



# Personal AI assistant

A practical guide to building a supervised personal AI assistant for repeated knowledge work.

WORKS WITH THE ASSISTANTS TEAMS ALREADY USE



EDITION 25 / EMBER & MINT

EXECUTIVE WORKING EDITION - 08 OCT 2026

# 25

## AT A GLANCE

A practical guide to building a supervised personal AI assistant for repeated knowledge work.



A personal AI assistant is not a product you install. It is a set of habits, context files, standing instructions and routines that make a general AI tool behave like a reliable junior colleague for your own work. This playbook shows how to build one: choose the right tasks, assemble context packs, write standing instructions, design routines, handle memory and privacy, and keep a review habit that catches errors. It also states the limits plainly, so you know what to keep for yourself.

### WHO IT IS FOR

Managers, consultants, analysts, founders, lawyers, marketers and other professionals who do repeated knowledge work and want a dependable personal setup, plus the leaders who support them.

### TIME TO USE

60 minutes to read; a weekend afternoon to build a first version



## What you will have at the end

- A shortlist of recurring tasks suited to assistance
- A first context pack and set of standing instructions you can reuse
- Three routines with a clear review step
- A personal privacy and memory policy that fits your employer's rules

## Contents

|           |                                                        |    |
|-----------|--------------------------------------------------------|----|
| <b>01</b> | What a supervised personal assistant is                | 03 |
| <b>02</b> | Where a personal assistant helps and where it does not | 04 |
| <b>03</b> | How the pieces work together                           | 06 |
| <b>04</b> | Routines you can run every week                        | 07 |
| <b>05</b> | Memory, privacy and accuracy controls                  | 09 |
| <b>06</b> | Knowing whether it is working                          | 11 |
| <b>07</b> | Build your first version in an afternoon               | 12 |
| <b>08</b> | Pitfalls, limits and an illustrative scenario          | 14 |
| <b>09</b> | Questions to ask before you commit to a tool           | 16 |
| <b>10</b> | A first quarter that produces evidence                 | 17 |
| <b>11</b> | Terms used in this publication                         | 18 |



## EXECUTIVE BRIEF

# What a supervised personal assistant is

01



The aim is a repeatable working arrangement: the assistant prepares, drafts and checks, and you decide and sign.

Most professionals start with AI by asking one-off questions. The results are uneven because every conversation begins from nothing. A personal assistant setup fixes that by giving the tool stable context about your role, your preferences, your standards and your recurring tasks. Over a few weeks you stop writing long prompts and start running short, reliable routines: prepare me for tomorrow's meeting, draft the weekly update from these notes, check this document against my checklist.

The word supervised matters. A good assistant makes you faster at preparation and first drafts, and it is only as good as your review. It can invent facts, misread tone, miss what is not on the page and say things with confidence it has not earned. Treat it like a capable new colleague who is quick and eager, has no memory of last week unless you provide it, and must be checked before anything goes out under your name.

- Context pack: the background the assistant needs about you, your work and your standards
- Standing instructions: rules for tone, format, sources and what to flag
- Routines: repeatable tasks with a defined input, output and review step
- Memory and privacy rules: what is stored, where, and for how long
- Review habits: quick checks that catch the predictable errors
- Limits: the tasks you keep for yourself

**START SMALL**

Pick two or three tasks you repeat weekly and dislike. Build the setup for those. Add more only after a month of honest use. A small reliable assistant beats a large neglected one.



This playbook is written for individuals but also works as guidance for teams that want consistent practice. It assumes you use tools approved by your employer for any work content.

If you are self-employed, the same discipline applies to your clients' information.

## WORKING QUESTION

Which three tasks do you repeat every week where the first draft or preparation is the part you least enjoy?

## WHERE IT FITS

Where a personal assistant helps and where it does not

02

It is strongest on preparation, drafting, structuring and checking. It is weakest on judgment, relationships and anything that depends on facts it cannot see.

