

Youth Internet Safety Review Worksheet Instructions

This worksheet is a structured auditing tool designed to help parents, guardians, educators, or caseworkers systematically evaluate the safety, security, and risk profile of a specific online account used by a youth.

It is divided into three key areas:

1. **Account Details & Technical Settings:** Collects identifying information (platform, username) and assesses basic security posture 2 Factor Authentication (2FA), password sharing, privacy settings).
2. **Interaction & Content Features:** Evaluates how the youth communicates on the platform (voice, video, private messaging) and indicates immediate content concerns like bullying or self-harm.
3. **Safety & Risk Indicators:** A broader checklist to determine if proactive safety measures are in place (parental controls, safety contracts) and to identify behavioral "red flags". (sudden increase in usage, contacts with unknown individuals, or grooming concerns).

How to Use it

A separate worksheet should be completed for each major platform the youth utilizes (e.g., one for TikTok, one for Instagram, one for Roblox).

Step 1: Gather Information

- Sit down with the youth and open the app or platform together. It is highly recommended to complete this as a collaborative review rather than a secretive investigation. Working on this together can help to build trust.

Step 2: Complete the "Account" Section

- Fill in the blanks and check the appropriate boxes regarding the technical setup.
- Crucial checks: Look at the actual privacy settings (is it truly private?, check if location sharing is on, and verify if private messaging and voice/video chat are enabled, as these are primary avenues for risk.

Step 3: Complete the "Safety & Risk Indicators" Section

Be honest when checking these boxes.

- If you check "Yes" for items like "sudden increase in usage," "new 'important' online friend," or "contact with unknown individuals," these warrant immediate further conversation and monitoring.
- If you check "No" for "parental controls in place" or "internet safety and data usage contract" where you may want to take immediate, proactive action...

Step 4: Schedule Reviews

- This should be an ongoing process, not be a one-time event. Schedule a review every 90 days to ensure settings haven't changed and no new risks have emerged. You can always review more frequently if that feels necessary or if you have noticed any concerns between scheduled reviews.

Glossary

Term	Meaning in plain English	Example
2-Factor Authentication (2FA)	An extra "deadbolt" for an account. Even if someone steals the password, they can't get in without a code sent to your phone.	After typing in your password, the app asks for a 6-digit code sent to the phone/email or entered from an app.
Recovery Email/Phone	The "backup" contact info used to get back into an account if the password is forgotten or changed by a hacker.	If a child is locked out of an account, the "reset password" link is sent to a specific email or phone.
Location Sharing	A feature that uses GPS to show exactly where the device (and youth) is on a map to other users.	"Snap Maps" on Snapchat showing the child is currently at the local park.
Parental Controls	Settings within the app or device to limit time or block content.	Setting "Screen Time" on a device to turn off all apps at 9:00 PM.
Monitoring Software	Third-party apps you install that "watch" for red flags (keywords, nude photos, bullying) and alert you.	An app that sends you an alert because it detected a conversation about self-harm in a message or search.

Term	Meaning in plain English	Example
Grooming	When another person builds an emotional connection with a child to lower their inhibitions for the purpose of abuse.	An another "gamer"; giving a child free in- game currency and telling them, "Don't tell your parents, they wouldn't understand our friendship".
Sextortion	A form of blackmail where someone threatens to share private or sensitive images of a youth unless they provide more images or money.	Someone pretending to be a peer convinces a person to send a photo or video, then threatens to send it to their entire school, friends, parents, etc. unless they send money or more photos/videos.
Account Breach	When an unauthorized person gains access to an account ("being hacked").	A child logs into account and finds all their in-game currency gone and their password changed.

Pro-Tip for Parents: If you aren't sure if a setting is "Private" or "Public" try searching for your child's username on a different device that isn't logged in. If you can see their photos or friends list, the account is likely **Public**.

