

Protecting Privacy. Supporting Presence.

A Guide to How The Commons
Protects Student Data and Supports
Distraction-Free Learning



The Commons is a privacy-first platform designed to support student focus and well-being without surveillance or invasive data collection.

Privacy-First by Design

At The Commons, we help students stay focused during the school day by minimizing digital distractions, not by monitoring or tracking them.

Our system is built for schools and students without compromising privacy, safety, or trust.



What The Commons Detects	What We <u>Never</u> Access
Entry/exit from school zone	Browsing history
Whether app is functioning properly	App content or messages
Time-on-phone in school zone	Student names, IP addresses, precise location

Why This Matters

- **Non-invasive:** Emails, texts, web history, or media are never accessed or stored.
- **Privacy built-in:** By design, we don't access personal information. While schools can see general usage patterns, no private content, messages, or account details are ever collected or shared.
- **Compliance and best practices:** We align with FERPA and COPPA and follow the security protocols outlined in the NIST Cybersecurity Framework.

The Commons operates without access to any student content, messages, or accounts – and that's intentional.

Commitments & FAQ

Built for Schools, with Students in Mind

The Commons reduces classroom disruption, supports digital wellness, and builds student agency without requiring phone collection.

Legally Compliant

The Commons complies with:

- FERPA – Family Educational Rights and Privacy Act
- COPPA – Children’s Online Privacy Protection Act
- District technology policies

Following NIST Standards

We follow best practices informed by the NIST Cybersecurity Framework, the national standard for protecting sensitive data and reducing digital risk.

Does The Commons read my kid’s messages or browsing history?

No – We don’t track phone content at all. Our VPN is a simple protection layer over students’ distracting applications to ensure they can’t be accessed during the school day.

Can The Commons see who my child is or where exactly they are?

No – We only detect entry or exit from a general school zone, not precise location or identity.

Why don’t you collect names or accounts?

Because we pair devices to school rosters using QR codes, not usernames or passwords. That keeps everything anonymous within the app.

Still have questions? For more information, visit:

www.the-commons.app/faq and www.the-commons.app/privacy-policy



Permissions Used by Popular Apps – How The Commons is Different

Permissions				
Personal information: Name, Age, Email, Password	✓	✓	✓	
Camera, Photos & Microphone	✓	✓	✓	
Location	✓		✓	✓
In-App Ads & Cross-App Tracking for Ads	✓	✓		
Search History	✓	✓		

Graph adapted from [Apps that Track You](#)

- ✓ = Required or requested permission is optional and is typically enabled by default for an optimal app experience.
- ✓ = The Commons only uses location to detect school entry/exit – never to track, store history, or build profiles.

Teens' personal information is being exploited by big tech. By quickly enabling all app permissions—like camera, microphone, or search history— teens unlock popular features like filters, sharing, or live content.

These permissions give platforms deeper access to track behavior and build detailed profiles.

The Commons is different.

We only use the minimum needed to support safe use during school hours—specifically, device motion, notifications and a school-specific VPN to detect location when students arrive on campus to automatically block distracting apps. We don't track personal activity, browsing, or location history.

The Commons stores only limited, non-personal data for functionality. Your student's content, messages, or personal information is never collected or shared.

That's our promise.