| TASK TYPE                                                           | FIT                     | REASON                                                      |
|---------------------------------------------------------------------|-------------------------|-------------------------------------------------------------|
| Meeting preparation and briefing notes                              | Strong                  | Pulls material together; you verify the facts that matter   |
| First drafts of emails, memos, updates                              | Strong                  | Speeds writing; you set tone and decide content             |
| Summarizing long documents or threads                               | Strong with spot checks | Saves reading time; may omit or distort details             |
| Research planning and source comparison                             | Moderate to strong      | Helps structure questions; verify claims in primary sources |
| Checking your draft against a checklist                             | Strong                  | Consistent second pair of eyes                              |
| Analysis of numbers in spreadsheet                                  | Moderate                | Use tools that calculate; verify results independently      |
| Sensitive conversations, performance feedback, negotiation strategy | Weak                    | Needs your judgment and knowledge of the people             |

| TASK TYPE                               | FIT               | REASON                                    |
|-----------------------------------------|-------------------|-------------------------------------------|
| Legal, medical, tax or financial advice | Not a replacement | Use qualified professionals for decisions |



## A simple sorting test

- Is the task repeated often enough to justify a routine?
- Can I check the output quickly against something I trust?
- Is the information I will share allowed to go into this tool?
- What is the cost if the output is wrong and I miss it?
- Does the task depend on relationships or context that I only hold in my head?

Tasks with a high answer to repetition and checkability, and a low cost of error, are your best starting points. Tasks with a high cost of error need a stricter review or should stay with you. A useful distinction is between preparation and decision. Let the assistant prepare; keep the decision. Even for preparation, think about whose information goes in and who sees the output.



### COMMON MISTAKE

Using the assistant to produce finished work for audiences who matter, without reading it closely. Clients and colleagues can tell, and the errors are yours.

### WORKING QUESTION

Of your recurring tasks, which have a quick way to check the output and a low cost if a mistake slips through?



## HOW IT WORKS

# How the pieces work together

03

A general model becomes a personal assistant through the context you give it, the instructions you set and the routines you run.

AI models respond to what is in front of them: your message, any documents you attach and any stored instructions or memory the tool provides. They do not know your clients, your organization or your priorities unless you supply them. They also have a limit on how much they can consider at once, so long, messy context can dilute results. Short, well-organized context usually beats a dump of everything.

## Context packs

A context pack is a small set of documents you keep and reuse. Keep each to one or two pages and write them in plain language. Update them when things change. Packs may be stored as files you attach, as project instructions in your tool, or as notes you paste. Do not include confidential material that your policy does not allow.

| PACK                 | WHAT IT CONTAINS                                                          | UPDATE WHEN                     |
|----------------------|---------------------------------------------------------------------------|---------------------------------|
| About me and my role | Responsibilities, audience, priorities, constraints                       | Role or priorities change       |
| Style guide          | Tone, preferred structures, words to use and avoid, examples of good work | You see repeated style errors   |
| Domain notes         | Key terms, definitions, standards and sources you rely on                 | Standards or terminology change |
| Project brief        | Goal, stakeholders, status, decisions made, open questions                | Weekly or at milestones         |
| Checklists           | Your quality checks for emails, reports, proposals                        | Mistakes reveal a gap           |

## Standing instructions

Standing instructions are the rules you want applied every time. Write them as short, testable statements rather than vague wishes. Good examples: 'Use US spelling and plain business English.' 'Give the answer first, then the reasoning.' 'If you are not sure, say so and say what would confirm it.' 'Never invent a quotation, statistic, citation or name; mark missing information as unknown.' 'List the assumptions you made at the end.'



## 01 Write

Draft eight to twelve standing instructions covering tone, format, honesty about uncertainty and what to flag.

## 02 Test

Run five typical tasks and see where the output ignores or misreads the rules.

## 03 Tighten

Rewrite unclear rules as specific ones. Remove those that never matter.

## 04 Version

Keep a dated copy so you can see what changed when quality shifts.



### WORKING QUESTION

If a colleague read your standing instructions, would they know how you want work done and what you never want?

### OPERATING MODEL

Routines you can run every week

04



A routine has a trigger, an input, an output format and a review step. Writing it down makes it repeatable and easy to improve.



A routine turns a good prompt into an operating habit. It takes five minutes to define and saves repeated explanation. Store routines as short documents or saved prompts, and give each one a name you can recall. Where your tool supports scheduled tasks or connected calendars, use them cautiously: the more the assistant touches live systems, the more careful the

permissions need to be.

