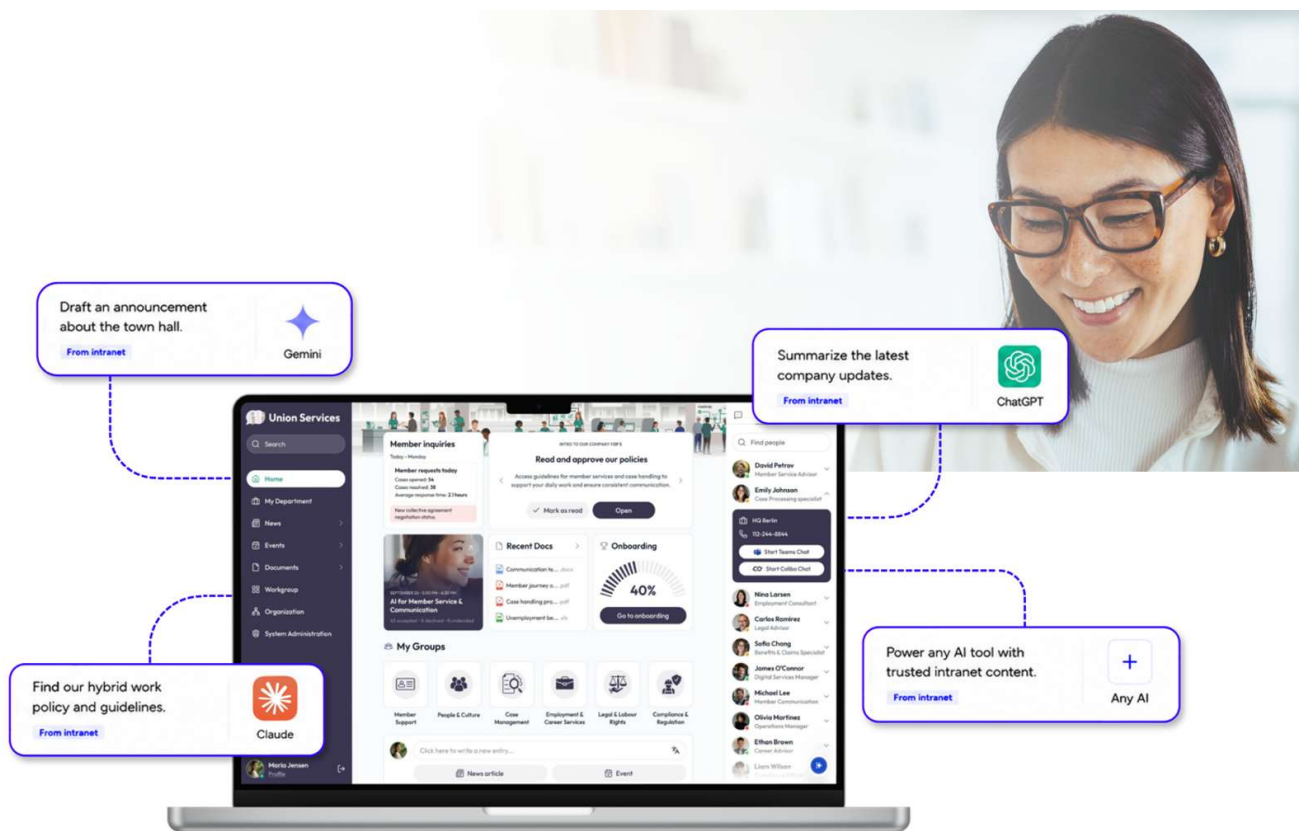


Colibo AI Enabler

Your intranet has the answers. Let your AI use them.

Security and governance without compromise · No AI vendor lock-in · Cloud or On-Prem



About this white paper

This white paper introduces Colibo AI Enabler, a new capability that connects organisations' existing AI tools and their Colibo intranet, in both directions. It is written for two audiences: communications and HR managers who want to understand what becomes possible, and IT and security managers who need to understand how it works and how data is governed.

Chapters 1 to 5 are primarily written for communications and intranet managers. Chapters 6, 7, and 8 address AI platform choice, architecture, and security in detail for IT teams. Chapter 9 covers getting started and pricing.

CHAPTER 01

The knowledge gap

Your organisation's knowledge lives in your intranet. It is stored in policy documents, HR guides, onboarding materials, news articles, and procedure pages, carefully written, maintained, and structured to help employees find what they need.

Your employees' AI tools do not know any of their existence.

Every time a colleague asks their AI assistant about your hybrid work policy, your parental leave entitlements, or the process for submitting an expense claim, they get a generic answer drawn from the open internet. Not your policy. Not your process. A guess.

This is not a failure of AI. It is a gap in integration. The knowledge is there. The AI is capable. The connection is missing.

Two problems, one gap

FOR COMMUNICATIONS AND INTRANET MANAGERS

For communications, HR, and intranet managers, this gap has a tangible cost. When employees cannot find reliable answers from AI tools they are already using, they do one of three things: they email HR or IT directly, they ask a colleague, or they make an assumption. All three outcomes represent a failure of the knowledge infrastructure you have invested in building.

