Sequoia AI-Assisted Software Development Policy

Objective

At Sequoia, we are excited about how AI can boost productivity and improve the quality of our software. But we also have a responsibility to use AI tools thoughtfully — protecting our codebase, our customers, and our intellectual property. This policy explains how to use AI tools safely, responsibly, and in alignment with our vision to become an AI-first organization.

Scope

This policy is applicable to:

- All engineers, QA testers, non-engineering staff (including product managers, designers, analysts, DevOps engineers, HR, Finance, Sales, and Marketing teams), and contractors using AI tools
- Any tool that helps generate, review, or modify code or content with the help of AI
- All software projects, internal tools, customer-facing products, and content-related workstreams

General Policy

1. **What You Can Use AI For**

   We encourage the use of AI tools for tasks like:

   - Code suggestions and auto-completion
   - Generating unit tests and test templates
   - Writing or improving comments and documentation
   - Offering code refactoring ideas or performance improvements
   - Flagging bugs or code smells through AI-based analysis tools
   - Drafting user stories, specifications, internal communication, or creative assets where applicable.
   - Automating reports, generating analytical insights, content creation, and drafting HR or financial summaries
   - Supporting AI-enabled pair programming to enhance collaboration and problem-solving with real-time AI assistance

These are great time-savers, but the developer or contributor is always responsible for the result.

2. **What You Should Avoid**

   There are some clear limits to AI use:

   - Do not copy and paste AI-generated code or content directly into production environments without reviewing it
   - Do not use AI to generate critical code for regulated areas (like medical software or finance) without an extra layer of human audit
   - Do not input confidential code, customer data, or business logic into public AI tools unless we have approved the tool for that use
   - Do not rely on AI alone to implement security-sensitive code like authentication or encryption

3. **Keep Things Legal and Ethical**

   Code and Content Ownership and Licensing

   - Always check if AI-generated output might conflict with open-source or proprietary licenses
   - Use tools that can trace where code or content comes from, when available
   - AI-written contributions should be reviewed just like human-generated work

   Confidentiality

   - Never paste sensitive code, customer info, or proprietary logic into AI tools unless we've cleared it
   - Only use company-approved AI tools that meet our data and licensing standards

4. **Code and Content Reviews Still Matter**

   AI does not replace engineering or professional judgment. Treat AI suggestions as untrusted until you:

   - Review the content yourself
   - Run or test it to make sure it behaves as expected
   - Include it in the same security, QA, or editorial processes as any other work
   - If something feels off, trust your instincts and ask a teammate or manager

5. **Training, Certification, and Knowledge Sharing**

- Sequoia will provide the required training that covers responsible AI use, risks, and limitations
- Employees are encouraged to complete AI-related certification courses from approved providers
- Teams should document and share pilot projects and AI use cases through internal knowledge channels
- Regular workshops and updates will keep teams informed as tools and risks evolve

6. **Getting a Tool Approved**

Before using a new AI tool for development or business content creation, it needs to be approved. We will check:

- How it handles and stores data
- What are the licensing terms?
- Whether it fits smoothly into our stack

An AI Committee will be constituted by Sequoia and this committee will support tool vetting and maintain an approved tools list.

An initial set of approved AI tools will be published along with this policy. A dynamic registry of currently approved tools will be maintained and communicated to all.

7. **Oversight, Governance, and Metrics**

- Team leads and team managers will audit projects periodically to ensure proper AI use
- The AI Committee is responsible for defining policy direction, tool approval, and knowledge sharing
- The committee will collect metrics and curate success stories

Sample Key Performance Indicators (KPIs) may include:

- Reduction in development or content creation time
- Increase in test coverage or documentation completeness
- Percentage of team members trained and certified
- Number of approved tools adopted per department
- Count and quality of AI-generated pilot use cases

These KPIs will evolve over time as our understanding of impact deepens and our AI-first goals mature.

Adherence and Self-Study Declaration

All employees must complete a mandatory self-study module covering this policy and sign an adherence declaration, like the company's POSH compliance model. In addition, employees will undergo annual internal assessments to evaluate understanding and appropriate application of AI tools in their workflows. This ensures that everyone understands their responsibilities when using AI tools.

Improving the Policy

This policy will grow and evolve. Version history will be tracked, and input is welcomed. If something is unclear or needs updating, let your manager or the policy owner know.

Let us use AI as a smart, powerful assistant - not as a replacement for good judgment and collaboration.

Annexure – Approved Tools

- GitHub Copilot
- Tabnine
- ChatGPT
- Google Gemini