

CyberSafely is the student safety app that is the trust layer for parents and schools. An AI-powered parental safety platform built around a smart keyboard that replaces the standard keyboard on a child's device, detecting risks like cyberbullying, sextortion, drug references, and self-harm language in real time, across every app a child uses.

THREE PRODUCT PILLARS

AI-POWERED MONITORING

The CyberSafely keyboard replaces the standard keyboard and uses AI to detect risks like cyberbullying and sextortion in real time.

ALWAYS-ON COVERAGE

Works seamlessly across all apps and social platforms. Actionable insights for early intervention, before online risk becomes real-world harm.

INSTANT PARENT ALERTS

Notifications within seconds with severity ratings. Parents choose their detail level and are notified if the app is disabled.

THREE-TIER ALERT SYSTEM

● Acceptable

Normal, non-harmful communication.
Ex: Coordinating a gaming session with a friend.

● Questionable

Context-dependent; parent decides.
Ex: Message references a party with drugs or alcohol.

● Critical

Real-time push notification sent.
Ex: Self-harm language, sextortion, or direct threat.

PRIVACY-FIRST ARCHITECTURE & SECURITY PROTOCOLS

- ✓ **On-device analysis.** Keystrokes are analyzed in real time and parents are notified based on preferences.
- ✓ **Passwords never collected.** Social media passwords are never seen or stored by CyberSafely.
- ✓ **Risk signals only.** Parents see context and severity, not their child's private conversations.
- ✓ **Secure data handling.** Limited data (posts, media) is securely stored only to detect harmful content and improve protection.
- ✓ **No human surveillance.** No manual review of children's accounts by CyberSafely staff.
- ✓ **Tamper notification.** Parents are alerted if the app or keyboard is disabled on the child's device.

WHAT CYBERSAFELY WILL NEVER DO

- ✗ Store or transmit your child's passwords
- ✗ Retain the substance of private conversations
- ✗ Share keystrokes with anyone beyond a parent
- ✗ Use child data for advertising or third-party resale
- ✗ Operate as surveillance or spyware – protection only

HOW IT WORKS

1. Parent signup and adds child via email — a unique secure access code is generated.
2. CyberSafely keyboard is installed on the child's device and set as the default keyboard, mimicking the native phone keyboard.
3. AI analyzes typed content in real time across every app for risk signals.
4. Parent dashboard receives color-coded alerts; critical risks trigger instant push notifications.