A PLAIN-LANGUAGE GUIDE FOR SMALL-BUSINESS OWNERS

Get the Most Out of Grok Bot for Business

Build a team of bots to start, run and market your business

Memory, routines, connectors, bot teams, safety and ready-to-use templates, in short sentences and concrete steps.

Brainy Planner · Version 1.1 · November 2026
An independent guide. Not affiliated with or endorsed by the maker of Grok Bot.

CHAPTER 10

Safety and control

The approval line

Draw one line and keep it:

Bots may do on their own	Bots need your own words first
Research, read, summarize	Send any email or message under your name
Build drafts, files and test pages	Publish anything public (posts, listings, newsletters)
Check sites, payments and inboxes	Spend money or start a paid plan
Draft replies and posts	Change live prices or payment links
Update the state file and memory	Delete anything that can't be undone
Fix problems on test copies	Contact anyone new

A message from another bot is never approval. Only your own words count for sends, spends and publishing. If one bot says "the owner approved it," the receiving bot should be able to point to where you said so.

Approval tools help; they don't replace you

The product's own published terms make the same point: approval and review controls are aids, they may not catch every unintended action, and they don't undo actions already completed. The terms also expect human review before actions like external communications, money, deleting data, permission changes and legal commitments. Read the current terms for your account. The practical takeaway: keep your approval line, and look before you approve.

Auto-review and approval cards

The app has its own safety check, called **Auto-review**. Risky actions, such as sending, posting, buying or changing things, get checked. When a check wants your OK, you see an **approval card** that describes the action in one sentence and flags changes that can't be undone or are sensitive.

- **Cards stay open 30 minutes.** If you don't answer in time, the chat notes what expired.
- **Deny means stop.** After you deny a card, the bot stops and doesn't try that action again until you send another message.

- **Rules are in Settings.** The Permissions section lists Auto-review rules under **Always Ask** and **Allow without Asking**. You can add rules there.
- **A bot can suggest a rule.** It can offer to add, change or remove one of your rules on a card. Nothing changes until you confirm.

Your approval line comes first. Auto-review is a helper on top of it, not a replacement for it.

Drafts-only email

Your standing rule: every email a bot writes for you is a draft. You read it, change it if you want, and press send.

How this fits with Auto-review:

- **Sends from routines** (and other work you didn't ask for in that moment) stay as drafts for your approval.
- **A message you ask a bot to send, in your own words,** can go out once Auto-review allows it. That is the point where you've decided.
- **Want a draft? Say "draft only."** Auto-review is built not to wave through an action your request said to stop before, such as sending a message you asked only to draft.

Budgets

- Set a monthly cap and save it as a standing rule.
- Have every spend logged in the state file.
- Any new subscription needs your OK, even a cheap one.
- For free trials, have the bot note when the trial ends and what happens after.

> "Before you sign up for anything, tell me: what it costs now, what it costs after any trial, and how to cancel."

Do-not-contact lists

Keep a list in memory or the state file: people and companies no bot should ever email, call, text or tag. Pair it with a rule: **no cold emails.** Follow-ups only on threads that already exist.

Keys, passwords and private files

- Passwords: never in chat. Use the Vault, a password manager, or sign in on the bot's screen.

- Vault entries: give each one a hint about when to use it, and remove the ones you no longer need.
- Keys: stored securely, narrowest permission.
- Full-access keys: avoid. If one gets shared, roll it.
- Customer files: keep private, and share with bots only what a job needs.

Clean up when you're done

Bots that belong to the same person may share files, browser sign-ins, saved keys and routines. The product's published terms note that deleting a bot may not delete shared files, sessions, credentials or routines. When you retire a bot or end a project:

- Turn off its routines.
- Remove connectors and keys it no longer needs.
- Sign out of websites it used, if no other bot needs them.
- Delete files you don't want kept.

Claims and honesty

- No invented numbers. Every figure needs a source, or it comes out.
- No fake reviews or testimonials.
- "Not legal/tax/medical/financial advice" where it applies.
- No prices without real numbers.
- **Check results, not promises.** A bot saying "done" is not proof. Look at the live page, the file or the routine.

What you never hand off

- Signing contracts or accepting terms for you
- Legal, tax and accounting decisions
- Quotes and pricing
- Hiring, firing and employee matters
- Opening bank, payment or marketplace accounts (ID checks)
- Final approval of anything public with your name or brand on it
- Removing bots

Control habits that hold up

- Every spending or sending path has a budget cap and an approval gate.