

How our AI is governed

Our work is executed by autonomous software. That is unusual enough that you are entitled to ask how it is controlled. This document answers that directly, and tells you where the limits are.

Version 1.0 · Date 20 September 2026 · Status Approved for release — 12 October 2026 · For Clients and advisers

The short version

Who is accountableThe director, personally. There is no one else to blame. Who reviews the workThe director, before anything reaches you Leaves our systemsNo. The processing pipeline has no network access. Every action recordedYes, in a tamper-evident log Acts on its ownNot on anything that matters. See below.

Your data does not leave the machine

This is the most important thing on this page.

The pipeline that reads and structures your documents is deterministic software running on our own hardware. It is not an AI model called over the internet. It contains no network code at all: it cannot send your data anywhere, because it has no mechanism to do so.

We state this plainly because the usual arrangement is the opposite. Most "AI document processing" sends your documents to a third-party model provider, where they may be retained or used for training. Ours does not, and the reason is architectural rather than a matter of policy: there is no code path that could.

A model provider is used for the software that drafts and reviews our own documents and correspondence — the kind of work a person would otherwise do at a keyboard. Client records are not placed into that. The two are kept separate by design, and this is set out in Data processing terms.

The Two-Key protocol

The software can act on its own for research, drafting, analysis and testing. It cannot act on its own for anything that crosses a boundary. Those actions require the director's explicit confirmation, every time:

Gated action	Why it is gated
Sending anything outside our systems	Nothing reaches a third party without a person deciding it should
Deleting or overwriting files	Destruction is deliberate, and recorded
Changing system configuration	The environment is not altered by the software that runs in it

Incurring cost or making commitments	No financial or contractual act is taken autonomously

The gate is not a setting that could be changed by accident. It is the documented rule the software operates under, and its decisions are logged.

The audit record

Every automated action is written to an append-only log. Each entry is cryptographically chained to the one before it, so removing or altering an entry breaks the chain and is detectable.

The log records what was done, when, and by which session. It does not record the contents of your data. Entries that could contain a credential are redacted before being written.

What the software cannot do

It cannot unlock your data. The encrypted storage is opened only by the director typing a passphrase. The software holds no key and no keyfile.

It cannot approve its own boundary-crossing actions. Those require a human at a keyboard.

It cannot change the rules it operates under. The governing documents are version-controlled, and changes are visible.

It cannot spend without limit. Spend is capped at the provider, not merely monitored.

What it will not do, by choice

These are refusals, not technical limitations. They are written into the company's governing charter and are not traded away for a contract:

No military, kinetic or targeting work.

No covert surveillance or deceptive design.

No work that depends on exploiting the people it touches.

No helping anyone evade regulatory scrutiny.

If a request conflicts with those, we decline it. More detail is in What we will not do.

Where the limits are

We would rather you heard this from us than discovered it later.

One person. If the director is unavailable, work stops. There is no team behind this.

No certifications yet. We hold no ISO 27001 or Cyber Essentials certification at this date. We are not going to imply otherwise.

Young company. Incorporated September 2026. The technical record is real; the trading history is short.

Verifying any of this

Ask, and we will show you. The audit log can be produced, the encryption header can be dumped, and the absence of network code in the pipeline can be demonstrated. We would rather be checked than trusted.

Questions to info@inferencesystems.co.uk.

Inference Systems Ltd — registered in Scotland, company number SC903263. Registered office: 116 Peggieshill Road, Ayr, Scotland, KA7 3RA. info@inferencesystems.co.uk