



10

FREE GUIDE

AI agents at work: what to hand over and what to keep

Last checked: 27 September 2026 · 22 minute read · For owners, no tech needed

INSIDE

1. Try this now: the approval rule
2. Start here if you've never used AI
3. What an agent can do today, and what it can't
4. The options side by side
5. Connecting your apps safely
6. The first 5 jobs to hand over
7. How to check its work: the 2-minute review
8. What not to delegate yet
9. The 2-week trial plan with a keep-or-drop score
10. A worked example
11. Quick reference

Joe | Droom

@joebuildswithai · droom.ca

The plan

1. Read the one-page difference between a chatbot and an agent (section 1), so you know what you're being sold.
2. Give every agent you try one standing rule: it drafts, you send. The prompt for that is right below.
3. Hand over one job from section 5 for two weeks. Check its work every day, then score it with the keep-or-drop table in section 8.

Try this now: the approval rule

An agent doesn't only write. It does things, and that's both the point and the risk. Before you let one near your email, calendar or accounts, give it this rule. Paste it into the agent's saved instructions (some tools call them custom instructions, preferences or project instructions), or at the top of any task you give it.

COPY THIS

You are helping me run [business name], a [type of business] in [city]. Standing rule for every task: you prepare, I approve. - Draft emails, messages and replies, but never send them. Show me the draft and wait. - Never buy, pay, book with a deposit, sign, accept terms, or share a card or account number. - Never delete, archive or move anything without asking me first. - Never contact a customer, supplier or staff member unless I've approved that exact message. - If a website asks for a password or a code, stop and tell me. - If you're unsure what I want, ask one question before doing anything. At the end of each task, give me a short list: what you did, what you're waiting on me for, and anything that looked wrong.

Now test it. Ask the agent to "send a thank-you email to [a friend or your own second address]". It should stop and show you the draft. If it sends anyway, that tool isn't ready for your customer inbox.

1. Start here if you've never used AI

An AI chatbot is a website or app you type to, and it writes an answer back. ChatGPT (made by OpenAI), Claude (Anthropic), Gemini (Google), Copilot (Microsoft) and Meta AI all started this way. You

ask, it writes, and you decide what to do with the words. Nothing leaves your screen unless you copy it somewhere.

An AI agent is a chatbot that's been given hands. You give it a goal, say "find three suppliers for this part and compare delivery times", and it works out the steps and does them. It opens websites, reads pages, fills in forms, and looks in your email or calendar if you've connected them. Then it comes back with a result. Some agents keep working after you close the app, or run on a schedule.

That one difference changes how careful you need to be. When a chatbot gets something wrong, you get a bad paragraph. When an agent gets it wrong, the bad paragraph can end up in a customer's inbox.

The one-page difference

	Chatbot	Agent
What you give it	A question or a request for writing	A goal with steps
What it gives back	Words on your screen	A finished task, or a task waiting for your OK
Can it open websites?	Some can look things up	Yes, and click, scroll and fill in forms
Can it use your email or calendar?	Only if you connect them	Usually that's the point
Can it act without you watching?	No	Some can, on a schedule or in the background
What goes wrong	A wrong fact in a draft	A wrong action: a sent message, a changed booking
Your job	Read before you copy	Set limits, approve actions, check the log

Agents are slow. One task can take several minutes while it visits pages and checks things. That's normal.

They still make things up sometimes. Everything in my other guides about checking facts applies here. The difference is you also check what it did, not only what it wrote.

Most of the agent features in this guide are on paid plans. The free plans of ChatGPT and Claude are fine for learning the chatbot side (see [ChatGPT and Claude for beginners](#)). Section 3 says which agent features I could confirm, and which you can use in Canada.

Keep private details out until you've read section 4. Connecting your inbox hands the tool your customers' names, addresses and messages. Make that call on purpose. Don't let it happen because you clicked through a sign-in screen.

