AI Usage Policy Starter (Pragmatic Edition)

Version: 1.0
Last Updated: January 2026
Owner: Engineering Leadership

Purpose

This policy provides practical guidance on using AI tools responsibly in software development. The goal is to enable productivity while managing risks—not to create corporate theatre.

In short: Use AI tools intelligently, but always apply human judgment.

Scope

This policy covers:

- Code generation tools (GitHub Copilot, Cursor, Claude, ChatGPT, etc.)
- Documentation assistance (writing, summarizing)
- Code review and analysis tools
- Testing and debugging assistance
- Research and learning

Acceptable Use

You **may** use AI tools for:

Code Development

- Generating boilerplate code and templates
- Implementing common algorithms and patterns
- Refactoring and optimization suggestions
- Writing unit tests and test cases
- Exploring alternative implementations

Documentation

- Writing README files and API documentation
- Creating code comments and docstrings
- Summarizing technical documents
- Drafting design proposals

Learning & Research

- Understanding unfamiliar code or concepts
- Exploring new frameworks and libraries

- Debugging and troubleshooting
- Learning best practices

Productivity

- Writing SQL queries and scripts
- Creating configuration files
- Generating sample data
- Automating repetitive tasks

Restricted Use

You **must not** use AI tools with:

Sensitive Data

- Customer personally identifiable information (PII)
- Authentication credentials (passwords, tokens, keys)
- Proprietary business logic or trade secrets
- Financial or healthcare records
- Unreleased product information

High-Risk Outputs

- Security-sensitive code without thorough review
- Cryptographic implementations
- Authentication/authorization logic
- Payment processing code
- Legal documents or contracts (without legal review)
- Compliance-related code (without compliance review)

Intellectual Property Concerns

- Code that may violate licenses or copyrights
- Competitor code or proprietary systems
- Patent-pending algorithms

Best Practices

1. Review Everything

Never blindly trust AI-generated code. Always:

- Read and understand what the AI generated
- Test thoroughly
- Check for security vulnerabilities
- Verify licensing compliance
- Ensure code follows team standards

2. Keep Sensitive Data Local

- Use local AI models for sensitive work when possible
- Redact PII before pasting into AI tools
- Use synthetic/sample data for demonstrations
- Consider privacy-preserving AI tools

3. Document AI Usage in Critical Systems

For production code, note when AI was used:

```
// AI-assisted implementation of retry logic
// Reviewed and tested by: [Name], [Date]
```

4. Attribute Properly

- If using substantial AI-generated code, document it
- Check if your organization requires AI usage disclosure
- Ensure generated code respects open-source licenses

5. Maintain Your Skills

- Don't outsource your thinking to AI
- Use AI to accelerate, not replace learning
- Understand the code you ship
- Stay current with fundamentals

Review Requirements

Mandatory Human Review

All AI-generated code requires human review before merge/deployment:

- ☐ Code logic is correct and efficient
- ☐ No security vulnerabilities introduced
- ☐ Tests are comprehensive and meaningful
- ☐ No sensitive data in prompts or outputs
- ☐ Licensing is compatible
- ☐ Follows team coding standards

When to Escalate

Seek additional review when:

- AI suggests security-related changes
- Generated code handles authentication/authorization
- Output includes external dependencies
- Unsure about licensing or IP concerns

- Working with regulated data (GDPR, HIPAA, etc.)

Approved Tools

Current approved AI tools:

- GitHub Copilot (Enterprise license)
- ChatGPT (with company account)
- Claude (with API access)
- [Add your organization's approved tools]

Tool requirements:

- Enterprise/business tier when available
- Data retention policies reviewed
- Privacy settings configured appropriately

Using unapproved tools? Discuss with engineering leadership first.

Training & Support

Resources:

- Internal AI usage training: [link]
- Security guidelines: [link]
- Q&A channel: #ai-questions
- Policy questions: engineering-leadership@company.com

Regular updates: This policy will be reviewed quarterly as AI tooling evolves.

Incident Reporting

If you suspect an issue:

- Exposed sensitive data to AI tool → Report to Security immediately
- Potential IP violation → Contact Legal
- Tool misuse → Discuss with manager

We encourage learning from mistakes. Report issues without fear of punishment.

Examples

☑ Good Use Cases

Example 1: Boilerplate API Endpoint

```
Prompt: "Create a REST endpoint in C# for retrieving user profiles with proper
error handling"
Action: Review generated code, add authentication, test edge cases
```

Example 2: Test Generation

```
Prompt: "Generate unit tests for this sorting function"
Action: Verify test coverage, add edge cases, ensure meaningful assertions
```

❌ Bad Use Cases

Example 1: Security Code (Wrong)

```
Prompt: "Create JWT authentication with these secret keys: [actual secrets]"
Problem: Exposed secrets, security-critical code needs careful review
```

Example 2: Customer Data (Wrong)

```
Prompt: "Debug this query: SELECT * FROM customers WHERE
email='actual@customer.com'"
Problem: Real customer PII shared with external AI tool
```

FAQ

Q: Can I use ChatGPT for code review?
A: Yes, but redact any sensitive data first. Use AI as a second pair of eyes, not the only reviewer.

Q: Is it okay to copy-paste code from AI into production?
A: Only after thorough review, testing, and validation. Treat it like code from Stack Overflow—helpful, but requires verification.

Q: What if the AI generates code with a restrictive license?
A: Don't use it. Check licensing and ensure compatibility with your project.

Q: Can I use AI to write documentation for internal APIs?
A: Yes, this is encouraged. AI is great for documentation. Just review for accuracy.

Q: Should I disclose AI usage in commits?
A: For significant contributions, yes. For minor autocomplete, not necessary. Use judgment.

Policy Updates

This is a living document. As AI tools evolve, so will this policy.

Feedback welcome: engineering-leadership@company.com

Revision History:

- v1.0 (2026-01) - Initial policy

Remember

Use AI to be more productive, not less thoughtful.

This policy exists to help you work safely and effectively—not to block innovation. When in doubt, ask questions.