Intranet content goes unread not because it is bad, but because it is invisible to the tools employees increasingly reach for first. Improving search helps. Better navigation helps. But neither solves the problem of AI assistants that operate entirely outside your knowledge base.

FOR IT AND SECURITY MANAGERS

For IT managers, the challenge is different but related. Your organisation has invested in AI tools, whether through a Microsoft licence, a public-sector AI platform, or a third-party subscription. Those tools are approved, contracted, and in use. They are also, in most cases, disconnected from your authoritative internal content.

This means the AI your organisation is paying for operates at a fraction of its potential. It can draft, summarise, and respond, but it cannot draw on the one source of information that makes those capabilities genuinely useful for internal queries: your intranet.

Colibo AI Enabler closes this gap. It gives your organisation's AI tools structured, permission-governed access to your Colibo intranet, without requiring you to change AI providers, compromise your data governance obligations, or rebuild your intranet.

Introducing Colibo AI Enabler

Colibo AI Enabler is an integration layer that connects your organisation's AI tools and your Colibo intranet, in both directions. Its foundation is built on MCP, the Model Context Protocol, an open standard developed for exactly this purpose: connecting AI tools to external data sources and systems in a controlled, structured way.

Colibo AI Enabler does not replace your AI. It does not require a specific AI provider. It does not move your data. It creates a governed pathway between the AI tools your organisation already uses and the knowledge your intranet already holds.

Bring your own AI

Most AI features in intranet and digital workplace platforms come bundled: the vendor provides both the AI and the integration. You use their AI. You accept their terms. You work within their constraints.

Colibo AI Enabler works differently. Your organisation chooses its AI platform, whether that is Claude, Microsoft Copilot, or any other tool your IT team has approved and contracted. Colibo provides the structured connection to your intranet data. The two remain separate. You control both.

This means your data governance obligations remain with the parties you have already contracted. It means you are not locked into a single AI provider as the technology evolves. And it means your organisation retains full flexibility to change, upgrade, or supplement its AI strategy without touching your intranet infrastructure.

What MCP is: in plain language

MCP (Model Context Protocol) is an open standard for connecting AI tools to external services and data sources. Think of it as a structured interpreter: when a user asks their AI a question, MCP enables the AI to request relevant information from connected systems, such as your Colibo intranet, and incorporate it into its response.

MCP is not a Colibo invention. It is an open protocol, which means any AI system that supports it can work with the MCP connector. This is the technical foundation of the AI-agnostic approach described in Chapter 6.

Two components, one product

Colibo AI Enabler consists of a base component and an optional layer.

The MCP connector connects your external AI tools to Colibo. Your organisation can have several connected at the same time, Claude for one team, Microsoft Copilot for another. The AI runs where it always has; the connector gives it governed access to your intranet content. This is the component described in detail in Chapters 5 to 7.

Colibo AI Actions works in the opposite direction. Colibo itself calls one AI provider you nominate and presents the answer inside the intranet, on the page the employee is already reading. This layer is described in Chapter 3.

Organisations can enable either component on its own, or both together, without reconfiguring the other. Nothing in Chapters 5 to 7 depends on AI Actions being enabled.

What changes for the employee

An employee using an AI tool connected to Colibo can ask it questions that it could not previously answer, and get responses that reference, cite, and link to the actual pages and documents in your intranet. They can ask it to draft content based on existing intranet material. They can ask for summaries of recent news, overviews of team pages, or guidance on procedures. The AI works from your content, not the open internet.

Colibo AI Actions

FOR COMMUNICATIONS AND INTRANET MANAGERS

Chapter 2 introduced Colibo AI Actions as the half of Colibo AI Enabler that works in the opposite direction from the MCP connector: instead of your AI tools reaching into Colibo, Colibo brings AI to the page an employee is already on.

