Source Code Management Policy

ONS Source Code Management Policies

Policy controls	Details
Implementation date (when this first became ONS or UKSA policy)	20/05/2024
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	Technical Advisory Group	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	30/04/25	New points 2 and 3. (See amendments document change SCMP-01 for details)

1. Policy Statement

1.1 This document outlines the policies and governance framework for the use of Source Code Management (SCM) and Version Control Systems (VCS) within ONS (referred to as “the Organisation”).

1.2 The key principles are as follows:

1.2.1 **Responsibility:** Users are responsible for the information they store in SCM and VCS applications and must use them carefully.

1.2.2 **Capability:** Users should be aware of the limitations and capabilities of SCM and VCS applications.

1.2.3 **Security:** Users must prioritise security and adhere to all relevant security policies when using SCM and VCS applications.

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 Establish clear guidelines for the use of SCM and VCS within ONS.
3.1.2 Promote responsible use of SCM and VCS tools.
3.1.3 Ensure compliance with relevant legal and regulatory requirements.
3.1.4 Maximise the benefits of SCM and VCS in ONS while mitigating potential risks.

4. Background

4.1 Source Code Management (SCM) systems or Version Control Systems (VCS) are systems which manage changes to computer programs. They have a set of features that support this activity including version control, rich audit history and multiple streams of change that can co-exist among many others. It is widely accepted best practice that source code should be managed within such a system. This policy specifies the way Digital Services and Technology (DST) utilise Source Code Management.
4.2 The policy is based on guidelines set in the GDS Way “How to store source code”, when using source control, but there are differences which are identified in this document.

4.3 **Alignment with Business Strategy**:
4.3.1 The policy seeks to leverage SCM and VCS to enhance productivity, improve coding practices, and support the development of high-quality software within ONS.
4.3.2 By outlining responsibilities and restrictions, the policy aims to minimise potential risks associated with the use of SCM and VCS, such as security vulnerabilities and inaccuracies.
4.3.3 The policy encourages users to adhere to ethical standards and best practices when using SCM and VCS, ensuring that the managed code is reliable and secure.

4.4 **Legal Context**

4.4.1 The policy ensures that the use of SCM and VCS complies with all relevant legal requirements, including data protection and intellectual property laws.

4.4.2 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.

4.5 **Regulatory Context**:

4.5.1 The policy aligns with regulatory standards and guidelines applicable to the use of version control and collaboration tools within the public sector.

4.5.2 The policy establishes a governance framework for the use of SCM and VCS, including roles and responsibilities, monitoring and enforcement mechanisms, and procedures for reporting and addressing policy breaches.

5. Policy Detail

5.1 All source code must be under source control in one of the ONS recognised source control systems (see section in Appendix for this).

5.2 All source control systems MUST have a system specific usage policy. These policies will set expectations in a system-specific manner and are the place to address features a given system may have.

5.3 Features of a source control system that are not yet generally available ('GA') MUST NOT be used for production workloads. They can be explored for their future utility in line with the ONS Proof of Concept Security Principles.

5.4 No sensitive data shall be kept in source control. This includes secrets, keys, private certificates, passwords.

5.5 Code repositories must be assessed at creation and regularly thereafter to ensure compliance with this policy.

5.6 Repositories must be created public by default unless you have a specific need for them to be more restricted, this is in line with UK Govt guidelines - Be open and use open source.

5.7 Code repositories that are not published openly must have the rationale for doing so recorded prominently within the repository using (PIRR).

5.8 All identities used for access to SCM systems must to be readily attributable to individuals and their organisations.

5.9 Access to code repositories must be on a least privilege basis.

5.10 All user authentication to internet facing SCM systems must utilise multifactor authentication.

5.11 All data exchanged with an SCM system must be protected in transit using encryption.

5.12 Users with contribute access to the ONS recognised source control systems must have completed mandatory training (see source control specific policy, i.e. GitHub Usage Policy etc).

5.13 If an application is no longer used in production and there is no update on the repository for the previous year, the Technical Lead or nominated senior team member should archive the repository, Update the README file accordingly and resolve any open security alerts on the repository.

5.14 Monitoring and Enforcement

5.14.1 G6 Programme Managers through Technical Leads or the senior member of respective software development team are responsible for monitoring and enforcing compliance with this policy, as well as application/system specific child policies.

5.15 Exception process

5.15.1 It is acknowledged that situations arise in which the Policy Detail as above may not be able to be met. Where this is the case a documented policy exception must be sought from the Policy Owner (specified in the table on the title page).

5.16 ONS Recognised Source Control Systems

5.16.1 **GitHub**:

5.16.1.1 For a list of GitHub.com organisations recognised by ONS, please see the GitHub Usage Policy linked in the supporting documents section

5.16.2 **GitLab**:

5.16.2.1 GitLab - General (on premises; available from your laptop/workstation)

5.16.2.2 GitLab - DAP (on premises and only available from a DAP virtual desktop)

5.16.3 If you believe there is a recognised source control system not listed above, please contact policy owner.

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.

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	Chris Penner (Dy Director – Digital Services)

8. Supporting documents

ONS GitHub Usage policy	[Link]
Atlassian – What is Version Control	[Link]
Gov.UK Service Manual – Maintaining Version Control in Coding	[Link]
GDS – How to Store Source Code	[Link]
NCSC – Secure Development and Deployment Guidance	[Link]
CDDO – Security Considerations when Coding in the Open	[Link]