Step-by-Step Guide for School-Issued Devices

School devices can open amazing learning doors—and hidden risks. This guide helps you lock down settings, monitor activity, and coach your child. Encourage your school to deploy a parental app across device.

Step 1. Review the Acceptable Use Policy

- Find the AUP on your school's website or request it from the school.

Highlight sections on chat rooms and monitoring so you know what protections exist.

Step 2. Secure the Account

- Change default login to a strong passphrase.
- Enable two-factor authentication if available.

Store credentials in a password manager or locked family vault.

Step 3. Approve Trusted Apps & Extensions

- Compile a whitelist of approved tools (e.g., Khan Academy, Google Classroom).
- Remove or block any unrecognized extensions.

Step 4. Set Parental Controls & Filters

- On Chromebooks: Use Family Link to enforce SafeSearch and time limits.
- On tablets: Use built-in screen-time and content-restriction settings.

Step 5. Schedule Weekly Check-Ins

- Block 15 minutes each week to review browsing history, installed apps, and chat logs.
- Ask open-ended questions: "What surprised you this week online?"

Turn it into a fun ritual—snacks + chat time.

Step 6. Teach Healthy Digital Habits

- Model closing unused tabs and logging out.
- Explain why random friend requests need caution.

Step 7. Create an Emergency Plan

- Save local police non-emergency and school resource officer contacts.
- Decide on a "family code word" to signal an urgent talk.

Quick-Reference Settings Table

Setting	Location	Recommended Value
Guest Mode	Chrome Settings → People	Disabled
SafeSearch	Google Account → Search Settings	On
App Installation	Chrome Web Store	Allow only whitelisted apps
Screen Lock	System Preferences → Security	5-minute auto-lock
Two-Factor Auth	Google Account → Security	Enabled