A DDH AI COUNCIL PUBLICATION

Framework for Employee Generative AI Usage Policy

Direct Digital Holdings

Colossus SSP® Orange 142®

Forward

Generative AI tools are transforming the workplace. Eager to explore their potential, employees are bringing these tools into the workplace and in the process, driving higher output and delivering higher-quality work. Their initiative bodes well for organizations in that they can expect to reap the benefits of greater efficiency and innovation.

At the same time, adopting generative AI is not without risks. Data leakage, reliance on inaccurate outputs, and other unforeseen challenges can pose significant threats to businesses if generative AI usage isn't managed correctly.

Despite the widespread use of generative AI, just 44% of companies have implemented formal Employee Generative AI Usage Policies. As these tools continue to proliferate, establishing clear guidelines is no longer optional -- it's essential.

This framework is not a governance document; rather, it is designed to supplement your organization's broader AI governance framework. The purpose of this framework is to help business leaders articulate to their employees that they are expected to comply with organizational policies while using generative AI tools. Our goal is to provide you with a foundation for crafting an Employee Generative AI Usage Policy that is tailored to your organization's needs.

The DDH AI Council created this framework to help organizations navigate this critical task. It provides a foundation for crafting an Employee Generative AI Usage Policy tailored to your organization's needs.

Keep in mind that generative AI is a rapidly evolving field. New developments will inevitably require periodic updates to your policy, ensuring it remains relevant, practical, and aligned with emerging best practices.

Important Note

This framework is designed to serve as a starting point for organizations crafting an Employee Generative AI Usage Policy. It is provided for illustrative purposes only and does not constitute legal or regulatory advice. You should customize this framework to align with your unique operational needs, industry requirements, and legal obligations.

We strongly encourage consulting legal, compliance, and data privacy experts to ensure your policy adheres to applicable regulations and safeguards your organization's interests. The information in this document is provided "as is," without warranties of any kind, and should be used at your discretion.

About the DDH AI Council

The DDH AI Council was founded to address a growing concern: the widening divide between organizations that embrace generative AI and those that are hesitant to adopt it. Generative AI is rapidly reshaping how we work, raising the overall caliber while enabling teams to innovate faster. For many business leaders, generative AI is still an unknown technology that comes with many risks. We aim to demystify generative AI and provide the education and insights business leaders need to build a roadmap for its adoption, with complete confidence that its use will be safe and transformative.

Table of Contents

1. Purpose & Scope

Why define a Purpose?
Your employees are likely already using generative AI in their day-to-day jobs. While you want to encourage that use, it's critical that they are made aware of the risks, and the steps you want them to take to mitigate harm.

When crafting your Purpose:

- **Clearly communicate expectations,** emphasizing the responsible and ethical use of generative AI tools in alignment with the organization's standards.
- **Describe the risks** associated with generative AI, such as data leakage, security breaches, and disseminating inaccurate or biased information.
- **Promote awareness** of the organization's goals for AI use, including safeguarding intellectual property, ensuring compliance with legal requirements, and maintaining trust with stakeholders.
- **Encourage transparency** by helping employees understand the reasoning behind the policies, and fostering a culture of informed and responsible usage.

Sample Purpose:

The purpose of this Generative AI Usage Policy is to provide clear guidelines for the responsible and effective use of generative AI tools within the organization. Generative AI has the potential to significantly enhance productivity, creativity, and efficiency in the workplace. From streamlining routine tasks to enabling innovative problem-solving, these tools empower employees to deliver higher-quality work at a faster pace.

However, the use of generative AI also introduces risks, including potential data security breaches, reliance on inaccurate or incomplete outputs, and the inadvertent dissemination of biased or inappropriate content. By adopting this policy, the organization aims to maximize the benefits of generative AI while mitigating its risks. This policy fosters a culture of responsible AI use that aligns with the organization's ethical standards, legal requirements, and operational goals.

Why Define Your Scope?
Your scope should define who the policy applies to and clarifies the types of generative AI tools and activities covered.

Sample Scope:

This policy applies to:

- **All personnel**, including full-time and part-time employees, contractors, interns, and third-party vendors, who use generative AI tools in their work for the organization.

