

L02 — Safety Rails

This is the most important lesson in the leader track, and I want to be straight with you about why. This ministry asks kids to call strangers and put things on the public internet. Done with rails, that is one of the best growth experiences a young person can have. Done without rails, it is how a well-meaning youth group ends up in an awkward situation. So this lesson is the rails. There are two kinds: people safety and account safety.

People safety first, because it matters most. Four rules, and they are not suggestions.

Rule one: calls happen on the church's terms. The kids call from the church phone, or from a number you own and control - never from their personal cell phones. The person on the other end should see the church calling, because the church is who is calling. The kids are its voice.

Rule two: you are in the room. Practice calls, real calls, every call - a leader is present and can hear how it is going. Not hovering, not scripting every word, just present. The kids will actually do better knowing you are there.

Rule three: no personal information, ever. Kids give first names only. Their personal phone numbers, emails, last names, and schools never go to the person being called, and just as important, they never go onto the websites they build. Every contact detail published on a site belongs to the church or the business the site is for. The starter kit's AI instructions enforce this too - the assistant has standing orders to refuse to put a kid's personal details on a page.

Rule four: the church is the named party. When the donation conversation happens, money goes to the church - its giving page, its address, its name. Never to a kid, never through a kid's payment app. And before any site goes live, the church or business it belongs to says yes out loud. We never publish anything about a real organization without their permission - the demo is shown to them, not the world, until they approve it.

Now account safety, and after last lesson you can guess the theme: the accounts are the church's, so treat them like the church's. Three habits.

Habit one: log out at the end of every meeting. Railway and GitHub especially. It takes ten seconds and it means a shared computer is never quietly signed in to the church's infrastructure all week.

Habit two: the passwords live with you, not the browser. Do not let a shared machine offer to save them. Keep them where the church keeps its other important passwords, and type them yourself when needed. Here is the line I want you to remember, because it makes everything simple: the kids never need a password. If a step asks for one, that step is yours. The kit was deliberately built so that everything the kids do - building, checking, previewing - needs no login at all.

Habit three: keep payment details out of the machine. The church's card lives in Railway's billing settings behind your login, and nowhere else - not saved in the browser, not in autofill on a computer a dozen people use.

And one piece of quiet reassurance to close. You might be wondering what happens when a kid asks the AI for something they should not, or tries to edit something fragile. The kit assumes it will happen. The AI's standing instructions keep it inside the website files and away from anything that can really break, and when something needs you, it is trained to say so: this needs your group leader. The safety net is not your vigilance alone; it is built in.

Your build for this lesson: write your house rules. One page, your own words, covering the four people rules and the three account habits, adjusted to your church - which phone, which room, which adult. Print it and tape it next to the computer the kids will use. When a parent asks what the rules are, and a parent will ask, you hand them the page.