Words you'll see

Word	What it means
Agent	An AI tool that carries out steps for you as well as writing.
Agent mode / Work mode	A switch inside a chatbot that turns on the agent.
Connector / connected app	A link you set up so the AI can read or act in another app, like Gmail or Google Drive.
Permission	What you allow a connector to do: read only, or read and change.
Approval / confirmation	The moment the agent stops and asks "OK to do this?" before acting.
Task	One job you give an agent. Some tools let you schedule tasks to repeat.
Activity log	A list of everything the agent did. Read it.
Take over	Taking control of the agent's browser yourself, usually to type a password.
Prompt injection	A trick where a web page or email hides instructions aimed at the agent, trying to get it to do something you didn't ask for.

2. What an agent can do today, and what it can't

The product names in this area changed several times this year. What the tools can do underneath has moved less. Here's what the agents I checked (section 3) say they can do.

Browse the web for you. Open sites, search, read pages, compare options, and bring back a summary with links. This is the most reliable part and the easiest to check, because you can click the links.

Fill in forms. Contact forms, quote requests, booking forms. Most tools stop and ask before submitting anything with personal information or money in it. Some let you "take over" the browser to type a password yourself, so the agent never sees it.

Work in apps you connect. It can read your email and draft replies, look at your calendar and suggest times, search a shared drive, or pull numbers out of a spreadsheet. How far it goes depends on the permissions you give the connection.

Make files. Documents, spreadsheets, presentations. ChatGPT Work and Microsoft's agents both list reports and spreadsheets as a main use.

Run on a schedule. Some agents can repeat a task every morning or every Monday. OpenAI, Microsoft and Google all describe scheduled or background tasks on their own pages.

Where they fall down:

Knowing your business. It knows what you've told it and what it can read. It has no idea you never send the Chilliwack crew out on Fridays unless that's written somewhere it can see.

Telling a good website from a bad one. It reads whatever is on the page, and a page can carry instructions aimed at the agent (the "prompt injection" from the word list). The companies build defences, and OpenAI's help pages say its agent tools may be unable to visit some sites for safety reasons. Your own defence is the approval rule. Nothing leaves without you.

Carrying the responsibility. If an agent sends a wrong quote, or a message that breaks the rules, it went out under your business name. Your customers and the law will treat it as coming from you.

3. The options side by side

I checked each company's own pages on 27 September 2026. These change month to month, so look at the company's page again before you sign up for anything. Where I couldn't confirm a detail, I left it out.

Product	Who makes it	What its own pages say it does	Can Canadian businesses use it now?
Muse	Meta	A personal agent that can send an email, book travel, open a browser, fill out forms and keep working after you close the app. Works in the Muse app or in WhatsApp.	Meta's announcement says it's rolling out in the US. I found no Canadian launch.

Product	Who makes it	What its own pages say it does	Can Canadian businesses use it now?
Meta Business Agent	Meta	Answers customer questions for a business on WhatsApp, Instagram and Messenger, books appointments and recommends products. You decide when a person steps in.	Meta says it's rolling out to businesses globally. It started free with paid plans to follow, so check the current terms when you sign up. Look for it in your WhatsApp Business or Meta Business Suite settings.
ChatGPT Work	OpenAI	An agent mode in ChatGPT for longer, multi-step jobs: reports, spreadsheets, presentations, browser tasks, connected apps like Gmail and Slack, and scheduled tasks. It shows a plan you can change or approve before it starts.	OpenAI lists it on its Plus, Pro, Business, Enterprise and Edu plans. Not on the free plan.
Microsoft Copilot Tasks	Microsoft	You describe a goal and Copilot plans and does the steps: browsing, filling in websites, making files, using connected email or storage. Can run once or on a schedule.	Microsoft calls it a preview and doesn't say who can use it or where.
Microsoft 365 Copilot agents	Microsoft	Ready-made agents for work accounts, including Researcher (reports from the web and your work files) and Analyst (turns data into charts and findings), plus meeting and project helpers in Teams and Planner.	For businesses on Microsoft 365. What you get depends on your licence, so ask whoever runs your Microsoft 365.
Claude with connectors	Anthropic	Connectors let Claude read from and act in apps like Gmail, Google Calendar, Google Drive, Slack and Microsoft 365. You add them under Customize in Claude and switch them on or off per chat.	Available across Claude's plans. Anthropic's help page says free users get one custom connector, so check which connectors your plan includes.

