AI Usage Controls for UK Professional Services

Version 1.0 — Published by Klyra Labs

Why This Document Exists

Companies are not yet in a position to fully understand their AI usage. Everything has happened so fast. Legislation cannot move as quickly as innovation and companies are putting themselves in risky positions.

AI is here to stay and its utilisation is becoming fundamental across almost all industries. But how can we ensure we are using it in a way that protects ourselves, our companies and our clients?

This document aims to answer some of these questions and lay the groundwork for compliant AI usage, so that all members of staff within a company can enjoy the benefits that AI provides without the complications of non-compliance and incorrect usage.

Who This Is For

These controls are intended for law firms, accountancies, consultancies, healthcare providers, and other professional services organisations that handle confidential client or commercially sensitive information and are adopting AI tools in day-to-day work.

What We Are Observing in UK Businesses

Most employees are unsure where they stand with AI. Some have been told not to use it. Some have been told not to use it in a certain way. But most are not told about the ramifications of unsafe AI usage.

It is not uncommon to hear about associates pasting full case files into ChatGPT, or receptionists sending emails regarding confidential medical records to Copilot. These acts might seem harmless but the damage can be immense.

For IP-driven industries, risk could look like sending Claude a recipe and asking it to alter measurements, without considering that Anthropic can now see your highly protected recipes.

Time and time again individuals are not seeing the full scope of their actions when utilising AI. And this is not just confined to LLM usage. When giving an AI full access to your emails, or building an automation that links into your company's Notion, have you really considered the power these companies are being given? What would happen if you were audited, or if a client were to see how their personal data was being handled?

The Risks This Creates

The risk does not stop at losing clients. It extends to losing licenses, trust and livelihoods.

Being the person within a company completely responsible for giving up industry-defining secrets is a very real scenario. Without the right processes and guardrails in place, this is very possible.

Companies can lose their competitive edge, give up secrets and lose trust in a matter of prompts.

The current usage of AI has no audit process, no visibility and no accountability. Everyone is doing their best without understanding their framework. There is no training, no policy and no real guidance on how to protect a company and its employees.

The Minimum Controls Every Company Should Have

Every company should have clear policies in place for AI usage. Each LLM has different policy around how it uses the data collected, but the underlying issue remains: companies are relying on this policy rather than their own.

Companies need to get ahead of this and determine for themselves what data gets sent outside of their company. Each employee should be aware of what can be used, what can be said, and how they can make the most of AI within their job role while still protecting themselves and the company.

Every company should have guardrails in place, a clear policy and visibility into their AI usage and how this complies with industry regulation and legislation.

The Klyra AI Usage Controls

Control 1: AI Usage Policy

The company must have a written AI usage policy that all staff are required to read and sign.

Control 2: Staff Training

All staff must receive basic guidance on acceptable and unacceptable uses of AI.

Control 3: Prohibition of Sensitive Data in Public AI Tools

Client data or sensitive company data must not be entered into public AI platforms.

Control 4: Approved AI Tools List

The company must maintain a list of approved AI tools staff are permitted to use, along with general guidelines for how to use them.

Control 5: Personal Account Restriction

Staff must not use personal AI accounts for work-related tasks. Company policy must prohibit sharing work-related information and data with personal AI accounts.

Control 6: Auditability

AI usage within the company must be capable of being reviewed or audited if required.

Control 7: Human Review

AI-generated outputs must be reviewed by a human before being used externally.

Control 8: Third-Party Integrations

Any AI tool connected to email, documents or internal systems must be reviewed for data access implications. The policy of any AI tool must be reviewed internally to ensure everyone is aware of how data is being handled.

Control 9: Responsibility

A designated person within the company must be responsible for AI governance and sign-off on the implementation of any new tools or frameworks.

Control 10: Ongoing Review

AI usage and policies must be reviewed periodically as tools evolve.

How Firms Can Implement These Controls

Company-wide policy is a good place to start. Set clear rules around what information can be sent out and what cannot. Make sure employees are aware that sending company data to personal AI accounts is prohibited.

A SaaS tool that tracks AI usage and provides an audit trail when required.

A dedicated compliance manager within the company who can answer questions and weigh in on the implementation of new tools.