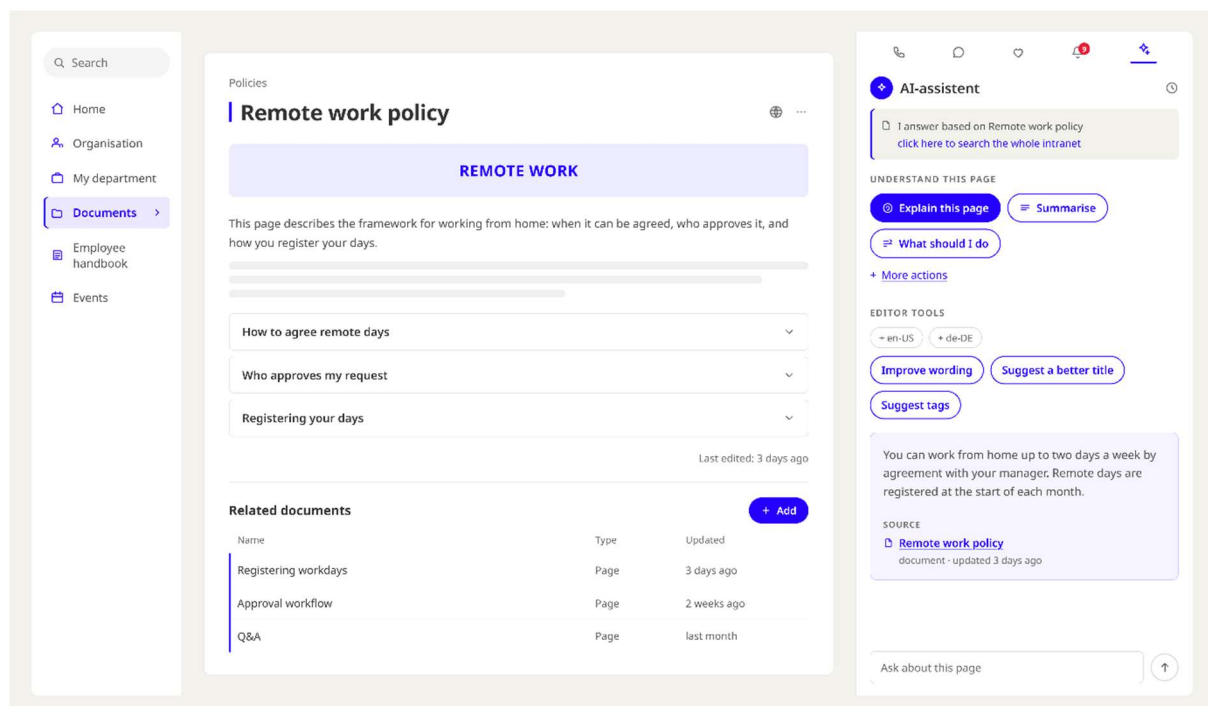
Most employees do not spend their day inside an AI tool. They spend it in the intranet, reading a policy, checking a news post, working through onboarding. Colibo AI Actions meets them there, with the same permission-governed access to your intranet content described throughout this document.

What the employee sees

A panel appears on relevant pages, labelled AI-assistent in the interface by default. The name is configurable per organisation, in the same way theme colours are. It offers a small set of actions written in plain language, so the employee knows what they will get before clicking, explaining the page, summarising it, or asking a free-text question, for example. Exactly which actions appear, and how many, is configurable per organisation and by content type, drawn from a register of actions rather than a fixed list.

The answer appears in the panel, with links to the Colibo pages it drew on. The employee does not switch application, install anything, or hold an AI account of their own.

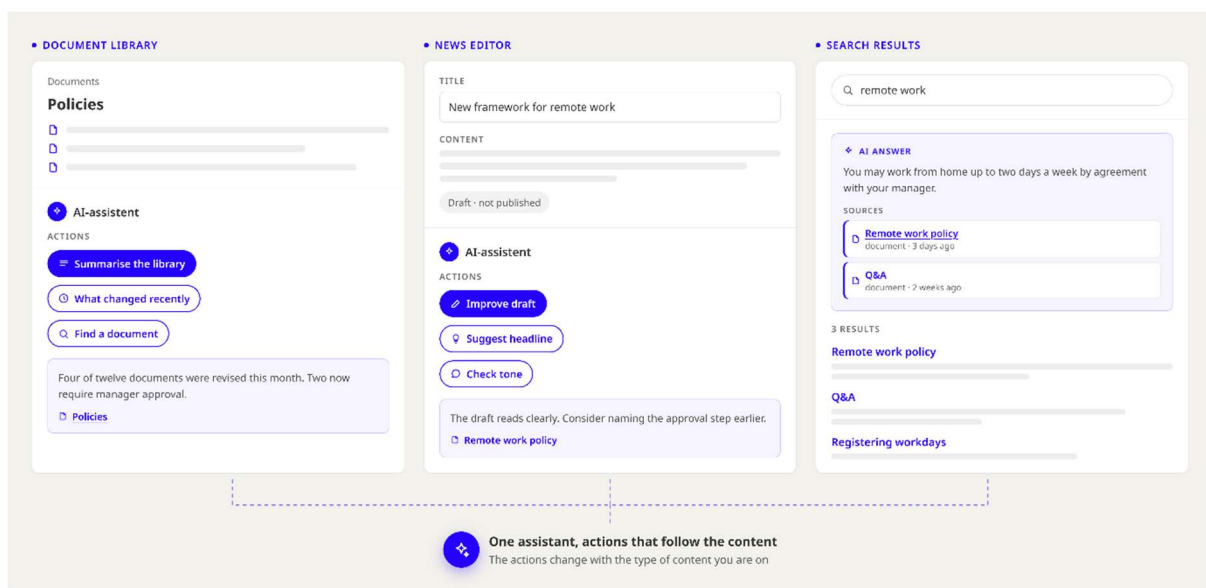
For editors, the same panel surfaces a further set of tools scoped to their role: improving a passage's wording, suggesting a better title, adding tags, or adding a translation, without leaving the page they are already working on.