- **All generative AI tools,** including but not limited to those used for:
    - **Text generation:** Tools that assist with drafting, summarizing, or editing text (e.g., reports, emails, or marketing content).

    - **Code development:**Tools that support coding, debugging, or generating software code.

    - **Graphic creation:** Tools used to produce images, videos, or other visual content.

The policy covers both organization-approved tools and any personal tools that employees or contractors may use for work-related tasks. Any unauthorized or improper use of generative AI tools that could compromise the organization's security, reputation, or compliance with regulations is strictly prohibited.

2. Guiding Principles

Why Create Guiding Principles?

Guiding principles establish the foundational values and standards for responsible AI usage within the organization. These principles:

- **Ensure Trust:** Reflect your organization's commitment to using AI in ways that enhance, rather than damage, the trust placed in it by customers, stakeholders, and the public.
- **Protect Reputation:** Signal the organization's dedication to maintaining a strong ethical standards, which in turn, will safeguard your reputation in the market.
- **Promote Accountability:** Set clear expectations for employees to uphold company values when using AI tools.
- **Align Practices with Ethics:** Foster confidence by demonstrating that AI practices align with the organization's mission, values, and regulatory responsibilities.
- **Provide a Framework:** Serve as a foundation for addressing emerging challenges as AI technologies evolve.

Sample Guiding Principles:

Transparency

Employees must disclose the use of generative AI when relevant, especially in customer-facing outputs, to maintain trust and clarity. Examples include:

- Noting when text or images are AI-generated in communications.
- Clearly labeling AI-generated visuals in presentations or marketing materials.

Accountability

Employees are responsible for ensuring AI outputs align with company standards, including:

- Verifying the accuracy of information before sharing.

- Ensuring AI-generated content complies with brand voice, quality, and ethical guidelines.

Ethical Use

Generative AI must not be used to create harmful, deceptive, or biased content. Prohibited uses include:

- Generating discriminatory or offensive material.
- Using AI to impersonate individuals or fabricate misleading content.

Compliance

AI usage must adhere to all applicable laws and regulations, such as:

- Data Privacy Laws: Avoid inputting personal or sensitive information unless tools meet compliance standards.
- Intellectual Property Laws: Respect copyright and licensing agreements for all AI-generated and training data.

- Industry-Specific Regulations: Ensure outputs meet standards set by governing bodies (e.g., HIPAA for healthcare data).

3. Acceptable Generative AI Uses

Why Spell Out Acceptable Uses?
Your acceptable use case policies should be designed to:

- **Meet customer expectations:** Customers and stakeholders expect organizations to leverage cutting-edge tools to enhance productivity and efficiency, but they don't want to forgo the expertise your teams bring to the table.

- **Clarify the role of generative AI:** Ensure employees understand that generative AI is a tool to support their work, not replace it. AI should streamline processes while preserving human oversight, creativity, and judgment.

- **Protect the company's reputation:** Clearly define acceptable use cases to prevent inappropriate or overly reliant use of AI, which could damage stakeholder trust or the quality of deliverables.

- **Encourage responsible innovation:** Communicate to employees that they are encouraged to adopt AI tools in approved scenarios while adhering to company standards and values.

Sample Acceptable Uses:

Acceptable Uses of Generative AI
Generative AI tools are powerful resources designed to complement human expertise and drive innovation. We encourage you to use approved AI tools to improve your efficiency and creativity, but we expect that any output you use meets our standards for accuracy, ethics, and quality. Below are the approved use cases, categorized by function:

Text Creation
- Drafting reports, emails, social media posts, or marketing copy.
- Generating ideas or outlines for proposals or creative content.
- Summarizing complex documents or translating text for accessibility.

Code Writing

- Automating repetitive or time-consuming coding tasks.
- Assisting with debugging, code review, or refactoring.
- Developing prototypes or small-scale software solutions to support innovation.

Graphics Creation

- Designing mockups, presentations, or marketing materials.
- Producing concept art or exploring design ideas for projects.
- Enhancing visuals for internal use or creating client previews.

4. Prohibited Generative AI Uses

Why Define Prohibited Generative AI Use Cases?
The use cases will naturally expand as employees experiment with generative AI tools. It's in your organization's best interest to encourage innovation, but you must set clear boundaries of what is acceptable and what isn't. The best way to do that is to provide explicit examples of uses for which generative AI may not be used.

