Read this first

IMPORTANT NOTICE

This AI Usage Policy Template is provided for informational and illustrative purposes only.
It is not intended to constitute legal advice or serve as a substitute for consultation with qualified HR, legal, or compliance professionals.

Employment laws, privacy regulations, and AI governance rules may vary by country, state, or industry.

Before implementing, distributing, or enforcing this policy within your organization, it is your responsibility to ensure alignment with:

- Local and national laws
- Your existing HR frameworks, privacy policies, or contractual obligations
- Guidance from your internal legal and compliance teams

The author and publisher accept no liability for any outcomes related to the use or misuse of this document.

Corporate Artificial Intelligence (AI) Usage Policy

Governance, Guidelines, and Acceptable Use Standards

[Company / Organization Name] [Publication Date] [Version Number]

GREEN VALLEY GRID
CORPORATE
SEAL
2025
SEATTLE
★

‘*** SAMPLE TEMPLATE ***

1. Purpose

This policy outlines how artificial intelligence (AI) tools may be used when performing work on behalf of [Company Name].

Its goal is to encourage responsible and productive use of AI while protecting data, ensuring legal compliance, and maintaining quality standards.

2. Scope

This policy applies to:

- All employees, contractors, freelancers, interns, and advisors working for or representing [Company Name]
- All business activities involving internal systems, tools, data, or client-facing work

3. Approved AI Tools

Only tools approved by [Company Name] may be used for work purposes.
Example approved tools include:

- Microsoft Copilot (Office 365)
- ChatGPT (Enterprise or Team edition)
- Google Gemini for Workspace
- Otter.ai for transcription
- AI tools embedded in company-licensed software

Use of personal AI tools or browser extensions without prior approval is not permitted.

Approved AI Tools Tracker

Tool Name	Purpose / Use Case	Approval Status	Data Sensitivity Warning	Reviewer / Contact
Microsoft Copilot	Embedded AI in Microsoft 365 for writing, analysis, and automation	Approved	Do not use with confidential documents unless encrypted	IT Manager
ChatGPT Enterprise	Text generation, summarization, ideation with data privacy controls	Approved	No PII or client data without masking	Compliance Officer
Google Gemini Business	Research, document generation, and summarizing for Google Workspace	Approved	Avoid uploading contracts or sensitive HR content	IT Manager
Otter.ai (Business)	Transcription, meeting summary, and collaboration	Approved	Only use company email login; avoid uploading private calls	Team Leader
Notion AI	Knowledge management, content drafting, and workflows	Pending Review	Review output; not suitable for final client documents	Knowledge Lead
GrammarlyGO	Email tone editing, document writing assistance	Approved	Do not rely for legal, compliance, or medical writing	Communications
Zapier AI	Automation of repetitive tasks and cross-app AI integrations	Pending Review	Test in sandbox before production use	Automation Lead

4. Acceptable Use

AI tools may be used for:

- Drafting outlines, summaries, or emails
- Brainstorming ideas or generating variations
- Summarizing meetings or notes
- Research support (with fact-checking)
- Automating repetitive internal workflows (e.g., scheduling, task categorization)

All AI output must be reviewed and verified before external use.

5. Prohibited Use

You must not use AI tools for:

- Uploading or exposing confidential data
- Creating legal, medical, or contractual content without review
- Replacing human approval in client communications
- Circumventing copyright, plagiarism, or ethical standards
- Impersonating individuals or generating deceptive content

6. Privacy and Security

To uphold data integrity and privacy:

- Never input personal data, financials, passwords, or client records into AI tools unless approved and encrypted
- Only use AI through company-managed platforms
- Follow [Company Name]'s IT security and privacy guidelines at all times

7. Ethical Use

You are expected to:

- Be transparent about when AI is used (where appropriate)
- Attribute content sources when summarizing or quoting
- Avoid bias, harmful stereotypes, or discriminatory AI outputs
- Report unexpected or concerning AI behaviors

8. Review and Oversight

- All AI-assisted work must be reviewed by a human before being submitted or published
- Supervisors are responsible for verifying that team members understand and follow this policy
- Maintain logs or notes of AI-generated contributions where applicable

9. Training and Readiness

Before using AI tools:

- Complete the AI Onboarding Session
- Read this policy in full
- Attend refresher updates as new tools or regulations emerge

10. Violations and Consequences

Violations may result in:

- Suspension of tool access
- Performance reviews or retraining
- Disciplinary action or contract termination in serious cases

11. Policy Maintenance

This policy will be reviewed every 6 months.
To request clarification or propose revisions, contact: [Policy Administrator Name / Email].

12. AI Use Outside the Office

Working remotely or while traveling brings flexibility — but it also requires additional care when using AI tools. The following rules apply when using AI tools in home offices, co-working spaces, while traveling, or on personal devices.

Allowed with Caution

- **Approved AI tools** may be accessed offsite, provided:
  - You are using a company-managed or secured device
  - You connect through a secure Wi-Fi or VPN connection
  - You do not input confidential data while in public or unsecured locations
- **Work-related AI use after hours** is permitted if aligned with your responsibilities and reviewable by your team lead

Use with Extreme Caution

- When working in **public spaces** (airports, cafes, libraries):
  - Avoid typing or copying sensitive information into any AI tool
  - Refrain from using voice transcription or meeting summaries with client or team names
  - Use privacy screens or headphones if discussing AI-generated outputs

❌ Not Permitted

- Using AI tools on unapproved or personal devices without security protocols
- Uploading or referencing **client names**, **project files**, or **financial data** outside secure systems
- Allowing family or non-staff members to interact with AI platforms tied to your business account

Data Security Reminders

- Use VPNs or company-secured login portals when traveling
- Never save AI prompts or content to shared or cloud folders that aren't company controlled
- Be cautious when using browser-based AI tools if you're unsure about their data retention policies