cornerstone

Supplier Artificial Intelligence (AI) Use Policy

Effective Date: 3rd September 2025

1. Purpose

1.1

This document outlines the expectations and obligations of Cornerstone's suppliers, contractors and subcontractors regarding the use of Artificial Intelligence (AI) or Machine Learning (ML) technologies in connection with Cornerstone's data, tools, systems and services. It is intended to:

- Protect Cornerstone's intellectual property.
- Prevent unauthorised use of AI on Cornerstone data.
- Ensure compliance with applicable legislation and standards.
- Ensure that AI use by Cornerstone's suppliers does not expose Cornerstone to reputational, operational, or legal risk.

2. Scope

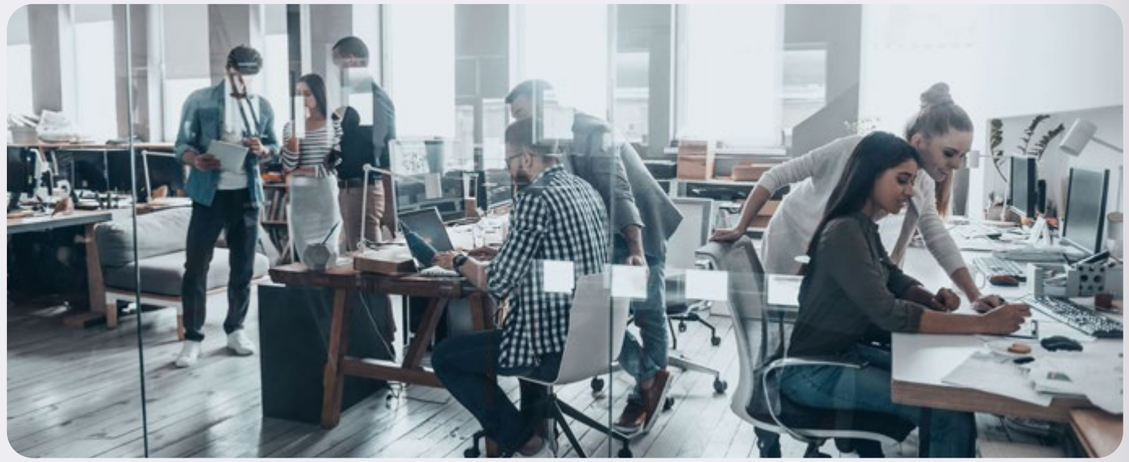
2.1

This document applies to any Cornerstone supplier that:

- Has access to Cornerstone data, systems, or environments.
- Collects, stores, generates, or processes data on behalf of Cornerstone.
- Uses AI or Machine Learning technologies in the delivery of services to Cornerstone.
- Builds, trains, or operates AI models using Cornerstone data.

2.2

This policy applies whether AI services are explicitly marketed as part of the supplier's offering to Cornerstone. It does not apply to suppliers who provide AI tools to Cornerstone for use by Cornerstone, provided those tools do not process Cornerstone data externally or without oversight.



3. Obligations for Suppliers

3.1 GENERAL REQUIREMENTS AND APPLICABILITY

3.1.1

The following obligations apply to all Cornerstone suppliers as described in section 2.

3.1.2

For new suppliers, the obligations must be reviewed, agreed to, and incorporated into the contractual agreement prior to contract execution, and must be adhered to for the duration of the engagement. The obligations will apply in addition to all other terms and conditions.

3.1.3

For existing Cornerstone suppliers, these obligations are intended to apply from the effective date of this policy. However, where existing contractual agreements do not include provisions requiring compliance with updated customer policies, Cornerstone may seek to incorporate this policy through a contract amendment.

3.1.4

These obligations are mandatory, and non-compliance may result in enforcement actions as described in section

3.2 EXPLICIT CONSENT FOR USE OF CORNERSTONE DATA FOR AI PURPOSES

3.2.1

Suppliers are not permitted to use Cornerstone data, or data collected, derived, generated, or processed on behalf of Cornerstone for the purposes of training, re-training, fine tuning, benchmarking, improving, or operating Artificial Intelligence or Machine Learning technologies without the prior written consent from Cornerstone's Information Security Officer. This includes structured data, unstructured data, metadata, logs, communications, user interactions and any data related to the use of Cornerstone systems or services. This restriction applies to all data obtained through the provision of services for Cornerstone, including data generated by supplier systems while operating within Cornerstone's environments.

3.2.2

If a supplier seeks permission from Cornerstone in accordance with 3.1.1, the supplier shall provide Cornerstone with all assistance and information required to perform all required assessments and related due diligence that Cornerstone deems necessary.

