Information and Consent to Participate in a Research Study

A. PURPOSE
The purpose of this research is to evaluate the feasibility, perceived benefits, and implementation challenges of draft AI usage policies for software bug fixing. By assessing developers' willingness to adopt these policies, their concerns, and their preferences across varying organizational policy conditions, this study aims to uncover practical insights for refining responsible AI governance in software engineering.

B. PROCEDURES
The study will take approximately 10 minutes to complete. Participants will be asked to fill out an anonymous online survey consisting of multiple-choice and open-ended questions exploring their experiences with proposed AI usage policies for bug fixing, specifically regarding disclosure practices and human oversight. Questions will cover perceptions of feasibility, implementation challenges, and trust in AI under different policy conditions. Participation is voluntary. The survey will be conducted via the SurveyMonkey platform (Here is a link to the privacy policy of the platform.)

C. RISKS
There are no known risks to participation.

D. BENEFITS
You may not personally benefit from participation, but your input will help shape ethical guidelines and frameworks for AI-driven development practices.

E. CONFIDENTIALITY
Your responses will be anonymous, and no personal information (e.g., name or email) will be collected. Any quoted feedback will be anonymized. All data will be securely stored in OneDrive for five years post-publication, after which it will be destroyed.

F. CONDITIONS OF PARTICIPATION
Participation is voluntary, and you may withdraw at any time by closing your browser. Once submitted, responses cannot be withdrawn due to anonymity.

* 1. By choosing "I give my consent" below, you are indicating that you

- Have read and understand the Consent Form provided to you.
- Consent to participate in the research project.
- Understand that a copy of this consent form is available to you for your records.

Do you give your consent?

○ I give my consent

○ I do not give my consent

Demographic Information

In this section, we invite you to share a few details about your background. Your responses will help us better understand the context behind your experience and perspectives on AI usage.

* 2. Please select your age group.

○ Under 18

○ 18 - 24

○ 25 - 34

○ 35 - 44

○ 45 - 54

○ 55 or above

* 3. To which gender identity do you most identify?

○ Woman

○ Man

○ Transgender Woman

○ Transgender Man

○ Gender Variant/Non-Conforming

○ Prefer Not to Answer

○ Prefer to self-describe (Please specify)

* 4. Which country are you currently living in?

* 5. **NOT including education**, how many years of **professional programming experience** (for example, industry experience, commercial freelancing, or participation in recognized open-source projects) do you have in software development?

○ Less than 1 year

○ 1 - 3 years

○ 4 - 6 years

○ 7 - 10 years

○ More than 10 years

* 6. Which of the following best describes your current role or affiliation in the software industry?

○ Software Engineer / Developer

○ Data / ML Engineer

○ QA / Test Engineer

○ Product / Project Manager

○ Team Lead / Architect

○ Other (please specify)

* 7. What is the size of your organization based on the number of employees?

○ 1–10

○ 11–50

○ 51–200

○ 201–500

○ 501–1000

○ 1001+

○ Not applicable / I am not currently working in an organization

* 8. How frequently do you use LLMs for bug fixing?

○ Always (almost daily)

○ Frequently (a few times per week)

○ Occasionally (a few times per month)

○ Rarely (a few time per year)

○ Never

Policy

The following sections describe high-level summaries of two example policies designed to support responsible and transparent use of AI tools in software bug fixing from a broader perspective. Please read them carefully to have some idea of the content of each policy. You will be asked to reflect on the feasibility, challenges, and your perception of implementing these in a real-world software development environment.

The following definitions are for your understanding to answer the questions in this section.

Disclosure Levels:

- **No Disclosure**: AI usage is never recorded or communicated.
  Example: "I used the LLM to write this patch but didn’t mention it in the commit or docs."
- **Partial Disclosure**: Some details about AI usage are shared, but not fully.
  Example: "I noted that I got help from the LLM but didn’t explain when or how."
- **Full Disclosure**: All relevant details of AI usage are documented and visible.
  Example: "I documented the prompt, response, and rationale in the code comments and repo log."

Human Oversight Levels:

- **No Human Oversight**: AI fixes are used directly without human review.
  Example: "I copied the LLM output and merged it without checking."
- **Partial Human Oversight**: AI fixes are reviewed or tested, but not fully validated.
  Example: "I checked that it runs, but I didn’t have time for code review or security tests."
- **Full Human Oversight**: Fixes go through complete review, testing, and human validation.
  Example: "I reviewed the LLM fix, ran unit tests, and got a teammate to approve it before merging."

