GitHub Copilot (AI Assisted Coding) Policy & Governance

Implemented on (date)	22/08/2024
Approved by (name & role)	Head of Software Practices (Fahad Anwar) In consultation with TAG (Technical Advisory Group).
Last review on (date)	
Reviewed by	TAG (Technical Advisory Group)
Next review due on (date)	22/08/2025
Policy owner (name)	Head of Software Practices In consultation with Technical Advisory Group (TAG) representing Software Engineers, CSS / Cloud Division, TISS and Security Division.
Policy owner (division)	Digital Services and Technology (DST)
Main point of contact (name)	Fahad Anwar Software Engineering Head of Practice
Status	Approved

Policy Review Record
This Review Record is to be completed on each time a review is conducted. Its purpose is to maintain a record of reviews, recording who conducted the review (policy owner), the date of the review and the outcome of the review (policy fit for purpose, amendment required, policy no longer required, etc).

This Policy is to be reviewed bi-annually.

Review No	Review Conducted By	Review Date	Review Outcome
01			

Amendment Details

Date	Amendment Summary	Amended by	Version

RASCI (For detail please – RASCI Information document)

Responsible	G6 Program Managers through Technical Leads, G7 and SEO's
Accountable	Head of Software Practices
Supportive	Cloud Services and Support (Amazon, GCP, Azure) SAIM SIRA Software Engineering Community of Practice (SE-CoP)
Consulted	Head of Software Practices (Fahad Anwar) In consultation with Security Team, Head of Innovation & CSS.
Informed	Senior Leadership Team Software Engineering Community SAIM SIRA Design Authority Chair

GitHub Copilot & GitHub Copilot Chat Acceptable Use Policy & Governance

This document outlines the policies and governance framework for the use of GitHub Copilot within ONS (referred to as “the Organisation”).

Scope

Digital Services and Technology and any external parties delivering services into DST (unless by agreement).

Responsibility

The Head of Software Engineering Practice assumes the overall responsibility for the policy on using GitHub Copilot at DST.

Acceptable Use Policy

1. Purpose

This policy aims to:

- Maximise the benefits of GitHub Copilot while mitigating potential risks.
- Promote responsible and ethical use of AI-powered tools.
- Ensure compliance with relevant legal and regulatory requirements.
- Establish clear guidelines for the use of GitHub Copilot within ONS.

2. Key Principles

- **Responsibility:** Users are responsible for the code generated by GitHub Copilot and must review and test it carefully.
- **Transparency:** Users should be aware of the limitations and capabilities of GitHub Copilot.
- **Accuracy:** Users should strive to ensure the accuracy and reliability of the code generated by GitHub Copilot.
- **Security:** Users must prioritise security and adhere to all relevant security policies when using GitHub Copilot.

3. Responsibilities

3.1 GitHub Copilot Service Owner: Responsible for:

- Ensure that all new GitHub users have reviewed this policy and provided their acknowledgment of it (via Service Now request form) before being granted access to GitHub Copilot.
- Ensure adequate training and resources are completed by new GitHub Copilot users before granting access (please see “Training and Awareness” section).
- Ensure the correct GitHub Copilot Policy is implemented to protect the intellectual property rights related to the code generated by GitHub Copilot.
- Ensure that GitHub Copilot enterprise/organisational settings are configured to prevent Copilot Chat from using Bing search results for its responses (please see Using GitHub Copilot Chat in GitHub.com). This is crucial because the process of how context information is transmitted to Bing is not fully understood at the moment.
- Communicate this policy and its updates to all GitHub Copilot users, including ONS employees and contractors.

3.2 Users: Responsible for:

- Adhering to all provisions of this policy.
- Understanding and acknowledging the limitations and capabilities of GitHub Copilot.
- Reviewing and validating all code generated by GitHub Copilot before use.

- Reporting any issues or concerns related to GitHub Copilot to their line manager, who then report to head of software engineering (if required).
- Pull requests comments should clearly mentioned if GitHub Copilot is used to generate the code.

4. Use Cases and Restrictions

4.1 Permitted Use Cases: (this list is not exhaustive)

- **Code Completion and Suggestion:** Generating code snippets and suggestions for various programming tasks.
- **Code Exploration:** Discovering new code patterns and best practices.
- **Learning and Development:** Enhancing coding skills and understanding of programming concepts.
- **Code Conversion:** Converting code from one programming language or framework to another, such as from legacy to modern technology stack.
- **Code Testing:** Writing unit tests, integration tests, and other scripts to ensure the quality and functionality of code.

4.2 Restricted Use Cases:

- No sensitive data should be open within the Integrated Development Environment whilst the GitHub Copilot extension is enabled. e.g. having a temporary tab open where API keys/secrets/production data may be temporarily copy and pasted or inspected is not permitted. This includes the explicit referencing of files/code with such contents via the #file, #workspace and #VSCode chat variable available within GitHub Copilot Chat. The reason for this is that the GitHub Copilot extension can take context from any open file within the IDE, not just the one in focus.
- Using GitHub Copilot for any illegal or harmful activities.

5. Code Review and Validation

- All code generated by GitHub Copilot must be thoroughly reviewed validated before use.
- Users should consider factors like (this list is not exhaustive):
    - **Security:** Identifying potential vulnerabilities and security risks.
    - **Functionality:** Ensuring the code meets the intended requirements and performs correctly.
    - **Non-Functional requirement:** Evaluating the code from non-functional requirements of system such as performance, usability, reliability, and scalability.
    - **Accuracy:** Verifying the code against known best practices and industry standards.

6. Training and Awareness

The user must complete the following training before using the GitHub Copilot

- Generative AI: Introduction
- Introduction to GitHub Copilot (percipio)
- Introduction of using GitHub Copilot responsibly & ethically

7. Monitoring and Enforcement

- GitHub Service Owner must monitor compliance with this policy through regular audits and reviews.
- Any violation of this policy must be addressed in accordance with the ONS disciplinary procedures.

8. Disclaimer

By using GitHub Copilot, employees and contractors acknowledge and agree to comply with all provisions of this policy & IT usage policy.