

Putting AI to Work

# 13

## Legal and Policy Considerations

# Learning Objectives

- Evaluate who holds ownership over AI-generated content and determine what qualifies as copyright infringement
- Identify harmful, illegal, or deceptive uses of AI and outline strategies to prevent them
- Explain the importance of disclosing AI involvement and maintaining clear documentation of how it was used
- Compare how different organizations establish policies for responsible AI use and enforce ethical guidelines

# Module 13.1: Intellectual Property

- IP refers to creations of the mind (art, music, inventions, written works) that can be legally protected.
- Most copyright laws require human authorship, so AI-generated content may not qualify for protection.
- Users may not automatically own AI-generated outputs even if they prompted the tool.
- Copyright infringement is a risk when AI outputs closely resemble copyrighted training data.
- There are complex legal gray areas: Who owns the result? The user, the AI company, or no one?
- Consult legal counsel when commercially using AI-generated content.

# Module 13.1: Ethics in Action

- Legal AI use may be unethical if the user is claiming sole authorship without giving credit.
- Ethical creators respect artistic integrity and disclose AI involvement.
- Avoid deceptive practices; transparency builds trust with audiences.

# Module 13.1: Techie Dive

- Generative models are trained on vast datasets that include copyrighted internet content.
- Models don't store material directly but can generate similar outputs.
- Style transfer and fine-tuning increase the risk of resembling protected works.
- Technical safeguards exist but are imperfect, so user responsibility remains critical.

# Module 13.1: Business Lens

- Establish clear policies for AI-generated content use in an organization.
- Legal departments must vet content for potential IP issues before publication.
- Marketing teams should disclose AI involvement where needed.
- Failure to address IP concerns can lead to lawsuits, penalties, and a damaged reputation.

# Module 13.2: Legal and Inappropriate Use

- AI introduces serious risks:
  - Deepfakes
  - Impersonation scams
  - Disinformation
  - Plagiarism
- Users are responsible for ethical use even when the laws haven't yet caught up to technology.
- Key questions:
  - Is it deceptive?
  - Is it dangerous?
  - Does it break laws or violate terms of service?
- Examples:
  - Deepfake videos
  - Voice cloning fraud
  - AI-generated cheating
  - Fake reviews
- Think critically: What AI can do vs. what it should do creates a responsibility gap.

## Module 13.2: Ethics in Action

- AI makes creating convincing but false or harmful content easy.
- Responsible use asks "should I?" not just "can I?" for every application.
- Consider the impact on others, avoid deception, and disclose AI involvement appropriately.



## Module 13.2: Techie Dive

- Many AI tools have built-in restrictions that block violence, self-harm, and impersonation.
- No system is foolproof, and jailbreaking bypasses safety filters.
- Platform rules, user education, and enforcement are critical protection layers.
- Technical solutions alone cannot prevent misuse, and human judgment is essential.

## Module 13.2: Business Lens

- Companies must ensure AI use complies with local laws (for example, GDPR and consumer protection).
- Legal misuse, even when unintentional, can lead to fines, lawsuits, and loss of trust.
- Build internal checks for legal and ethical AI use as a risk-management strategy.
- Reputational damage from AI misuse can exceed any efficiency gains.

# Module 13.3: Transparency and Documentation

- Clearly communicate when, how, and why AI was used.
- This includes disclosing AI involvement and documenting processes for accountability.
- This is critical in education, journalism, research, marketing, and public communication.
- Documentation tracks the prompts, tools used, outputs selected, and human edits.
- Building credibility through transparency goes beyond rule following to trust building.

## Module 13.3: Ethics in Action

- Transparency prevents unintentional deception and builds audience trust.
- Acknowledging AI involvement gives credit where it's due.
- Hiding AI use may be an ethical breach even if the content is accurate.

## Module 13.3: Techie Dive

- AI tools include metadata (for example, timestamps and prompt history), but it's not always visible.
- Manual documentation remains essential despite automated tracking features.
- Platforms like GitHub Copilot generate activity logs for usage tracking.
- Understanding captured data informs better documentation practices.

## Module 13.3: Business Lens

- Teams must know when to disclose AI involvement and how to keep records.
- Not disclosing in critical areas (financial reports, legal language) creates liability.
- Documentation protects against disputes and supports audit trails.
- Transparent practices enhance brand trust and demonstrate corporate responsibility.

# Module 13.4: Company Policies

- Clear organizational policies define acceptable, prohibited, and reviewed AI uses.
- Policy goals:
  - Protect privacy
  - Prevent misinformation
  - Ensure compliance
  - Clarify roles
- Types:
  - Prohibited use
  - Allowed with approval
  - Disclosure requirements
  - Review protocols
- Policies vary by industry: tech (innovation), healthcare (safety), education (integrity).
- Not having clear policies can lead to legal violations, security breaches, and a loss of public trust.

## Module 13.4: Ethics in Action

- Ethical policies balance efficiency and innovation with responsibility.
- Policies should be transparent, enforceable, and regularly updated.
- Employee training on policies and their reasoning ensures compliance.



## Module 13.4: Techie Dive

- There are data-privacy concerns when prompts or user data are stored or used by AI tools.
- Companies often ban tools from sending data to external servers.
- IT departments can integrate AI into secure environments for easier policy enforcement.
- Technical infrastructure should support, not hinder, policy compliance.

## Module 13.4: Business Lens

- Clear AI policies reduce legal risk and increase internal trust.
- Tailor policies to fit the industry, customer base, and brand values.
- Cross-functional teams (for example, legal, HR, marketing, and IT) should collaborate on development.
- Diverse perspectives ensure policies address real-world use cases effectively.

# Key Takeaways

- AI-generated content may not qualify for copyright due to human authorship requirements.
- Users are responsible for ensuring AI outputs don't infringe on existing copyrights.
- Harmful AI uses carry legal and ethical consequences regardless of their intent.
- Transparency and documentation build trust and accountability in professional contexts.
- Organizations must develop clear, enforceable AI policies tailored to their needs.
- Legal frameworks are still evolving, and personal and organizational responsibility is critical.
- Ethical AI use requires considering its impact on others beyond its technical capabilities.
- Cross-functional collaboration ensures comprehensive policy coverage.