3.2.3

Any permission granted by Cornerstone to a supplier in accordance with 3.1.1 is limited to one (1) year, unless otherwise specified in the agreement. Following this period, without a renewal of the permissions, any use of Cornerstone data with Artificial Intelligence or Machine Learning technologies is a breach of this policy and may be subject to enforcement as described in section 4. Consent must be documented and retained for audit purposes.

3.3 GOVERNANCE

3.3.1

Prior to AI deployment a DPIA will be completed by Cornerstone with Supplier input. Suppliers will be asked to assess their use of AI prior to it's deployment or use and should periodically review use following deployment to identify any risks or impacts to Cornerstone and their stakeholders.

3.3.2

If a supplier is using or intends to us AI in the provision of services to Cornerstone, it is required to have an AI governance framework in place with defined policies and procedures. These must comply with relevant legislation and must meet or exceed current best industry standards. Governance frameworks must include human oversight mechanisms, explainability and bias mitigation.

3.3.3

Suppliers must designate a responsible AI officer or equivalent point of contact.

3.4 DATA PROTECTION AND SECURITY

3.4.1

Cornerstone data, or data collected, derived, generated, or processed on behalf of Cornerstone, must not be downloaded, copied, transferred, or shared from the agreed storage location or processing environment for the purposes of AI analysis, model development, or any form of AI/ML experimentation, unless explicitly authorised by Cornerstone as part of the permissions granted in accordance with

3.4.2

This applies to all forms of data movement, including manual extraction, automated pipelines, server mirroring, and API based access.

3.4.3

Where suppliers are authorised to process data in accordance with 3.4.1, they shall ensure that such activities are carried out in compliance with Cornerstone's Information Security and Data Protection Policies and recognised industry best practices.

3.4.4

Any data which is processed using AI tools should be anonymised or pseudonymised where reasonably practicable, in accordance with data protection laws and Cornerstone policies.

3.4.5

Where Cornerstone data is processed, transformed, enriched, or otherwise modified using AI tools, suppliers must maintain a comprehensive data lineage and audit history including timestamps and access logs. This information must be made available to Cornerstone upon request for compliance, audit, or investigation purposes in any requested format.

3.4.6

Suppliers must ensure that no Cornerstone data is used in publicly accessible or shared AI environments.

3.4.7

Suppliers must implement safeguards against data leakage, model inversion and unauthorised or unintended inference. Any instance of data leakage, model inversion or inference which results in exposure of Cornerstone data or sensitive information must be reported to Cornerstone with 48 hours of becoming aware.

3. Obligations for Suppliers (continued)

3.5
LEGAL AND REGULATORY

3.5.1

Suppliers using AI or ML in the provision of services for Cornerstone must comply fully with the EU AI Act and any other applicable data protection and AI regulations.

3.5.2

Suppliers must monitor and comply with evolving AI regulations in all jurisdictions where Cornerstone operates or where Cornerstone data is stored.

3.6
CONTRACTORS

3.6.1

It is the responsibility of the Supplier to ensure that any subcontractor complies with all obligations stated in this policy and all other policies which suppliers are contracted to.

3.6.2

Subcontractors must be contractually bound to comply with this policy.

3.7
AUDITING

3.7.1

Where permission is granted by Cornerstone in accordance with 3.1.1, Cornerstone reserves the right to audit supplier AI practices, data flows, and AI governance frameworks at any time, with reasonable notice.

3.7.2

In addition, Cornerstone reserves the right to initiate an audit where there is reasonable suspicion that a supplier has used AI or Machine Learning technologies in connection with Cornerstone data without appropriate authorisation.

3.7.3

Where an audit is requested, suppliers must provide timely access to relevant documentation, systems, personnel, and environments necessary to conduct the audit. This includes, where applicable, secure access to platforms or interfaces used to delivery services to Cornerstone. Audits may include, but are not limited to, reviews of AI model usage, data processing activities, risk assessments, governance frameworks, and adherence to applicable policies and legislation.

4. Enforcement

4.1
NON-COMPLIANCE

4.1.1

Non-compliance with the obligations listed in this document may result in:

- Termination or suspension of the contract of work.
- Reporting to relevant regulatory authorities.
- Legal action for breach of data protection or AI regulations.

4.2
DAMAGES

4.2.1

Cornerstone may seek indemnification for damages resulting from breach of this policy.

Connecting with you

Hive 2, 1530 Arlington Business Park
Theale, Berkshire, RG7 4SA

www.cornerstone.network

0800 084 3454

cornerstone