Actions adapt to the content

The same actions on every page would be a limited use of AI Actions. What is useful on a policy page is not what is useful in a document library or in the news editor, so the actions offered change with the context: a document library might offer to summarise the whole library or flag what has changed recently; a news editor might offer to improve a draft or suggest a headline; a search results page might show an AI answer above the results, with its sources.

Administrators control which actions are available, on which content types, and for which groups. Actions can be disabled individually or switched off entirely.



How it works

When an employee triggers an action, Colibo assembles the relevant context: the page content, its metadata, and related documents the employee is permitted to see, and sends it to your nominated AI provider's API. The response is rendered in the panel.

Content retrieval uses the same mechanism as the MCP connector: every read is performed under the requesting employee's own Colibo credentials. An action cannot surface content the employee could not have opened themselves. The permission model is unchanged, and the AI configuration has no bearing on it.

What it requires

AI Actions requires one addition to the standard MCP connector setup: an API account with an AI provider, held by your organisation, and its key configured in Colibo Admin.

This is a separate arrangement from any AI chat subscription your organisation already has. A Claude Team or ChatGPT Enterprise subscription covers people using those products directly. It does not cover API calls made by another application. The API account is created directly with the provider, and your organisation holds it, including the payment relationship.

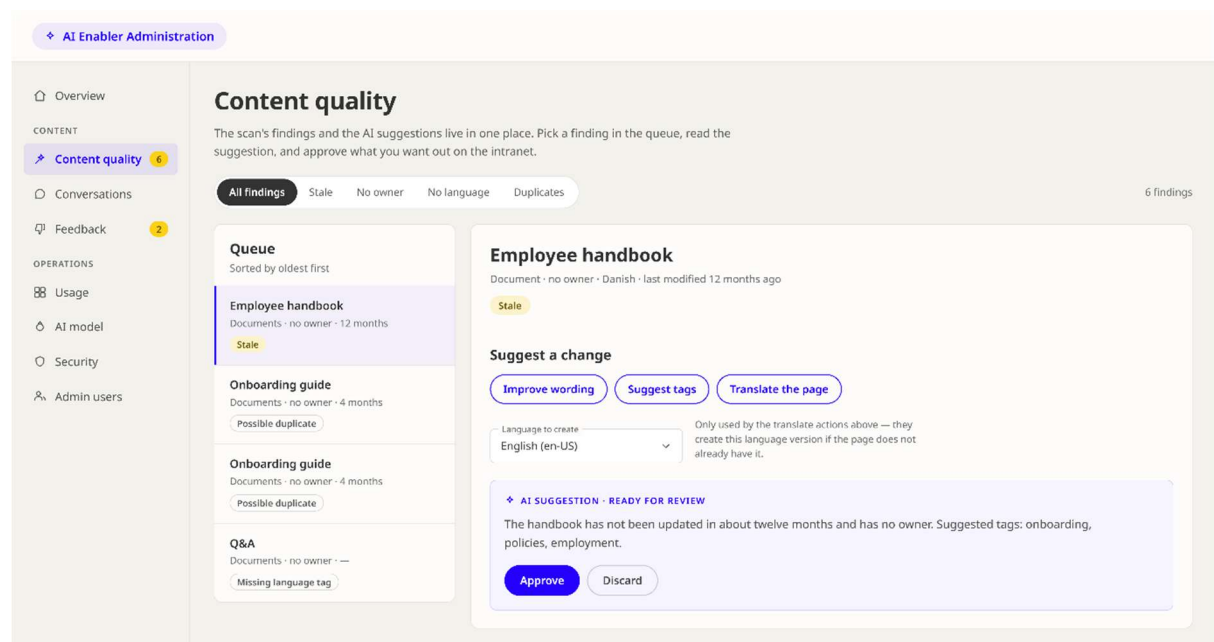
Because the account is yours, the controls are yours as well. Spend limits, usage dashboards, and rate limits are managed in the provider's own console, by your IT team, at whatever level they judge appropriate. Colibo does not resell AI capacity and does not sit between your organisation and your AI provider commercially.

Supported AI providers: Anthropic, OpenAI, and Azure OpenAI.

AI Enabler Administration

Turning AI Actions on for an organisation raises three ordinary questions: is the underlying content actually good enough to answer from, what is it costing, and is it working. AI Enabler Administration is where those questions get answered, as a companion site alongside Colibo itself.