Product	Who makes it	What its own pages say it does	Can Canadian businesses use it now?
Gemini Spark	Google	A personal agent that works across Gmail, Calendar, Drive, Docs and Sheets and handles email, research and scheduling. Google says it's "designed to ask you first before performing high-stakes actions like spending money or sending emails".	Google's Canada blog says it's rolling out to Google AI Pro and Ultra subscribers in Canada, 18 and over. Paid plans only, so check yours.

What this means for a Canadian owner today. The ones you can most likely use this week are ChatGPT Work (on a paid plan) and Claude with connectors. If your office already runs on Microsoft 365, ask about Copilot, since it can already see your work files and email. Google's Gemini Spark is here too, on paid Google AI plans, and it works inside Gmail and Calendar, so if your business runs on Google it's a real third option. Meta's Muse isn't here yet. When it arrives, the rest of this guide applies to it the same way.

How to find the agent part. In ChatGPT, look for Work next to Chat at the top of the screen. In Claude, connectors live under Customize, and you turn them on per chat from the + button. In Copilot, look for Tasks. Each one shows you a plan or asks before it acts. Read that screen properly the first time.

Phone calls are a different product. An agent that answers your phone has its own rules. My [AI receptionist guide](#) covers that.

4. Connecting your apps safely

Connecting an app is where an agent stops just writing things and starts doing things with your data. Give it five minutes.

Before you connect anything

Use a separate account where you can. A shared inbox like info@ is safer to connect than your personal one, which has your bank, your family and your lawyer in it.

Read the permission screen. When you connect Gmail, Microsoft 365 or anything else, a screen lists what the tool wants: read your email, send email, delete email, see your contacts. If the job only needs reading, look for a read-only option. If there isn't one, good to know before you say yes.

Only connect official connectors for services you trust. Anthropic's help page puts it simply: "only connect services you trust and need". That goes for every tool. Use the connector listed in the app's own settings, not a look-alike you found in a search.

Keep approvals on. Every product in section 3 has some kind of "ask me first" step for sensitive actions. OpenAI's help page for its Business and Enterprise workspace agents says write actions are set to "Always ask" by default. Microsoft's Copilot Tasks page says it asks before purchases, before submitting personal information to websites, before sending emails or messages, and before deleting files or changing account settings. Leave those where they are. If a tool offers "always allow", don't use it for anything that sends, pays or deletes.

What never to connect (for now)

- Your business bank account or payment processor.
- Your accounting software with permission to create or approve payments.
- Your payroll system, or anything with staff SINs and banking details.
- Patient, client health or legal files.
- An inbox that receives password reset emails for your important accounts, if you can avoid it.
- Your social media accounts with permission to post, until you've run the section 8 trial on drafts.

Privacy: the Canadian part

Once you connect an inbox, the AI company can see your customers' personal information. Canada's private-sector privacy law (PIPEDA), and BC's own law (PIPA) for many BC businesses, expect you to protect the personal information you collect, including when a service provider handles it. In practice:

- Check the tool's settings for whether your data is used to train future models, and switch that off if you can. Business plans often have different defaults from personal ones, so read the one for your plan.
- Say in your privacy policy that you use service providers, including AI tools, to help handle enquiries.
- Don't connect anything holding health, financial or children's information without talking to a privacy professional first.

This isn't legal advice. If you handle sensitive information, check with a professional before you connect it.

After you connect

- Find the list of connected apps in the tool's settings. Know where it is before you need it in a hurry.
- Disconnect anything you stop using. Each connection you leave on is another way into your data.
- Once a month, go down the list and ask of each one: do I still need this?

5. The first 5 jobs to hand over

Each of these ends in something you can check before it matters: a draft, a list, a report. None of them sends, pays or deletes by itself. Each has a setup prompt. Use it along with the approval rule from the top of this guide.

