Staff Training Resources for Digital Safety

Train school staff to recognize, respond to, and prevent online exploitation, grooming, and digital abuse. Use this guide to integrate into your professional development program.

I. Foundational Training Topics (All Staff)

- Understanding grooming, sextortion, and image-based abuse
- Red flag behaviors in student language, social withdrawal, or secrecy
- Reviewing common red flag apps (Snapchat, Discord, Telegram, vault apps)
- How to listen and respond when a child discloses abuse
- School-wide protocols for reporting and responding to digital threats

II. Specialized Sessions (Counselors, Admins, IT, Safety Officers)

- How to conduct trauma-informed interviews with affected students
- Digital forensics basics - what staff should and shouldn't do
- Platform-specific risks (Instagram, TikTok, Roblox, etc.)
- Incident reporting to law enforcement and national cybertip services
- Coordination with parents post-incident

III. Training Format Recommendations

- Scenario-based roleplay (what to say, what NOT to say)
- Review real case studies (anonymized) for applied learning
- Invite law enforcement or child protection experts for Q&A
- Make training mandatory for all grade levels and departments
- Repeat annually - update with latest app trends and threats

IV. Onboarding New Staff

- Include digital safety in onboarding packet
- Provide a checklist of device/app supervision expectations
- Ensure they know the school's incident reporting protocol

V. Tools and Resources to Include in Training

- Red Flag Apps List (see separate PDF)

- Educator Digital Safety Checklist (see separate PDF)

- Incident Reporting Protocol (see separate PDF)

- K-12 Curriculum Guide (see separate PDF)

- Crisis resources: https://report.cybertip.org, https://takeitdown.ncmec.org

Reminder: Digital safety training is not optional. It is a frontline defense against trauma that can follow a child for life.