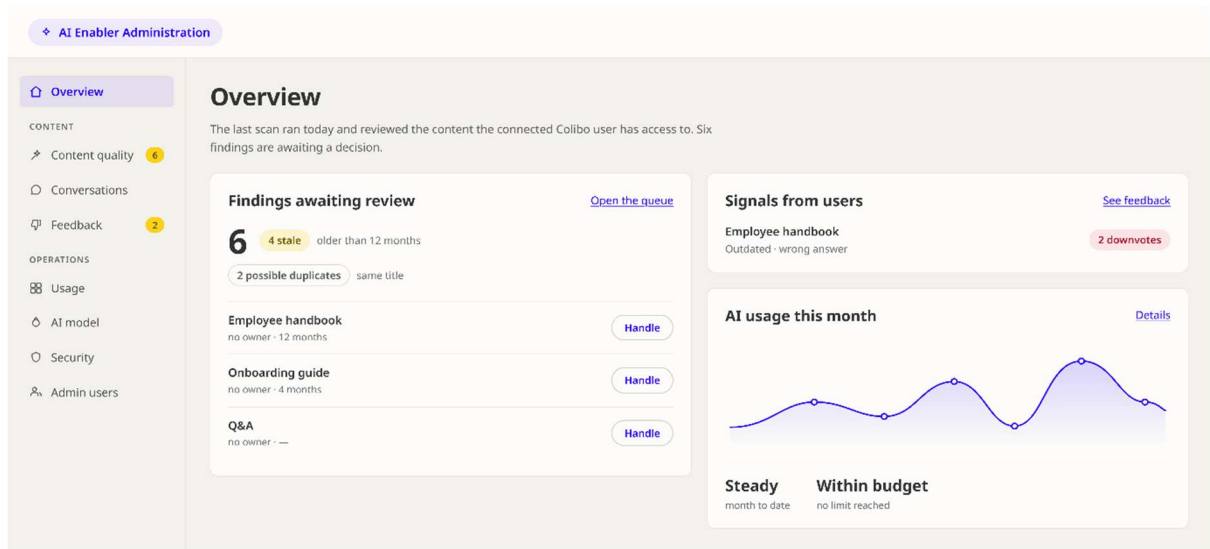
Intranet content ages. Pages lose their owner when someone leaves, policies get duplicated across departments, translations fall behind the original. Administration surfaces exactly that: which pages need attention and why, with an AI-drafted fix ready to review rather than a bare list of problems. Nothing changes on the intranet until an administrator approves it.



Usage and cost are visible in the same place, broken down by what is actually being asked, with the option to set a ceiling so spend cannot climb unnoticed.

When an employee marks an answer as wrong or outdated, that signal is not lost. It lands next to the content it came from, so the person responsible for that page can act on it, closing the loop between a poor answer and a better one.

A single overview ties these together, so an administrator can see what needs attention without hunting across screens.



Starting without it

AI Actions is an optional layer, not a prerequisite. An organisation can deploy the MCP connector, connect the AI tools its teams already use, and get the full value described elsewhere in this document without configuring an AI API account at all.

Adding AI Actions later requires no change to the MCP setup, the permission model, or the Connector Intelligence configuration. It is an addition, not a migration, which means the decision can wait until your organisation has settled which AI provider it wants to build on.

Connector Intelligence: intranet-aware AI behaviour

Connecting an AI to your intranet data is the beginning. A generic AI given access to intranet content will answer questions about it, but it will not know that it should always cite its source, or ask for confirmation before publishing, or escalate employment questions to HR rather than answering directly.

Raw API access and intelligence are not the same thing. Colibo AI Enabler ships with a library of pre-defined AI instructions, behaviours and guardrails designed specifically for how AI should operate in an intranet context. These instructions run as part of Colibo AI Enabler's configuration and shape the AI's behaviour every time it interacts with your Colibo environment.

Colibo calls this capability Connector Intelligence.

What Connector Intelligence includes

Note on how instructions work:

The behaviours described in this section are delivered as AI instructions, guidance provided to the AI model as part of Colibo AI Enabler's configuration. This is different from Colibo's permission-based data access controls, which are enforced at the API level and cannot be bypassed. AI instructions are not a technical guarantee: Colibo cannot ensure that any AI model will follow them in every circumstance, and behaviour may vary between platforms, model versions, or depending on how a question is phrased. Connector Intelligence significantly improves the likelihood of responsible AI behaviour in your intranet context, but it should be understood as governance guidance rather than technical enforcement. For workflows with significant operational consequences, human review remains recommended.

Source attribution

When the AI retrieves information from your intranet to answer a question, it cites the specific document, page, or section it drew from. Employees do not just receive an answer. They receive a link to the source content they can read, verify, and share. This matters for policy questions and HR guidance, where accountability and accuracy are essential.

Where Colibo AI Actions is enabled, source attribution is stronger than an instruction. Because Colibo renders the answer itself, the sources are displayed as actual links to the Colibo pages the answer drew on, together with their last-updated date. The employee can click straight through and verify. This is enforced by the interface rather than requested of the model.

Confirmation before action

Before the AI creates, edits, publishes, or deletes any content through the intranet, it describes exactly what it intends to do and asks for explicit user approval. This applies to drafting news posts, updating documents, activating onboarding notifications, or any other write operation. The user remains in control of every action. Nothing is irreversible without consent.

Scope boundaries

The AI draws on your intranet content when answering internal queries, not the open internet. When an employee asks about a specific company procedure or policy, Colibo AI Enabler ensures the AI references your organisation's actual documentation, not general information that may conflict with or contradict your established rules.

Escalation awareness

For sensitive categories, such as employment disputes, disciplinary matters, legal questions, and confidential compensation topics, the AI recommends that the employee consults the appropriate person or team rather than providing a direct answer. These categories are configurable per organisation and can be aligned with your HR and legal functions' preferences.