Job 1: Inbox triage

What it does. Reads new email in one inbox, sorts it into piles (customers who need a reply today, quotes and enquiries, suppliers, invoices, junk), drafts replies for the easy ones, and gives you a short list.

When to use it. When your inbox is where the day goes, and most messages need one of a handful of replies.

The setup prompt.

COPY THIS

Look at the unread email in [inbox name] from the last [24 hours]. Sort every message into one of these groups: Reply today, Quotes and enquiries, Suppliers, Invoices and bills, Can ignore. For each message give me one line: who it's from (first name and business only), what they want, and which group. For messages in Reply today and Quotes and enquiries, write a draft reply in my voice and save it as a draft. Don't send anything. Don't delete, archive, label or move any email. Our usual answers: [paste your hours, service area, how to book, what you don't do]. If a message is a complaint, a legal letter, or mentions money owed, don't draft a reply. Put it at the top of the list for me.

What to check. Open three drafts at random and compare each with the original email. Make sure nothing important landed in Can ignore, and that no draft promises a date, price or discount you didn't give it.

Job 2: Booking and reminders

What it does. Looks at your calendar and incoming requests, suggests times that fit, drafts the confirmation, and drafts reminders for tomorrow's appointments.

When to use it. When you or your front desk spend the day going back and forth about times. It needs both your calendar and your inbox connected, so do Job 1 first.

The setup prompt.

COPY THIS

You help with bookings for [business name]. Our booking rules: [opening hours, how long each type of appointment takes, gaps needed between jobs, days we don't book, areas we cover on which days]. 1. Look at my calendar for the next [7] days and list the open slots that follow these rules. 2. Look at booking requests in [inbox or form responses]. For each one, suggest two slots and draft a reply offering them. Don't send it. 3. Draft a reminder for each appointment tomorrow: first name, time, address or location, and what to bring. Don't send them. Don't create, move or cancel any calendar event. Show me what you'd change and wait.

What to check. Hold the suggested slots up against your real calendar, especially around travel time and lunch. Check each reminder has the right day. Text reminders about an appointment are usually transactional rather than marketing. Add a promotion to one, though, and it may fall under Canada's anti-spam law (CASL). Keep reminders to the appointment.

Job 3: Research and comparisons

What it does. Goes out on the web, finds options, reads their pages and brings back a comparison table with links.

When to use it. Choosing a supplier, a piece of equipment, a software tool or a venue. Seeing what other businesses in your area list as services. Finding the right government form or program page.

The setup prompt.

COPY THIS

Research [what you're comparing, for example: commercial dishwasher suppliers that deliver to Surrey, BC]. Find [5] options. For each one, give me: name, website link, what they offer that matters for [my need], delivery or service area, how to get a quote, and anything that looks like a red flag. Only use information you found on their own website or an official page. Put the link next to every fact. If you can't find something, write "not found". Don't guess. Don't fill in any contact or quote forms. Don't create accounts. Finish with a short table and your top pick, with one line on why.

What to check. Click at least two links per option and make sure the fact is really there. Watch for out-of-date pages, US companies that don't ship to Canada, and prices in US dollars. Treat its top pick as a starting point. You still make the call.

Job 4: Weekly reports

What it does. Reads a spreadsheet or export (sales, jobs completed, enquiries, hours) and writes a short weekly summary with a simple table.

When to use it. When you keep meaning to look at the numbers on Monday and never do.

The setup prompt.

COPY THIS

Here is this week's [sales / jobs / enquiries] data: [attach the file or name the spreadsheet in your connected drive]. Write a weekly report for me, the owner, in plain words, under [300] words: - The three numbers that matter most this week and how they compare with last week. - Anything unusual, with the rows it came from. - One question I should ask my team. Make one simple table. Only use numbers from the file. If a number looks wrong or is missing, say so instead of fixing it. Don't edit the original spreadsheet. Put the report in a new document called [Weekly report, date].