| ROUTINE           | INPUT                                 | OUTPUT                                   | YOUR REVIEW                             |
|-------------------|---------------------------------------|------------------------------------------|-----------------------------------------|
| Morning brief     | Calendar, key documents, open actions | One page: meetings, prep needs, risks    | Check names, times, facts               |
| Meeting prep      | Agenda, past notes, attendee list     | Briefing with questions to ask           | Verify claims, adjust tone              |
| Weekly update     | Your notes and ticket list            | Draft update in house format             | Confirm accuracy, add judgment          |
| Reading digest    | Articles or reports you supply        | Summary with points that matter to you   | Spot check against source               |
| Draft review      | Your draft and checklist              | List of gaps, unclear lines, tone issues | Decide which to accept                  |
| Follow-up capture | Meeting notes or transcript           | Actions, owners, dates                   | Confirm with attendees where it matters |

## EXAMPLE, ILLUSTRATIVE

A consultant pastes rough notes after each client call into a 'call capture' routine. The assistant returns decisions, actions, owners and open questions in a fixed format. She checks it against her memory in two minutes and sends it the same day.

## Anatomy of a good routine

- Trigger: when do I run this, and what do I need ready?
- Inputs: exactly which files or notes, and which are off limits
- Instruction: the standing prompt, kept short and versioned
- Output: the format, length and sections I want back
- Review: the three things I always check, such as names, numbers and commitments
- Record: where I save the final version and any lesson learned

Keep a short log of what each routine produced and what you had to change. After a month, the log shows you which routines earn their place, which need better inputs and which should be dropped. This is the personal equivalent of an operating review.

WORKING QUESTION

Which routine would give you back the most time next week, and what are the three things you must always check in its output?



RISKS AND CONTROLS

## Memory, privacy and accuracy controls

05



Decide in advance what the assistant may know, what it may keep, and what you will never give it.

Many tools offer memory, which stores facts about you across conversations. This can help consistency, and it creates privacy and accuracy questions. Stored memory can be wrong, outdated or include details you did not intend to keep. Review what the tool remembers, correct it, and know how to delete it. Apply the same thinking to projects and shared folders: who else can see them?

| INFORMATION TYPE                          | GUIDANCE                                                         | WHY                          |
|-------------------------------------------|------------------------------------------------------------------|------------------------------|
| Public or your own non-sensitive work     | Generally fine in approved tools                                 | Low risk                     |
| Client or customer confidential material  | Only if contracts and policy allow in approved tools             | Confidentiality duties apply |
| Personal data about others                | Minimize; anonymize where possible; follow data protection rules | Privacy obligations          |
| Credentials, keys, financial account data | Never                                                            | Compromise risk              |
| Regulated or privileged material          | Only with explicit approval                                      | Legal exposure               |
| Your own health and private life          | Your call; consider whether it is needed                         | Hard to retract              |



## Personal privacy and memory policy

- 
- I use only tools approved by my employer or client for work content
  - I know whether my inputs are retained or used for training, and I have set the options
  - I do not paste credentials, secrets or regulated data
  - I anonymize names and figures when the task does not need them
  - I review stored memory monthly and delete what is wrong or unnecessary
  - I keep final work in my own systems, not only in the chat history
  - I know how to export or delete my data if I stop using the tool
  - I check current requirements under data protection law and my contracts when unsure

## Review habits

- 
- Read it aloud or skim for tone: would I say this to this person?
  - Check every name, date, number and quotation against the source
  - Look for what is missing, not only what is wrong
  - Ask the assistant to list its assumptions and uncertainties, then judge them
  - For anything that goes outside the organization, read it fully and slowly
  - Keep a record of recurring errors and add them to the standing instructions

### BEWARE AGREEMENT



Assistants tend to agree with you and to polish weak ideas. Ask explicitly for the strongest objection, the missing risk or the opposing view.

### WORKING QUESTION

What is the one category of information you will never share with an assistant, and is it written down?



## MEASURING VALUE

# Knowing whether it is working

06

Track time, quality and trust in simple ways. If a routine does not pay back, change it or drop it.

Personal productivity claims are easy to inflate. A quick feeling of speed is not evidence, because review and rework take time. You do not need an elaborate system. A small log kept for four weeks is enough to see what is paying back and what is not.

| MEASURE             | HOW TO TRACK                                            | WHAT TO LOOK FOR                                   |
|---------------------|---------------------------------------------------------|----------------------------------------------------|
| Time per routine    | Note minutes with and without assistance for a few runs | Net saving after review                            |
| Edit load           | Rate how much you changed: light, moderate, heavy       | Falling edit load as instructions improve          |
| Errors caught       | Tally mistakes you found in review                      | Patterns to add to your checklist                  |
| Errors missed       | Note any error found after sending                      | The most important signal; review habits need work |
| Quality of outcomes | Feedback from colleagues or clients                     | Clearer, more consistent output                    |
| Cognitive load      | How prepared and calm you feel                          | Better preparation, less rushing                   |

Illustrative example, not a benchmark: if a weekly update takes 60 minutes now and 35 minutes with the routine including review, the saving is 25 minutes a week. That is worthwhile if quality is equal or better. If you find you now spend 30 minutes of the 35 fixing the draft, the routine needs better inputs or should be dropped.