A well-defined prohibited generative AI use case policy will:

- **Mitigate risks to reputation:** Clear boundaries will protect your organization from reputational damage caused by inappropriate or harmful uses of AI.
- **Ensure compliance:** Explicitly defined prohibited activities will prevent violations of data privacy laws, intellectual property rights, and industry-specific regulations.
- **Set clear expectations for employees:** Eliminate ambiguity about what is and isn't acceptable, ensuring employees understand the limits of generative AI use.
- **Prevent misuse of AI tools:** Safeguard against unintentional harms, such as data leaks, generation of misleading or biased content, or over-reliance on unverified outputs.

Sample Prohibited Uses:

Text Creation:

- Generating public-facing content (e.g., emails, reports, or social media posts) without human review for accuracy and brand voice.
- Unless explicitly authorized, produce content involving sensitive or proprietary information, such as financial data or client names.
- Creating outputs that could be deceptive, biased, harmful, or violate the organization's ethical standards.

Code Writing:

- Using AI tools to develop code without conducting thorough testing and review for errors, security vulnerabilities, or unintended consequences.
- Automating mission-critical systems or operations without proper oversight and validation.
- Inputting sensitive or proprietary code into free or public generative AI tools that do not meet the organization's security requirements.

Graphics Creation:

- Using AI-generated visuals for external use (e.g., marketing campaigns or client deliverables) without appropriate review to ensure brand compliance and accuracy.
- Generating graphics based on unlicensed or copyrighted materials without verifying proper permissions.
- Producing visuals that could mislead or harm stakeholders, such as fabricated charts or manipulated imagery.

5. Data Handling & Privacy

There have been a number of high profile data leaks that were the result of employees uploading sensitive or proprietary information to a free generative AI tool. To a large extent, these tools are new and employees aren't aware of the risks they may prevent. For this reason, it is essential that you provide explicit instruction about the data your employees are permitted to use as inputs.

Your data handling & privacy policy should:

- **Prevent data leaks:** A clear policy ensures sensitive or confidential information is not exposed.
- **Meet legal and regulatory obligations:** In industries like healthcare or finance, legal frameworks (e.g., HIPAA, GDPR) mandate strict guidelines for how data is used and protected.
- **Protect client and stakeholder trust:** Your organization's reputation depends on safeguarding the information clients entrust to you. Failure to do so can lead to significant reputational and financial consequences.
- **Clarify employee responsibilities:** Provide employees with explicit instructions on what data can and cannot be shared with AI tools to prevent unintentional violations.

Sample Data Handling & Privacy:

Input Guidelines:
To meet our commitments, all employees and contractors are expected to follow these guidelines regarding data can and cannot be entered into generative AI tools.

- **Permitted Data:**
    - Publicly available information, such as published research or industry benchmarks.
    - Anonymized internal datasets, where all personally identifiable information (PII) and sensitive client data have been removed.

    - Non-sensitive internal content used for brainstorming or generating outlines.

- **Prohibited Data:**
    - Personally Identifiable Information (PII), such as names, addresses, Social Security numbers, or financial details.
    - Confidential client data, including project specifics, contracts, or proprietary insights.
    - Trade secrets, such as algorithms, strategies, or intellectual property.
    - Data restricted by legal or contractual obligations (e.g., HIPAA-protected health information, NDAs).

Output Guidelines:
The company expects that all employees and contracts who use generative AI to review and validate AI-generated outputs to ensure compliance and quality. Specific obligations include:

- **Validation of Outputs:**
    - Cross-check AI outputs against verified sources to ensure factual accuracy.
    - Review content for alignment with company policies, ethical standards, and brand voice.
    - Confirm outputs do not include unverified or sensitive information.

- **Escalation Requirements:**
    - If an AI output contains potentially harmful, biased, or non-compliant content, employees must escalate it to the appropriate supervisor or compliance officer.

6. Approved Tools & Ongoing Monitoring

Why Create Approved Tools & Ongoing Monitoring Policies?
Just about every generative AI tool offers a free version, but "free" always comes with a hidden cost. Free tools leverage user input to train the model -- which can put your proprietary data and intellectual property at risk.