If you attached the file rather than connecting a drive, ask for the report in the chat and copy it out yourself.

What to check. Check two of the headline numbers against the spreadsheet yourself. Agents misread columns, double count and mix up weeks. If it "finds" a big drop or jump, look at the rows before you react.

Job 5: DM replies

What it does. Drafts answers to messages on Instagram, Facebook or WhatsApp from a list of your real answers. Meta's Business Agent (section 3) is built for exactly this. With other agents, you paste the messages in and get drafts back.

When to use it. When the same five questions land in your DMs every day (hours, price range, do you come out to my area, how to book), and a slow reply loses you the customer.

The setup prompt.

COPY THIS

You draft replies to customer messages for [business name]. Here's everything you're allowed to say: [hours, services, areas, how to book, booking link, what we don't do, how long jobs usually take]. Rules:

- Answer only from the list above. If the answer isn't there, write "I'll check and get back to you today" and flag it for me.
- Never quote a price unless it's on the list.
- Never promise a date or time. Offer the booking link instead.
- If someone is upset, complaining, or mentions an emergency, don't reply. Flag it for me straight away.
- Friendly, short, no emoji walls. One question at most per reply.

Here are today's messages: [paste, or connect].

What to check. Read every reply for the first two weeks, looking for anything it answered that wasn't on the list. If you use an agent that replies by itself, find out how and when a person takes over, and make sure customers can reach one. Replying to someone who messaged you is one thing. Sending them promotions later is another, so read up on CASL consent before you do any sales follow-up.

6. How to check its work: the 2-minute review

An agent fails quietly. It won't tell you it picked the wrong week. So give yourself a routine: do this after every task during the trial, and once a day after that.

1. **Read its summary.** The approval rule asks it to list what it did, what it's waiting on and what looked wrong. No summary? Ask for one.
2. **Open the activity log.** Most agent tools keep one. Look for anything you didn't ask for: a page that seems unrelated, a form it started, a file it opened.
3. **Spot-check one thing properly.** Pick one draft, one number or one link and check it against the source. Pick a different kind each day.
4. **Check nothing left the building.** Look in your Sent folder, your calendar and any outbox. Everything there should be something you approved.
5. **Write down one correction.** If it got something wrong, add a line to its saved instructions ("We don't book on Fridays", "Always use our booking link, never the phone number"). This is how it learns your business.

Keep score as you go. A note on your phone works, or print this and stick it by the desk. You'll need it for section 8.

Day	Ran it	Mistake caught	Correction added
1			

Day	Ran it	Mistake caught	Correction added
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			

When it goes wrong

What happened	What to do
It sent something you didn't approve	Turn off the connection now. Check your approval settings. Contact the person it went to if needed. Don't reconnect until you know why.
It stopped halfway	Usually a login, a pop-up or a site that blocks agents. See where it stopped and do that step yourself.
It keeps asking for approval on everything	That's the safe setting doing its job. Once a task has run cleanly for two weeks, you can decide whether it still needs to ask.
It made up a fact or a number	Add "Only use information from [source]. If it's missing, say so." to its instructions. Check every number for a week.
It went to a strange website	Stop the task, read the log, and don't let it carry on at that site.

What happened	What to do
It's slower than doing it yourself	For some jobs it will be. Drop that job. That's what the trial is for.

7. What not to delegate yet

Some jobs are a bad fit for an agent however much you trust it. Keep these, even if a tool offers to take them.

Payments and money. Paying bills, approving invoices, issuing refunds, moving money between accounts, entering card details. An agent can draft a list of what's due. You pay.

Hiring decisions. It can write a job ad and suggest interview questions. It shouldn't screen people out, rank candidates or reject anyone. Human rights law covers hiring in Canada, and a tool can filter people unfairly without anyone noticing.

Anything legal. Signing or accepting contracts, replying to a lawyer's letter, answering a government notice, agreeing to terms for you. It can summarise the document. A person decides, and for anything serious a professional reads it.