### 01 Baseline

For one week, note how long your target tasks take and how they feel.

### 02 Run and log

For the next three weeks, run the routines and log time, edits and errors.

### 03 Review

At week four, keep what paid back, fix what almost did and drop the rest.

## 04 Repeat quarterly

Models, tools and your work all change, so recheck the setup regularly.



### WATCH FOR SKILL EROSION

If you stop writing first drafts, the skill of structuring an argument can fade. Keep some tasks fully yours, and use the assistant to challenge your work rather than only to produce it.



### WORKING QUESTION

What would you need to see in four weeks to say that the setup was worth keeping?



### IMPLEMENTATION GUIDE

# Build your first version in an afternoon

# 07

A simple sequence gets you from nothing to a working, reviewable setup.

## 01 List and choose tasks

Write down ten recurring tasks. Mark each for repetition, checkability and risk. Select two or three.

## 02 Check the rules

Confirm which tool you may use for work content and what data may be shared. Ask if unsure.

## 03 Write the packs

Create About me, Style guide and one Project brief. Keep each to a page or two.



---

## 04 Draft standing instructions

Write eight to twelve rules, including the honesty rules about uncertainty and invented facts.

---

## 05 Define routines

For each chosen task, write trigger, inputs, instruction, output format and review checks.

---

## 06 Test and refine

Run each routine on three real examples. Edit the instructions wherever output disappoints.

---

### A starting template for a routine

- Name: Meeting prep
- Use when: a meeting is within two working days
- Provide: agenda, last notes, attendee list, my goal for the meeting
- Ask for: a one-page brief with context, three questions to ask, likely objections and what I do not yet know
- Rules: do not invent facts about people or companies; mark anything not in the material as unknown
- My review: check names and titles, verify any figures, adjust tone, add what only I know

### First version ready

- Approved tool chosen and settings reviewed
- Three context packs written and dated
- Standing instructions tested on five tasks
- Two or three routines defined with review steps
- Privacy and memory policy written
- Log started for time, edits and errors
- Date set for a four-week review

As you become comfortable, add richness: examples of your best work in the style pack, a library of saved prompts, and connections to calendar or documents if your organization permits. Add connections slowly. Every connection widens what the assistant can see and, if you grant it, what it can do. Read-only access is a good default.

If you lead a team, share the structure rather than the personal content. A common template for packs, instructions and routines helps colleagues start well, and a short team agreement on data and review keeps practice consistent.

WORKING QUESTION

What is the smallest version of this setup you could finish this week?

PITFALLS

## Pitfalls, limits and an illustrative scenario

08

Most problems are about trust and drift: believing too much, checking too little, and letting the setup go stale.

- Sending unreviewed drafts to people who matter
- Pasting confidential material into tools that are not approved
- Letting memory accumulate wrong or outdated facts
- Overlong context packs that bury what matters
- Treating confident tone as evidence
- Building many routines and using none
- Handing over decisions that require your judgment

ILLUSTRATIVE SCENARIO, HYPOTHETICAL

A manager's meeting-prep routine states that an attendee 'recently joined the board.' The assistant inferred it from a vague note. She catches it in review because her checklist says to verify every claim about people. Without that line, an awkward error would have been spoken aloud.

### Honest limits

| LIMIT                                           | WHAT IT MEANS FOR YOU        |
|-------------------------------------------------|------------------------------|
| No real memory of events unless you supply them | Keep notes and packs current |

| LIMIT                                          | WHAT IT MEANS FOR YOU                                                       |
|------------------------------------------------|-----------------------------------------------------------------------------|
| Can state falsehoods fluently                  | Verify names, numbers, quotations and citations                             |
| Sees only what you show it                     | It will miss context in your head and in other systems                      |
| Tends to please the user                       | Ask for objections and counterexamples                                      |
| Not a professional adviser                     | Use qualified professionals for legal, medical, tax and financial decisions |
| Can change when the provider updates the model | Retest key routines after noticeable changes                                |

There are tasks you should keep because they carry your accountability: final decisions, sensitive messages, commitments to others and anything where trust between people is the point. The assistant can help you prepare for those conversations, but the conversation is yours.