A well defined list of approved tools and ongoing monitoring will:

- **Ensure data security:** Different AI tools have varying levels of privacy controls. By reviewing the privacy policies of each tool, and approving only secure, enterprise-level tools, your organization reduces the risk of data leaks.

- **Mitigate compliance risks:** Certain tools may not meet regulatory requirements for data handling, particularly in industries governed by laws like HIPAA, GDPR, or CCPA. Approving tools ensures compliance with these standards.

- **Standardize tool usage:** Without clear guidelines, employees may adopt a patchwork of tools that are difficult to monitor or integrate. A centralized approval process ensures consistency and better oversight.

- **Leverage enterprise-grade capabilities:** Paid, enterprise-grade tools often come with enhanced features, such as administrative controls, encryption, and detailed usage tracking, which align with organizational security needs.

- **Build trust with stakeholders:** Clients and partners expect your organization to use secure, vetted tools. A robust approval and monitoring policy demonstrates your commitment to protecting their data and interests.

Sample Approved Tools & Ongoing Monitoring:

Tool Approval Process:
Below is the process employees and contractors must follow in order to use a generative AI tool in the workplace:

- **Tool Evaluation**

    - Submit a request to IT or the designated approval team to evaluate the tool (include contact info)

- **The team will assess the tool for:**
    - Privacy policies: Does the tool explicitly state it doesn't use input data to train its models?
    - Security features: Does it offer encryption, data access controls, and enterprise-grade privacy measures?
    - Compliance: Is it compatible with relevant regulations (e.g., GDPR, HIPAA)?

- **Approval**
    - Only tools that meet organizational standards will be added to the approved tools list.
    - Employees may not use unapproved tools for work-related purposes.

Ongoing Monitoring

To ensure ongoing security and compliance the company will monitor ongoing use of tools, including:

- **Access Controls:**
    - Require login credentials tied to the organization for all AI tools.
    - Ensure tools are configured to restrict unauthorized access.

- **Activity Audits:**
    - IT or compliance teams will conduct periodic audits of AI tool usage to identify potential risks or misuse.
    - Implement monitoring for unusual activity, such as excessive data uploads or non-standard queries.

- **Feedback Mechanisms:**
    - All employees are expected to report any concerns or potential issues with approved tools, such as output inaccuracies or security vulnerabilities. Submit your reports to [contact information].

Revocation Policy

- If a tool no longer meets security or compliance standards, it will be removed from the approved list.

- Employees will be notified of the change and directed to alternative, approved tools.

7. Human Oversight & Responsibility

We can't emphasize this enough: Generative AI serves as an assistant to humans, but it should never replace them. Requiring human oversight will protect your organization in numerous ways, including:

- **Ensure accuracy and reliability:** AI-generated outputs are prone to errors, biases, or hallucinations (outputs that are plausible but incorrect). Human review ensures the final content is accurate, factual, and fit for its intended purpose.

- **Preserve brand voice and standards:** Generative AI tools produce generic outputs unless guided by your internal experts. Humans are essential for refining AI-generated content to reflect the organization's unique voice, values, and style.

- **Uphold ethical and legal standards:** AI tools cannot inherently understand complex legal, ethical, or cultural considerations. Human oversight ensures outputs comply with relevant laws and avoid causing harm or offense.

Sample Human Oversight & Responsibility Policy:

Our organization recognizes the inherent limitations of generative AI in terms of reasoning and understanding the nuances of our industry. For this reason, all employees are expected to follow the guidelines below.

Review for Accuracy and Reliability:

- Fact-check all AI-generated outputs before publication, especially in customer-facing or high-stakes contexts.
- Validate any data, statistics, or quotes generated by AI against reliable sources.

Maintain Brand Voice and Standards:

- Refine AI-generated content to align with the organization's tone, style, and branding.
- Use approved templates or style guides to guide AI outputs and human refinements.

Ethical and Legal Compliance:

- Review AI-generated content for potential ethical concerns, such as biased or harmful language.
- Ensure compliance with industry-specific regulations, such as those governing advertising, privacy, or accessibility.