Role-based framing

Connector Intelligence can be configured to adapt its behaviour based on the user's role or department. A communications manager's session can be pre-configured to surface content creation and editing tools prominently. An administrator can have analytics and health overview tools available by default. HR managers can have policy citation and escalation behaviours tuned to their workflows.

Customisation

The Connector Intelligence library ships with sensible defaults that work well for most organisations from day one. Customers can adopt the defaults without configuration, extend the library with organisation-specific instructions, or build a fully custom instruction set for their environment.

For customers working with Colibo's implementation team, instruction customisation is part of the onboarding process. This includes reviewing the default behaviours, identifying any organisation-specific rules or escalation paths, and validating the output before go-live.

What this means for your organisation

Connecting AI to intranet data is a starting point, not a finished solution. Without guidance, an AI given access to your content has no way of knowing it should cite its sources, ask before acting, or route sensitive topics to the right people. Connector Intelligence solves this from day one. You get an AI that handles your intranet content responsibly, with behaviours your team can trust and customise, without requiring prompt engineering or specialist AI expertise. The defaults work out of the box. Customisation is available when you need it.

Bring your own AI: chat with Colibo from your own AI tools

FOR COMMUNICATIONS AND INTRANET MANAGERS

Chapter 2 introduced the MCP connector as the other half of Colibo AI Enabler: instead of AI appearing inside Colibo, your organisation's own AI tools reach into Colibo. The following scenarios illustrate how that works in practice, drawn from the capabilities demonstrated during the development and testing of the connector. The specifics, names, content, and results, are illustrative. They reflect the types of tasks the connector enables, not a particular customer's data.

Scenario 1: Employee self-service for policy queries

Situation: An employee working remotely wants to know whether they are entitled to an ergonomic equipment allowance under company policy. Previously they would search the intranet, possibly not find the right page, and email HR.

With the MCP connector: The employee asks their AI assistant: "What is the company's policy on home office equipment?" The MCP connector retrieves the relevant section from the HR policy document in Colibo. The AI responds with a clear summary and a direct link to the source page. The employee has their answer in seconds. HR receives one fewer email.

Outcome: Faster resolution for employees. Reduced volume of repetitive HR queries. Increased relevance and visibility of intranet content.

Scenario 2: Intranet health and content oversight

Situation: An intranet manager wants to understand which topics employees are searching for but not finding, and which pages in the knowledge base are outdated or contain unreliable content.

With the MCP connector: The intranet manager asks their AI: "Which topics do employees search for most often that we have no guide for?" and "Which pages haven't been updated in the last six months?" The MCP connector retrieves document metadata and search data from Colibo. The AI returns a prioritised list of content gaps and a list of stale pages, each with a direct link to the relevant page in Colibo.

Outcome: A structured content action list that previously required manual review across hundreds of pages. The manager can act immediately on the highest-priority gaps.

Scenario 3: Onboarding activation

Situation: An onboarding administrator identifies that a significant proportion of new employees have not started or completed the onboarding module on the platform. Manually identifying and contacting each one is time-consuming.

With the MCP connector: The administrator asks their AI to identify which users have not started the onboarding module, draft a personalised activation message, and send it via the platform's

notification system. The MCP connector retrieves completion data from Colibo's onboarding API, the AI drafts the message, and then, in line with the Connector Intelligence confirmation behaviour, asks the administrator to review the draft and confirm before sending.

Outcome: A targeted re-engagement action completed in minutes. The administrator reviews and approves the output; the AI handles the execution.

Scenario 4: Content drafting with intranet context

Situation: A communications manager needs to draft a news article about a new flexible working arrangement. The article should reference the existing hybrid work policy and link to the relevant HR section.

With the MCP connector: The manager asks their AI to draft a news post about the new arrangement, referencing the hybrid work policy. The MCP connector retrieves the policy content. The AI drafts the article with accurate references and inline links to the policy pages. Before publishing, it presents the draft to the manager, explains what it proposes to post, and waits for explicit approval.

Outcome: Consistent, policy-accurate communications with significantly less manual effort. The manager's role shifts from drafting to reviewing and approving.

AI-agnostic by design

Your organisation does not have to make one AI decision about Colibo AI Enabler. It can make two, independently.

- **Want your team's own AI tools to read your intranet?** Connect Claude, Microsoft Copilot, ChatGPT, or another MCP-compatible AI through the MCP connector.
- **Want AI answers to appear inside Colibo itself, on the page an employee is already reading?** Enable AI Actions with the AI provider your organisation nominates.
- **Want both?** They do not have to run on the same provider.

One of the most significant decisions an organisation makes about AI is which platform to use. That decision involves procurement, data processing agreements, user training, and internal governance. It should not be made permanent by an intranet vendor.

The MCP connector is built on the Model Context Protocol, an open standard, not a proprietary technology. Any AI system that supports MCP can connect to Colibo through the same integration. This means your choice of AI platform remains yours to make, change, and revisit as the technology evolves.

Supported platforms

The MCP connector's architecture is designed to support any MCP-compatible platform.