Discipline, firing, or anything about a named staff member. Keep staff matters between people.

Complaints and apologies. An agent can draft one for you to rewrite. Sending an apology is a decision about your reputation, and that's yours.

Anything with health, financial or children's information. Clinics, bookkeepers, daycares and the like should keep that data out of general agent tools until a privacy professional has signed off.

Deleting things. Emails, files, bookings, customer records. There isn't always an undo.

Promotions to your customer list. Agents can draft them. Who gets them, and whether you have consent under CASL to send them, is your call.

Here's a quick test. If this went wrong, would I have to phone someone and apologise, or phone my lawyer? If the answer's yes, the agent drafts and you do the rest.

8. The 2-week trial plan with a keep-or-drop score

One job at a time. Two weeks catches a busy day and a quiet one, and it's short enough that you'll actually finish.

Before day 1

- [] Pick one job from section 5. Just one.
- [] Pick one tool you can actually use in Canada today (section 3).
- [] Save the approval rule from the top of this guide in its instructions.
- [] Connect only what that job needs, with the fewest permissions that work.
- [] Test it once on something harmless, like your own second email address.
- [] Note which plan you're paying for, so on day 14 you can weigh the time saved against it.
- [] Write down roughly how long the job takes you now, in minutes per day.

Week 1: watch everything

- Run the job every working day.
- Do the 2-minute review (section 6) every time.
- Approve or fix every draft yourself. Nothing goes out without you.
- On any day it gets something wrong, add a correction to its instructions.

Week 2: time it

- Keep running it the same way.
- Now time yourself. How long does the whole thing take, checking included?
- Note any day it made a mistake you only caught because you checked.

Day 14: score it

Give each line 0, 1 or 2. Be honest. Nobody else sees this.

Question	0	1	2
Did it save time, including checking?	No, or it cost time	A little	Clearly
How were its drafts or results?	Mostly rewritten	Some edits	Mostly usable

Question	0	1	2
Did it make any mistake that would have reached a customer?	More than once	Once	Never
Did it stay inside the rules you set?	It broke one	Close calls	Always
Did you trust it more on day 14 than on day 1?	Less	The same	More

8 to 10: keep it. Carry on with the same approvals. Give it another month before you think about a second job.

5 to 7: fix it or drop it. Look at where it lost points. If the instructions are the problem, rewrite them and run one more week. If the tool is, try the same job in a different one.

0 to 4: drop it. Disconnect the apps and go back to doing the job yourself, or use a chatbot for drafts. You haven't lost anything. You found out what not to hand over.

A 0 on either the "reached a customer" or the "broke a rule" line overrides the total: drop it until you know why.

9. A worked example

This is a made-up business, written to show how the pieces fit together. It isn't a customer.

A landscaping company, 18 staff in season

The office manager tries inbox triage in ChatGPT Work, connected to the shared info@ inbox and nothing else. Week 1 goes badly on one thing. It keeps filing supplier invoices under Can ignore, because they come from a no-reply address. She adds a line to the instructions ("Anything with an invoice or statement attached goes in Invoices and bills"), and it stops. By day 14 the drafts need small edits and nothing has gone out without her. Score: 8. She keeps it, and leaves the owner's personal inbox unconnected.

10. Quick reference

- Save the approval rule in every agent: it drafts, you send.
- In Canada today, the agents you can most likely use are ChatGPT Work (paid plans), Claude with connectors, and Gemini Spark on paid Google AI plans. On Microsoft 365, ask about Copilot. Meta's

Muse wasn't available here when I checked.

- Never connect banking, payroll, or health and legal files.
- First five jobs: inbox triage, booking and reminders, research, weekly reports, DM replies.
- Check its work every day: summary, log, one spot check, the Sent folder, one correction.
- Keep payments, hiring, legal, complaints and deleting for yourself.
- Trial one job for two weeks, score it out of 10, keep it at 8 or more.
- For phones, see the [AI receptionist guide](#). For drafts without an agent, see [30 copy-paste prompts](#). For your first automation, see [first automation](#).