* 9. If your organization were to adopt AI tools, what level of *disclosure* would you personally choose when using an LLM for bug fixing?

	No Disclosure	Partial Disclosure	Full Disclosure
LLM Usage Purpose	○	○	○
LLM Code Contribution	○	○	○
LLM Usage Pattern	○	○	○
LLM Usage Restriction	○	○	○
Disclosure Channel	○	○	○
Disclosure Access Level	○	○	○

* 10. What concerns would you face when asked to fully *disclose* LLM involvement?

□ Increased workload- Efficiency/Time constraints

□ Intellectual property risk and security concerns

□ Reputational Impact- May raise doubts about code quality or team competence

□ Loss of control over own work

□ Fear of judgment about AI reliance

□ Legal/IP uncertainty

□ Lack of documentation tools

□ No concerns

□ Other (please specify)

* 11. What implementation challenges or trade-offs do you see between being transparent and staying compliant when following an *AI usage disclosure policy* in low-risk vs. high-risk domains?

[For example, in low-risk domains, full transparency might feel like extra paperwork that slows down delivery, so minimal disclosure may be enough to stay compliant. But in high-risk domains, strict compliance requires more detailed disclosure, which can increase workload and reduce speed, though it provides stronger accountability and trust.]

High-risk Domain (e.g., authentication, encryption, financial systems, healthcare systems, compliance-sensitive areas)

Low-risk Domain (e.g., UI layout, static content, logging and telemetry, internal documentation, non-critical front-end features)

* 12. What personal benefits do you associate with following the *AI usage disclosure* policy?

	Strongly Agree	Agree	Disagree	Strongly Disagree
Disclosing AI usage in my code protects me from being unfairly blamed for bugs later.	○	○	○	○
I believe that documenting AI involvement increases trust in my contributions.	○	○	○	○
Transparency about AI usage improves team collaboration and communication.	○	○	○	○
I would be more likely to disclose LLM usage if it meant earning formal credit or recognition.	○	○	○	○

* 13. What other things would motivate you most to follow the *AI usage disclosure* policy in your day-to-day work?

* 14. Please select 'Neutral' to confirm you are paying attention.

○ Strongly Disagree

○ Disagree

○ Neutral

○ Agree

○ Strongly Agree

* 15. If your organization were to adopt AI tools, what level of *human oversight* would you personally choose when using an LLM for bug fixing?

	No Human Oversight	Partial Human Oversight	Full Human Oversight
Code Verification	○	○	○
Sensitive Data Protection	○	○	○
Security and Automated Testing	○	○	○
Review Responsibility	○	○	○
Credit and Liability Evaluation	○	○	○
Final Decision Ownership	○	○	○

* 16. What concerns would you face when asked to ensure full *human oversight* of LLM-generated bug fixes?

□ Added workload due to mandatory manual review

□ Lack of time or resources to verify every AI-generated change

□ Limited technical understanding of the AI-generated code

□ Uncertainty about who is accountable for mistakes

□ Absence of clear organizational standards for validation

□ Difficulty coordinating review responsibilities within the team

□ Over-reliance on automated tools makes manual oversight redundant

□ No concerns

□ Other (please specify)

* 17. What implementation challenges or trade-offs do you see between speed of delivery and assurance of reliability when following the *AI usage human oversight* policy in both low and high-risk domains?

[For example, in low-risk domains, having a human review every AI-generated bug fix might slow down delivery without adding much value, since the risk of errors is minor. But in high-risk domains, even though oversight reduces speed, it’s necessary to ensure reliability and compliance — so the trade-off is between moving fast and meeting safety or quality standards.]

High-risk Domain (e.g., authentication, encryption, financial systems, healthcare systems, compliance-sensitive areas)

Low-risk Domain (e.g., UI layout, static content, logging and telemetry, internal documentation, non-critical front-end features)

* 18. What personal benefits do you associate with following the *AI usage human oversight* policy?

	Strongly Agree	Agree	Disagree	Strongly Disagree
I feel more confident deploying code that has gone through human oversight, even if it was AI-assisted.	○	○	○	○
Human validation of AI-generated fixes helps me learn and improve my own debugging skills.	○	○	○	○
If oversight is enforced, I feel less personally responsible for future issues in the code.	○	○	○	○
I would get recognition for responsible coding.	○	○	○	○

* 19. What would motivate you most to follow the *AI usage human oversight* policy in your day-to-day work?