Human Accountability:

- Employees are ultimately responsible for the quality and accuracy of any AI-generated outputs they submit or publish.
- Outputs must go through designated approval processes (e.g., manager review, legal sign-off) before release.

Reinforce the Role of Human Expertise:

- AI tools are designed to assist, not replace, human creativity, judgment, and critical thinking.
- Final decision-making must always rest with a human, ensuring outputs align with organizational goals and values.

9. Consequences of Misuse

Why Define Consequences for Misuse?
Generative AI tools burst onto the scene, promising a dazzling array of efficiencies and accuracies. Less discussed by the AI companies are the risks of inaccurate prompts and data leakage. Many employees are simply not aware of the risks.

The severity of consequences will depend on your sector and legal obligations. Only your organization can determine the consequences of misuse should be.

10. Parting Thoughts

Generative AI offers unprecedented opportunities to enhance efficiency, creativity, and innovation in the workplace. However, with these opportunities come significant responsibilities. By implementing a clear Employee Generative AI Usage Policy, organizations can strike the right balance—leveraging the power of AI tools while safeguarding their data, reputation, and stakeholder trust.

This framework is designed to serve as a starting point. It provides organizations with a solid foundation for defining acceptable practices, managing risks, and aligning employee behavior with broader governance principles. As AI technologies continue to evolve, so too should your policies, ensuring your organization remains agile, secure, and forward-thinking.

Additional Reading
For additional resources and guidance, explore other publications by the DDH AI Council, including:

- **The Generative AI Roadmap**
- **Responsible AI: A Beginner's Guide**
- **Best Practices for Generative AI Prompting**

About Direct Digital Holdings

Direct Digital Holdings (Nasdaq: DRCT) brings state-of-the-art sell- and buy-side advertising platforms together under one umbrella company. Direct Digital Holdings' sell-side platform, Colossus SSP, offers advertisers of all sizes extensive reach within the general market and multicultural media properties. The Company's buy-side platform, Orange 142, delivers significant ROI for middle-market advertisers by providing data-optimized programmatic solutions for businesses in sectors ranging from energy to healthcare to travel to financial services. Direct Digital Holdings' sell- and buy-side solutions generate billions of impressions per month across display, CTV, in-app, and other media channels.

Direct Digital Holdings
1177 West Loop South | Suite 1310
Houston, TX 77027
marketing@directdigitalholdings.co

Important Note

The resources and guides provided by the DDH AI Council are designed to serve as starting points for organizations navigating the evolving landscape of generative AI. They are provided for illustrative purposes only and do not constitute legal, regulatory, or operational advice.

Organizations should tailor these materials to align with your specific needs, industry requirements, and legal obligations. We strongly recommend consulting legal, compliance, and data privacy experts to ensure adherence to applicable regulations and the safeguarding of organizational interests. All information is provided "as is," without warranties of any kind, and should be used at your discretion.

Disclaimer: The responses provided by this artificial intelligence system are generated by artificial intelligence based on patterns in data and programming. While efforts are made to ensure accuracy and relevance, the information may not always reflect the latest data and programming news or developments. This artificial intelligence system does not possess human judgment, intuition, or emotions and is intended to assist with general inquiries and tasks. Always conduct your own independent in-depth investigation and analysis of ANY information provided herein, and verify critical information from trusted sources before making decisions.

Interested parties should not construe the contents of ANY responses and **INFORMATION PROVIDED** herein as legal, tax, investment or other professional advice. In all cases, interested parties must conduct their own independent in-depth investigation and analysis of ANY responses and information provided herein. In addition, such interested party should make its own inquiries and consult its advisors as to the accuracy of any materials, responses and information provided herein, and as to legal, tax, and related matters, and must rely on their own examination including the merits and risk involved with respect to such materials, responses and information.

We nor any of our affiliates or representatives make, and we expressly disclaim, any representation or warranty (expressed or implied) as to the accuracy or completeness of the materials, responses and information **PROVIDED** or any other written or oral communication transmitted or made available with respect to such materials, responses and information or communication, and we, nor any of our affiliates or representatives shall have, and we expressly disclaim, any and all liability for, or based in whole or in part on, such materials, responses and information or other written or oral communication (including without limitation any expressed or implied representations), errors therein, or omissions therefrom.