The MCP connector is available out-of-the-box for:

- Claude (Anthropic): available for Cloud and API deployments
- Microsoft Copilot: for organisations with M365 deployments seeking a complementary intranet intelligence layer
- ChatGPT (OpenAI): for organisations with existing OpenAI Enterprise agreements

Integration with additional AI systems will require additional minor configuration:

- Any MCP-compatible LLM: the open protocol means any AI system with MCP support can be connected

Two different provider choices

The two components of Colibo AI Enabler make different demands on provider choice, and it is worth understanding the asymmetry before planning your setup.

The MCP connector supports several AI platforms simultaneously. Different teams can use different tools against the same Colibo environment, and adding another connected platform does not affect the ones already in place.

Colibo AI Actions uses one AI provider at a time. Because Colibo makes the API call itself, a single provider is nominated in Colibo Admin. It can be changed later, but it is one choice rather than several running in parallel.

The two choices are independent. An organisation can connect Claude and Microsoft Copilot through MCP while running AI Actions on Azure OpenAI, if that is what their agreements and infrastructure suit best.

A note on Microsoft: Microsoft 365 Copilot connects to Colibo through MCP. For AI Actions, where Colibo needs to call a chat completions API directly, the Microsoft service used is Azure OpenAI. Organisations with Microsoft agreements typically have access to both.

Changing your AI platform

As new AI platforms emerge and existing ones evolve, organisations will want flexibility to adapt. Because the MCP connector is protocol-based rather than platform-specific, switching from one supported AI to another does not require changes to your Colibo configuration. The intranet integration, the permission model, and the Connector Intelligence behaviours described in Chapter 4 are all maintained at the Colibo layer, independent of which AI sits on top.

This is a meaningful practical benefit: the investment your organisation makes in configuring and optimising the connection to your intranet is not tied to any single AI vendor's roadmap.

How it works: architecture

PRIMARYLY FOR IT AND SECURITY MANAGERS

Understanding the architecture of the MCP connector matters for two reasons: it clarifies what is technically possible, and it forms the basis of the security and governance model described in Chapter 8.

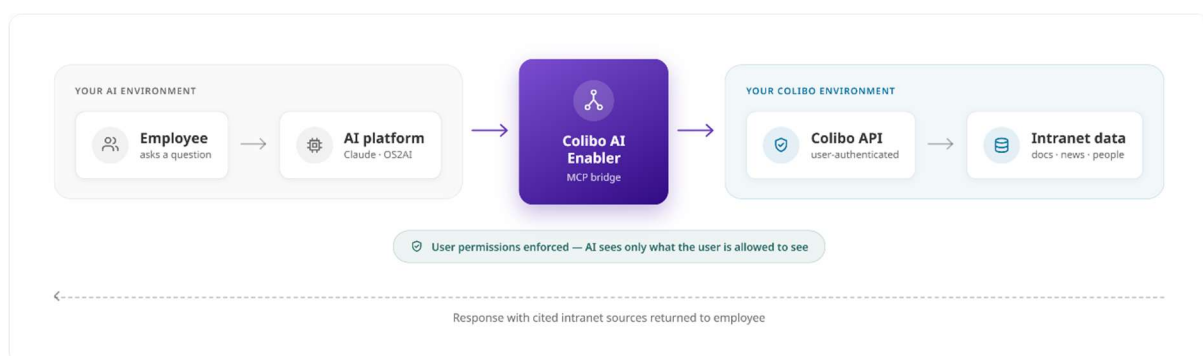
The two-environment model

The MCP connector operates across two distinct environments that remain separate throughout every interaction.

The first is your AI environment, the platform your organisation uses for AI processing. This is where the user interacts, where prompts are processed, and where responses are generated. This environment is under your AI provider's infrastructure and your organisation's data processing agreement with them.

The second is your Colibo environment, your intranet and the data it contains. This is where documents, news, employee directories, and structured content live. Access to this environment is governed by Colibo's existing permission model: every user can only access content they are authorised to see.

The MCP connector sits between them. When a user's AI needs information from your intranet, the MCP connector translates that request into a Colibo API call, retrieves the relevant data under the requesting user's authentication credentials, and returns it to the AI environment in structured form. The two environments exchange information through this bridge, but they remain separate.



The diagram above illustrates the two-environment model. The employee's AI platform sits entirely within the customer's AI environment (left). The MCP connector acts as the bridge between the two environments. All Colibo data access occurs through the Colibo API on the right, authenticated under the requesting user's credentials.

Authentication and permission enforcement

Every request the MCP connector makes to the Colibo API is authenticated using the requesting user's credentials. This means the MCP connector does not have a single privileged access key that bypasses your permission structure. It operates as that user, with that user's permissions. Nothing more.

If a user is not permitted to view a document in Colibo, their AI tool cannot retrieve it through the MCP connector. The permission model you have configured in Colibo applies fully to AI-mediated access. Sensitive content remains sensitive, regardless of how it is requested.

Security and data governance

PRIMARYLY FOR IT AND SECURITY MANAGERS

Security and governance are not features of Colibo AI Enabler. They are the architecture. This chapter explains the model in detail, addresses the questions IT and legal teams will ask, and is honest about what requires organisational confirmation.

