks across user or organisation boundaries within these managed sessions.

No External AI Training on Managed Platforms: For company-managed AI tools, your prompts and content are not used to train AI models outside your domain without explicit approval from Vista Group as the account administrator.

DLP and IRM Integration: All Data Loss Prevention and Information Rights Management policies continue to apply to AI-generated content. If a file has restricted access controls, company-managed AI tools cannot access it on your behalf.

External AI Tools (ChatGPT, Claude, Perplexity, DeepSeek, Kimi, Doubao): These tools are operated by third-party providers. Data submitted is processed on external servers. Always use enterprise or business accounts where available, and never submit restricted data categories (see Section 4) to any external AI platform.

Platform Certifications: Major enterprise AI platforms including Google Workspace Gemini, Microsoft Copilot, and Claude (Anthropic) hold industry certifications such as ISO 42001 and SOC 2. For any AI platform used for work purposes, employees must use business or enterprise accounts where data processing agreements are in place. If unsure whether your account qualifies, check with the IT team before use.

Prompt Injection Risks: Be cautious when pasting external or untrusted content into any AI tool. Malicious content can attempt to manipulate AI behaviour. This applies to all platforms.

6. Employee Responsibilities

By using any AI tool for Vista Group work tasks, you confirm your agreement to the following:

1. Read and understand this policy fully before using any AI tool for work purposes.
2. Use only company-approved or company-managed AI platforms for sensitive or internal work tasks. If using an external AI tool, use a business account and never submit restricted data.
3. Review all AI-generated content before sharing it externally. You are personally responsible for the accuracy of what you send. Gemini can and does make errors.
4. Never input prohibited data categories (especially banking, payroll, credentials, or personal identity data) into any Gemini prompt.
5. Do not share confidential AI session outputs with anyone outside Vista Group or with unauthorised internal parties.

6. Report any suspected data exposure, policy breach, or unusual AI tool behaviour to the IT team immediately.
7. Apply professional judgement. If a task feels sensitive, ask your manager or the IT team before proceeding.
8. **Freedom to use AI tools comes with clear personal responsibility.** The freedom to use AI tools across Vista Group comes with a clear responsibility to think, check, and take full accountability for every output. AI is a tool, not a decision-maker. You remain personally responsible for everything produced, shared, or acted upon using AI assistance.

6.1 Manager & Department Head Responsibilities

In addition to the above, all managers and department heads are expected to:

- Brief their teams on this policy before they use any AI tool for work purposes
- Ensure Finance team members understand the specific restrictions on financial data in Section 4.2, which apply to all AI platforms without exception
- Escalate any suspected misuse to the IT Director immediately
- Lead by example in the responsible and professional use of AI tools

All AI tool activity on managed platforms is auditable by administrators. Use all AI tools professionally and in accordance with this policy at all times.

7. AI Tool Limitations: What Employees Should Know

All AI tools, regardless of platform, have inherent limitations employees should be aware of:

- Managed AI tools cannot access files or emails you do not have permission to view. Access controls are always enforced
- Managed AI tools cannot access Client-Side Encrypted files under any circumstances
- Most AI tools do not retain memory between sessions. Each new session starts from scratch unless a memory feature has been specifically enabled
- All AI tools can produce factual errors (hallucinations), so always verify critical facts, figures, and legal or financial content before external use
- AI tools cannot access internal Vista Group systems such as ERP, CRM, payroll, or banking platforms unless a specific integration has been configured and approved by IT
- No AI tool is a substitute for professional legal, financial, or compliance advice

8. Incident Reporting

If you believe a policy breach has occurred, for example if restricted data was accidentally entered into a prompt or if you suspect unauthorised access, you must report this immediately. Do not attempt to investigate or resolve the incident yourself.

Primary Contact	Vista Group IT (Deepu Gopi)
Secondary Contact	Your Line Manager or Department Head
Escalation	Reach out to Taran Varyani for incidents involving financial or legal data
Response Time	All reported incidents acknowledged within 24 hours

9. Policy Review & Compliance

This policy will be reviewed annually or whenever significant updates are made to AI platforms used by Vista Group's capabilities or Vista Group's operational structure. Employees will be notified of any material changes.

Non-compliance with this policy, and in particular the restrictions in Section 4, may result in disciplinary action in line with Vista Group's HR and Code of Conduct policies, up to and including termination of employment where warranted.

Version 1.0, Issued April 2026. Next Review Due: April 2027