FREE RESOURCE

# AI Agent Starter Checklist | Digihandler Academy

Plan, run and review your first AI agent tasks safely. Facts checked on official pages in November 2026.

## 1 What an AI agent is, in one minute

An AI agent takes a goal and works through the steps itself: it **plans**, **acts** with tools (a browser, your files, apps), **checks** the result and repeats until the job is done or it needs you. A chatbot answers. An agent acts. That is why it needs clear goals, limits and your review.

## 2 Before you start

- [ ] I picked one task I already know how to do by hand.
- [ ] The task has a clear finish line (a sheet, a list, a draft).
- [ ] The task does not involve paying, sending, posting or deleting.
- [ ] I know which sites or folders the agent needs, and nothing more.
- [ ] Approval prompts ("ask before acting") are switched on.
- [ ] I will not type passwords, OTPs or card numbers into the chat.
- [ ] I have time to watch the first run from start to end.

## 3 Task picker: green, amber or red?

| Level | Examples | How to run it |
|---|---|---|
| Green | Research public websites into a sheet; summarise PDFs; rename files in a test folder; draft replies (not send) | Good first tasks. Review the output. |
| Amber | Fill a form you will submit yourself; edit a shared document; work inside your email to draft only | Watch live. Approve each step. |
| Red | Payments, bookings, sending emails or posts, deleting data, anything with passwords or ID numbers | Do these yourself for now. |

**Remember:** web pages and files can hide instructions that trick an AI (prompt injection). Security groups and AI makers say no agent is fully immune, so keep tasks small and keep approvals on.

DIGIHANDLER ACADEMY © 2026 Digihandler Academy. All rights reserved. digihandleracademy.com · Free for personal use; do not resell or republish.

## 4 Goal brief template (fill this in before every task)

**Goal in one line**

What should be true when the agent finishes?

**"Done" looks like**

Format, columns, number of items, file name

**Allowed sites, apps or folders**

List only what the task needs

**Must NOT do**

e.g. submit, buy, send, post, delete, sign in

**Stop and ask me when**

e.g. a login page appears, a price is shown, a form asks for personal data

**Show me the plan first?**

Tick one

☐ Yes ☐ No

## 5 Example brief you can copy

```
Goal: Make a sheet of 10 coaching centres in Rohtak that show course fees on their own
website.
Done looks like: a table with columns Name, Course, Fee, Page link. 10 rows.
Allowed: web search and the centres' public websites only.
Must not: fill or submit any form, sign in anywhere, or contact anyone.
Stop and ask me if: a page needs a login or asks for my details.
First, show me your plan in 5 steps and wait for my OK.
```

## 6 While it runs

DIGIHANDLER ACADEMY © 2026 Digihandler Academy. All rights reserved. digihandleracademy.com · Free for personal use; do not resell or republish.

- [ ] I read the plan and fixed anything wrong before saying OK.
- [ ] I watched each step and stopped it if it went off track.
- [ ] I took over myself for any login or payment screen.
- [ ] I denied any action that was not in my brief.

DIGIHANDLER ACADEMY © 2026 Digihandler Academy. All rights reserved. digihandleracademy.com · Free for personal use; do not resell or republish.

## 7 After it finishes

- [ ] I spot-checked at least 3 facts against the original pages.
- [ ] Nothing was sent, bought, posted or deleted that I did not approve.
- [ ] I removed access to folders or apps the agent no longer needs.
- [ ] I saved the brief that worked so I can reuse it.

## 8 Review log

| Date | Task | Tool | Result OK? | What to change next time |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## 9 Agents to try (as of November 2026)

| Agent | Who can use it (official pages, Nov 2026) |
|---|---|
| **Tasks in Gemini** | 18+, personal Google account, Google AI Pro or Ultra. Not in the EEA, Nigeria, Switzerland or UK. Up to 15 tasks at once. |
| **Chrome auto browse** | AI Pro and AI Ultra subscribers in India, desktop and Android, devices set to English. |
| **Claude Cowork** | Paid Claude plans: Pro, Max, Ultra, Team, Enterprise. |
| **Claude in Chrome** | Paid Claude plans. Anthropic says it is still risky; review its safety guide. |
| **ChatGPT agent** | Launched 17 July 2025 for Pro, Plus and Team (TechCrunch). Check OpenAI's help centre for current plans. |

Plans, prices and countries change often. Always check the official page before you subscribe.

DIGIHANDLER ACADEMY © 2026 Digihandler Academy. All rights reserved. digihandleracademy.com · Free for personal use; do not resell or republish.