AI Workforce Literacy

Level 1, Module 7: Company Guidelines & Data Confidentiality

Introduction

Throughout this course, we have explored the power of generative AI and the ethical principles that should guide its use. This final module of Level 1 brings these concepts into our specific work environment. Using AI tools is not just a matter of technical skill or ethical theory; it is also governed by company policy. Adhering to these guidelines is essential for protecting our company, our customers, and ourselves.

This module will provide a clear overview of the company's official policy on the use of artificial intelligence. We will cover which tools are approved for use, what kinds of data are permissible to use with them, and the best practices you are required to follow. The goal is to ensure that every employee can innovate with AI confidently and safely, without putting sensitive information at risk.

Chapter 1: The Importance of a Company AI Policy

A company-wide AI policy is not meant to stifle innovation. On the contrary, it is designed to **enable** it by creating a safe and secure framework. Without clear guidelines, employees are left to guess about what is and isn't acceptable, which can lead to hesitation or, worse, risky behavior. A clear policy ensures that we can all leverage the benefits of AI while mitigating the potential dangers.

The Core Goals of Our AI Policy:

1. **Protect Intellectual Property (IP):** To prevent company secrets, product plans, and proprietary code from being leaked to the public or absorbed into third-party AI models.

2. **Safeguard Customer & Employee Data:** To ensure that Personally Identifiable Information (PII) and other confidential data are handled in accordance with legal and ethical standards.
3. **Ensure Legal Compliance:** To adhere to copyright laws, data privacy regulations (like GDPR), and other legal requirements.
4. **Promote Consistency & Fairness:** To ensure that AI is used in a consistent and ethical manner across the entire organization.

Chapter 2: Approved & Prohibited AI Tools

Not all AI tools are created equal. Some have strong security and privacy guarantees, while others are public-facing and offer very few protections. Our company has evaluated and approved a specific set of tools for employee use. Using unapproved tools for company work is strictly prohibited.

[Placeholder for Company-Specific Information]

This section would be customized by the company with their specific list of tools.

Tool Category	Approved Tools	Prohibited Tools (Examples)
Public Chatbots	- **[Example: ChatGPT Enterprise]** - **[Example: Microsoft Copilot with Commercial Data Protection]**	- Free, public version of ChatGPT - Google Bard (standard version) - Any other public chatbot not on the approved list
Image Generators	- **[Example: Adobe Firefly]** - **[Example: Microsoft Designer]**	- Midjourney - Stable Diffusion (public instances)
Coding Assistants	- **[Example: GitHub Copilot for Business]**	- Any coding assistant not officially managed by the company

Why the Distinction?

Approved tools, like an Enterprise version of a chatbot, typically come with a contractual agreement that your company's data will **not** be used to train the public model and will be kept private and confidential. Public, free versions of these tools often have no such guarantee. The data you enter can and will be used to train the

model, meaning your confidential information could one day appear in a response to another user.

Always check the official, up-to-date list of approved tools on the company intranet before using a new AI service.

Chapter 3: Data Classification - What You Can and Cannot Use

Even with an approved tool, the most important rule revolves around the **type of data** you use in your prompts. Our company classifies data into different levels of sensitivity. Your responsibility is to understand this classification and never use high-sensitivity data with AI tools.

Data Classification Levels [Example]

Level	Data Type	Examples	Permissible to Use with Approved AI Tools?
Level 4: Highly Restricted	The most sensitive data, protected by law or regulation. Unauthorized disclosure would cause severe harm.	- Customer PII (names, addresses, social security numbers) - Patient health information (PHI) - Credit card and financial account numbers	**NEVER**
Level 3: Confidential	Internal company data that, if disclosed, could harm the company's competitive position.	- Unannounced financial results - Product roadmaps and strategic plans - Drafts of patent applications - Source code for proprietary software	**NEVER**
Level 2: Internal	Data intended for internal use but not highly sensitive.	- Internal team project plans - Drafts of internal presentations - General company process documents	**YES, with caution and only in approved tools.**
Level 1: Public	Data that is already publicly available.	- Published press releases - Marketing materials from our website - Publicly available industry reports	**YES**

The Golden Rule of Data:

If you are in any doubt, do not paste it. Assume the data is confidential until proven otherwise. It is always better to be too cautious than to be responsible for a data leak.

Anonymize Your Data:

When you need the AI to help with a task that involves sensitive data, you must **anonymize** it first. Replace all specific, sensitive details with generic placeholders.

- **Instead of:** "My customer, John Smith at 123 Main St, is having an issue with order #555-1234."
- **Anonymized Version:** "A customer at a specific address is having an issue with their order. The order number is [Order Number]."

Chapter 4: Best Practices & Your Responsibilities

Beyond tools and data, you are expected to adhere to the following best practices:

1. **Be Transparent:** Do not represent AI-generated content as your own original work. Be transparent with your colleagues and manager about how you are using AI to assist you.
2. **Verify, Verify, Verify:** As covered in the previous module, you are accountable for the accuracy of your work. Fact-check any claims or data points generated by an AI before using them.
3. **Retain Human Judgment:** Do not delegate decision-making to an AI. Use it as a tool for analysis and content generation, but the final judgment and decision must be yours.
4. **Respect Copyright:** Do not use AI to plagiarize or generate content in a way that infringes on the copyrights of others. Be especially careful with image generation tools; use only those that are trained on ethically sourced or licensed content (like Adobe Firefly).
5. **Report Issues:** If you discover that an AI tool is generating biased, harmful, or consistently incorrect information, or if you suspect a security issue, report it to the appropriate internal team immediately.

Conclusion

This module has provided you with the essential guidelines for using AI safely and effectively at our company. By following these rules, you become a responsible

steward of our company's and our customers' data. This allows you to innovate and improve your productivity without introducing unnecessary risk.

Key Takeaways: - Always use **company-approved AI tools** for your work. - Never input **Highly Restricted** or **Confidential** data into any AI tool. - **Anonymize** data by replacing sensitive details with generic placeholders. - You are **accountable** for all work you produce, and you must **verify** all AI-generated content. - When in doubt, always err on the side of caution and consult the official company policy or your manager.

Congratulations! You have completed Level 1 of the AI Workforce Literacy program. You now have a solid foundation in what AI is, how to use it, its limitations, and the ethical and company-specific rules that govern its use. You are ready to be a confident and responsible AI Explorer.