If the setup stops feeling useful, treat it as maintenance, not failure. Usually a pack is out of date, a rule is vague or a routine has outgrown its original job. A quarterly tidy keeps the whole arrangement trustworthy.

**WORKING QUESTION**

Which task will you deliberately keep fully yours, and why?

## SETUP QUESTIONS

# Questions to ask before you commit to a tool

09

Choose a tool on data handling, control and fit with your daily work, not on novelty.

## Questions for your tool or provider

- Is my content used to train models, and can I turn that off?
- How long are conversations and files retained, and can I delete them?
- Can I see and edit what the tool remembers about me?
- Does it support projects or saved instructions so I do not repeat context?
- Can I export my packs, prompts and history?
- What connections does it offer to calendar, email and files, and can I limit them to read-only?
- Does my employer or client approve it for the kind of content I handle?
- What happens to my setup if I change tools?

| SETUP CHOICE                              | BENEFIT                     | TRADE-OFF                                          |
|-------------------------------------------|-----------------------------|----------------------------------------------------|
| Tool provided by employer                 | Policy and security handled | Less flexibility, your own packs must follow rules |
| Personal paid tool for non-sensitive work | Flexible, quick to start    | Never for confidential content                     |
| Connected to email and calendar           | Richer preparation          | Larger exposure if mistakes or misuse occur        |
| Isolated, paste-in only                   | Tight control               | More manual effort                                 |

Cost is small relative to the time involved, but the real investment is your attention to building and reviewing the setup. Budget a few hours initially and about thirty minutes a week for maintenance and review.

If you want help designing this for a team or an executive group, Halden & Company offers free assessments at [halden.company/assessments](https://halden.company/assessments), and you can reach the team at [halden.company/contact](https://halden.company/contact). The core idea holds regardless: give the assistant good context, keep clear rules, run simple routines and always review before you rely on the result.

**WORKING QUESTION**

If you had to switch tools tomorrow, which parts of your setup would you be able to take with you?



30 / 60 / 90

## A first quarter that produces evidence

10



Build a small, reviewed setup, prove it with a log, and expand only where it pays back.

**First 30 days: ground it**

- Choose two or three recurring tasks and confirm the approved tool and data rules
- Write the About me, Style guide and one Project brief packs
- Draft and test standing instructions on five real tasks
- Start a simple log of time, edits and errors

**Days 31 to 60: test it**

- Run three routines weekly with a defined review step
- Tighten instructions using the errors you caught
- Review stored memory and delete anything wrong or unnecessary
- Add one new routine only if the first ones are paying back

**Days 61 to 90: decide**

- Review the log and keep, fix or drop each routine
- Update packs and retest key routines
- Share your template with a colleague or your team
- Decide whether to add read-only connections to calendar or files



## GLOSSARY

# Terms used in this publication

11

| TERM                  | MEANING                                                                                          |
|-----------------------|--------------------------------------------------------------------------------------------------|
| Context pack          | A short reusable document that gives an assistant background on you, your work or a project.     |
| Standing instructions | Rules applied to every task, such as tone, format and how to handle uncertainty.                 |
| Routine               | A repeatable task with a trigger, inputs, output format and review step.                         |
| Memory                | A tool feature that stores facts across conversations, which should be reviewed and correctable. |
| Hallucination         | Plausible output that is false, such as an invented fact, quotation or citation.                 |
| Human in the loop     | A design where a person reviews and approves output before it is used.                           |
| Data retention        | How long a provider keeps your prompts, files and outputs.                                       |
| Read-only access      | Permission to view information without changing it.                                              |
| Anonymization         | Removing or masking details that identify people or organizations.                               |
| Baseline              | A measurement of how long work takes or how well it goes before a change.                        |
| Prompt                | The instruction and material you give an AI model for a task.                                    |
| Sycophancy            | A tendency of assistants to agree with or flatter the user rather than challenge.                |



## A note on use

This playbook is general guidance. It is not legal, medical, tax or financial advice. Use only tools approved for your work content and check current requirements for data protection and confidentiality.

### TAKE THE NEXT STEP

Take the free Halden assessment at [halden.company/assessments](https://halden.company/assessments), or talk to us at [halden.company/contact](https://halden.company/contact) about turning this into a plan for your organization.

