GitHub Copilot Policy & Governance

ONS AI Assisted Coding Policy

Policy controls	Details
Implementation date (when this first became ONS or UKSA policy)	22/08/2024
Approver name	Fahad Anwar
Approver role	Head of Software Engineering
Board Approval Name	Technical Advisory Group
Last review date	05/03/2025
Next review due date	01/04/2026*
Policy owner name	Fahad Anwar
Policy owner division	Digital Services
Contact email (person or team email)	fahad.anwar@ons.gov.uk
Link to published version of policy (if applicable)	

*: Note that the policy is evolving, and regular reviews of specific sections are carried out in the regular (every other month) bases by the TAG as necessary.

Contents

Policy review record

Details of every review of the policy document

Review number	Reviewer name	Review date	Brief summary of review outcome
01	TAG	05/03/2025	Amendment to the GitHub Usage Policy.

Version history

Details of every change made to the policy document.

SharePoint version no.	Amended by	Version date	Summary of what has changed
1.1	Dom Ford	31/03/25	Updates to section 3, 6 and 7. (See amendments document for details)

1. Policy Statement

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

1.2 The key principles are as follows:

1.2.1 **Responsibility:** Users are responsible for the code generated by GitHub Copilot and must review and test it carefully.

1.2.2 **Transparency:** Users should be aware of the limitations and capabilities of GitHub Copilot.

1.2.3 **Accuracy:** Users should strive to ensure the accuracy and reliability of the code generated by GitHub Copilot.

1.2.4 **Security:** Users must prioritise security and adhere to all relevant security policies when using GitHub Copilot.

2. Scope

2.1 All employees of the UK Statistics Authority and Office for National Statistics.
2.2 Any external parties delivering services into the UK Statistics Authority and Office for National Statistics (unless by agreement)

3. Introduction

3.1 This policy aims to:
3.1.1 Maximise the benefits of GitHub Copilot while mitigating potential risks.
3.1.2 Promote responsible and ethical use of AI-powered tools.
3.1.3 Ensure compliance with relevant legal and regulatory requirements.
3.1.4 Establish clear guidelines for the use of GitHub Copilot within ONS.

4. Background

4.1 The GitHub Copilot Usage Policy is designed to align with the strategic objectives of ONS by promoting the responsible and ethical use of GitHub Copilot. The policy aims to maximise the benefits of GitHub Copilot while mitigating potential risks, ensuring compliance with relevant legal and regulatory requirements, and establishing clear guidelines for its use within ONS

4.2 **Alignment with Business Strategy**:
4.2.1 The policy seeks to leverage GitHub Copilot to enhance productivity, improve coding practices, and support the development of high-quality software within ONS.
4.2.2 By outlining responsibilities and restrictions, the policy aims to minimise potential risks associated with the use of AI-generated code, such as security vulnerabilities and inaccuracies.
4.2.3 The policy encourages users to adhere to ethical standards and best practices when using GitHub Copilot, ensuring that the generated code is reliable and secure.

4.3 **Legal Context**
4.3.1 Compliance with Legal Requirements: The policy ensures that the use of GitHub Copilot complies with all relevant legal requirements, including data protection and intellectual property laws.
4.3.2 The policy mandates that users prioritise security and adhere to all relevant security policies, preventing the exposure of sensitive data and ensuring the protection of intellectual property rights.

4.4 Regulatory Context

4.4.1 The policy aligns with regulatory standards and guidelines applicable to the use of AI-powered tools within the public sector.

4.4.2 The policy establishes a governance framework for the use of GitHub Copilot, including roles and responsibilities, monitoring and enforcement mechanisms, and procedures for reporting and addressing policy breaches.

5. Policy Detail

5.1 Responsibilities

5.1.1 GitHub Copilot Service Owner: Responsible for:

5.1.1.1 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.

5.1.1.2 Ensure adequate training and resources are completed by new GitHub Copilot users before granting access (please see “Training and Awareness” section).

5.1.1.3 Ensure the correct GitHub Copilot Policy is implemented to protect the intellectual property rights related to the code generated by GitHub Copilot.

5.1.1.4 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.

5.1.1.5 Communicate this policy and its updates to all GitHub Copilot users, including ONS employees and contractors.

5.1.2 Users: Responsible for:

5.1.2.1 Adhering to all provisions of this policy.

5.1.2.2 Understanding and acknowledging the limitations and capabilities of GitHub Copilot.

5.1.2.3 Reviewing and validating all code generated by GitHub Copilot before use.

5.1.2.4 Reporting any issues or concerns related to GitHub Copilot to their line manager, who then report to head of software engineering (if required). If the concern constitutes a security incident, follow the reporting set out in Security Incident Reporting Guidance.

5.1.2.5 Pull requests comments should clearly mentioned if GitHub Copilot is used to generate the code.

5.2 Use Cases and Restrictions

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

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

5.2.2 Restricted Use Cases:

5.2.2.1 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.
5.2.2.2 Using GitHub Copilot for any illegal or harmful activities.

5.3 Code Review and Validation

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

5.4 Content Exclusion

5.4.1 Organisational Level Exclusions: GitHub Copilot has undergone full security assurance. However, certain sensitive file types are excluded from analysis at organisation level. As GitHub Copilot is licensed through the organisation, these exclusions apply to any repository where the licensed version of GitHub Copilot is used. The exclusions can be viewed in each repository's settings.

5.4.2 Repository Level Exclusions: Repository Admins can add filetypes to this inherited list as they deem appropriate via their repository settings. They cannot remove filetypes excluded at the organisation level. Documentation on this is available from GitHub here.

5.5 Training and Awareness

5.5.1 The user must complete the mandatory training linked in the Learning Hub before using GitHub Copilot.

5.6 Monitoring and Enforcement

5.6.1 GitHub Service Owner must monitor compliance with this policy through regular audits and reviews.

5.6.2 Level of users GitHub Copilot activity will be monitored and before each billing date. Users with 6 weeks or more of inactivity will have their licences removed. Reinstatement will require the submission of a Service Now request.

6. Breach of Policy

6.1 Failure to comply with the requirements of this policy will be handled through the mechanisms outlined in the ONS Disciplinary Policy (Discipline_Policy.docx (sharepoint.com))

7. Roles and Responsibilities

Individuals who have a role in this policy:

Role	**Responsible for**	**Accountable to**
Fahad Anwar (Head of Software Engineering)	Overall responsibility	Deputy Director

8. Supporting documents

Generative AI Guidelines	[Link]
GitHub Usage policy	[Link]
Source Code Management Policy	[Link]