

For an employee requesting approval to use PurposeMapped as an individual productivity tool. Pair with the **Security & Data-Handling Brief**.

Summary for your approver

Question	Answer
What is it?	A private AI assistant on a server dedicated to one user (not a multi-tenant app).
Where does my data live?	On my own dedicated AWS instance (encrypted at rest), not in a shared vendor cloud.
Do AI vendors train on it?	No — requests go through commercial API terms (no training by default; retention per the Brief §4).
Can my employer's data be exposed?	Only what I choose to put in. I will follow my company's AI-use policy on what not to share.
Who pays / owns?	I do (individual subscription). Export Everything lets me take or delete my data.
Can PurposeMapped staff read it?	Policy: no; support is consent-based. A user-visible Access Ledger is planned for Q4 2026 (see Brief §7).

My declaration

- I will use PurposeMapped for my own work productivity, consistent with my employer's acceptable-use and AI policies.
- I will not enter data classified by my employer as restricted/prohibited for external AI tools, per our policy's "when not to use AI" rules.
- I understand the instance is mine; I am responsible for what I choose to share with it.
- I will report any security concern to my IT team and to support@purposemapped.com.

Use boundaries I will observe

Allowed (typical)	Not without approval
Drafting, summarizing, planning, personal task management, public/non-sensitive research	Client-confidential records, regulated data (PII/PHI/financial) unless policy permits, credentials/secrets

Employee name / signature / date

IT / Compliance approver / date

