AI safety: what protects you

Your AI Layer · https://schoolyland.com/docs/ai-safety-and-permissions/

Giving an AI access to your business platform is a big step. We built the service on the assumption that things will occasionally go wrong, so that when they do, you can roll back in seconds.

1. The dangerous actions are simply impossible

The AI cannot delete your site, change your password, create new admin users, or run code that endangers the platform. This doesn't depend on the AI's judgment: those actions are blocked in our code, on the platform side. Even if you explicitly ask for them, they won't happen.

2. Before every change, the previous state is saved

Every time the AI edits a page, a snippet or a course structure, the version that existed before the change is saved automatically, up to three versions back per item. If a result isn't what you wanted, tell the AI "roll it back". It takes seconds and needs no ticket or form.

3. Destructive actions are gated

Destructive and irreversible actions (deleting content, sending a campaign, running PHP) are gated. Some ask you to confirm; some are refused outright by our server until you explicitly approve. Routine content edits happen immediately, exactly as they would if you clicked "Update" in WordPress yourself, and like WordPress, every one of them is backed up and reversible. Every action is logged. And because the connection is a standard WordPress Application Password on your own user, you can revoke it yourself from your own dashboard, at any second, without asking us.

4. Your data lives in your own database

Client details, orders, members and content live in your platform's own database. The AI conversation stays between you and your AI provider. The connection credential is stored encrypted, and every

connection runs over HTTPS.

5. You control what's allowed

You choose which capabilities are open to the AI: read-only answers, edit-but-never-delete, or full access. The permission settings are flexible and you can change them at any moment from your customer portal.

6. Instant disconnect

One click in the portal cuts the connection and invalidates the credential. Reconnecting later is just as simple. You can also revoke an individual team member's connection without touching your own.

What the AI layer is not

- It doesn't act on its own. Everything starts from a conversation you (or a team member) initiate.
- It isn't Schoolyland watching your business. The AI conversation happens between you and your AI provider; our layer carries out the platform actions you ask for.
- It doesn't replace your judgment. It is fast, but review what it produces as you would a new assistant's work, especially in the first weeks.

The fine print, if you want it

The AI layer has its own short legal documents: AI Layer Terms and AI Layer Privacy. You accepted them at checkout; they're always available at those links. You can disable the AI layer entirely at any time. The rest of your platform is unaffected.