

AI Guardrails, in plain words

For reps and account managers. Use it to explain the service to a municipal buyer in under two minutes.

What it is

Before a town switches on an AI assistant such as Microsoft 365 Copilot, Harbourline checks who can see what, locks down the files the assistant should never surface and sets simple rules for staff. The assistant then works only with information each person is already allowed to open.

THE ONE-LINE VERSION

We make sure your AI can't show anyone a file they shouldn't see.

Why it matters to the buyer

No surprise disclosures

An AI assistant can surface any file a person can open, including old HR folders shared too widely years ago. We find and close those gaps first.

A clear answer for council and auditors

A one-page AI use policy and a monthly report on what the assistant can reach and who uses it.

Faster, safer adoption

Staff get approved tools and plain rules, so they use AI with confidence instead of avoiding it or working around IT.

How it works

1

Access check

Map shared folders, permissions and old sharing links across the town's files.

2

Clean-up

Remove oversharing and label sensitive files so the assistant leaves them out.

3

Rules and training

A one-page AI use policy and a 30-minute session for staff.

4

Monitor and report

A monthly plain-language report on access and use, ready for council.

Say this, not this

INSTEAD OF THE TECHNICAL TERM	SAY
"We remediate oversharing and apply sensitivity labels."	"We make sure the AI can't show anyone a file they shouldn't see."
"Data loss prevention policies."	"Rules that stop confidential files leaving by mistake."
"Tenant readiness assessment."	"A check of your system before you switch AI on."
"Least-privilege access model."	"Everyone sees what they need for their job, and nothing more."

Who cares, and why

- **CAO or city manager:** risk to the town's reputation and to council's trust.
- **Clerk and records:** confidential records and privacy requests.
- **Finance:** payroll and vendor files that must stay private.
- **IT manager:** a clean starting point and fewer access tickets.

Listen for

- "Staff are already trying ChatGPT."
- "Council asked us about AI."
- A planned Copilot rollout or licence renewal.
- A recent privacy complaint or audit finding.

CLOSE WITH "Before you switch AI on, can we run a two-week access check and show you what it would see?"

Leave behind: this explainer and the AI Guardrails seller FAQ.