Who processes what

The most important question in any AI integration is: where does data go, and who processes it? The answer differs slightly between the two components, and it is worth being precise about both.

With MCP connections

Colibo provides structured, authenticated access to intranet content. Your AI tool requests what it needs. Colibo returns it under the requesting user's permissions. The AI processes the request and generates its response entirely within your AI provider's environment. Colibo does not receive, process, or store the AI's prompts or responses.

With Colibo AI Actions

The flow is different, and the difference matters. When an employee triggers an action, Colibo assembles the relevant context from your intranet and calls your nominated AI provider's API using the credentials you have configured in Colibo Admin. Intranet content therefore passes through Colibo in transit as part of constructing the request.

Colibo stores prompts and responses from AI Actions, anonymised, so that administrators can review and act on them through AI Enabler Administration. This is covered by Colibo's standard data processing agreement, which already addresses Colibo's handling of user-generated content that may contain personal data. The AI processing itself takes place in your AI provider's environment, under the account your organisation owns and the agreement your organisation holds with that provider. What changes compared with MCP is that Colibo is the party transmitting the content, rather than responding to a request the AI initiated, and that Colibo retains an anonymised copy for administration.

For organisations whose data governance framework distinguishes between these two patterns, this distinction should be reviewed with your data protection function before enabling AI Actions.

User-level authorisation

Every content retrieval made through Colibo AI Enabler is executed under the requesting user's Colibo identity. Colibo AI Enabler cannot grant access to content the user is not permitted to view. Groups, departments, and content permission structures configured in Colibo apply in full to AI-mediated queries.

This means an employee in Finance who asks their AI to find a document from the Executive team's private workspace will receive the same response they would receive if they searched manually: no content is returned for documents they are not authorised to access.

Compliance certifications

Colibo holds the following certifications, applicable to the platform and its integrations:

- **ISO 27001** Information security management. Colibo's processes for managing information security risks meet international standards.
- **ISAE 3000** Independent assurance on Colibo's information security and data processing practices.
- **GDPR** Colibo operates in full compliance with the General Data Protection Regulation as a data processor under customer agreements.

Deployment options

Cloud deployment: The standard configuration. The MCP connector is hosted by Colibo, and all Colibo data access occurs through standard API calls over encrypted connections.

On-premises deployment: For organisations that require complete data sovereignty or operate in environments that prohibit cloud-hosted integration components, an on-premises deployment option is available. This places the MCP connector within the customer's own infrastructure.

Getting started

Requirements

Colibo AI Enabler requires the following:

- **An active Colibo subscription.** Colibo AI Enabler is available as an add-on to any current Colibo plan.
- **An approved AI platform with MCP support.** Your organisation must have an active subscription to an AI platform supporting MCP.
- **IT sign-off on the integration architecture.** The MCP connector establishes an authenticated API connection between your AI environment and your Colibo instance. Your IT team will need to review and approve the connection model, particularly for on-premises deployments.
- **An AI API account, needed only if you enable AI Actions.** AI Actions additionally requires an API account with a supported AI provider, held by your organisation, with its key configured in Colibo Admin. This is not required for the MCP connector and can be added at any time. See Chapter 3.

What the setup process involves

Onboarding is handled by Colibo's implementation team and follows a structured three-step process.

- **Technical configuration.** The MCP connector is deployed and authenticated against your Colibo environment. API access is validated.
- **Connector Intelligence configuration.** Default AI behaviours are reviewed with your team. Organisation-specific instructions, escalation categories, and role-based framing are configured and tested.
- **User acceptance testing and handover.** A structured UAT session confirms Colibo AI Enabler behaves as expected across key use cases.

Pricing

Colibo AI Enabler is available on three tiers. All tiers include the MCP connector, the default Connector Intelligence library, and a one-time onboarding and setup service.

Price (monthly)	1-499 employees: €200/month 500-999 employees: €300/month 1,000-4,999 employees: €400/month 5,000 and more employees: Contact Colibo
Deployment	Colibo Cloud or On-Prem
MCP connector	Included
Connector Intelligence library	Default behaviours - Customization on demand / hourly rate
AI platforms	1 platform included – more AI platforms can be added / hourly rate
Setup / onboarding fee	Colibo Cloud EUR 2.000 – On-Prem: EUR 3.000

All prices are exclusive of VAT. To discuss your requirements or request a demonstration, contact your Colibo account manager or visit colibo.com.

About Colibo

Colibo is a digital workplace platform that unifies communication, knowledge sharing, and collaboration across organisations. With customers across the private and public sector in Europe, including municipalities, public institutions, and enterprises, Colibo provides the intranet infrastructure that connects employees to their organisation's knowledge, tools, and people.

Colibo is headquartered in Aarhus, Denmark, and holds ISO 27001 and ISAE 3000 certifications. The platform is available as a cloud-hosted or on-premises solution and integrates natively with Microsoft 365.

colibo.com · marketplace.colibo.com