



Video Chat Safety Checklist

Video conferencing has quickly become part of our “new normal.” Whether it’s engaging in an online classroom or catching up with friends and family, we want to make sure your video chats are safe and secure.

8 Ways to Help Kids Video Chat Safely

1. **Grown-ups rule.** Parents, or another trusted adult, should always start and end all video chats and conferences.
2. **Don’t chat with strangers.** Make sure your child only video chats with someone you know and trust. Don’t click on any meeting links from an unknown source.
3. **Protect your privacy.** Never include any identifying personal information (full name, SSN, birthdate, etc.) in your child’s profile.
4. **Use caution with photos.** We recommend never posting your child’s photo in a video app profile. Instead, you can make an avatar that still gives your child a face, but protects their image from potential online pilfering. *NOTE: Always supervise your child’s use of avatar apps like Bitmoji or Zmoji.*
5. **Be on your best behavior.** Teach kids to behave as they would in a real classroom (or even better!). Anything they do can be recorded and saved, which means it could live on the internet forever.
6. **Keep tabs.** Check in and monitor all of your child’s video chats.
7. **Keep it out in the open.** Conduct video chats in a central, public area of your home—not in bedrooms.
8. **Use parental controls.** Always use the privacy and parental control settings on your devices and in video conferencing apps for extra protection.



safewise 

www.safewise.com



Get to Know Video Chat Apps

Which Ones Are Safe?

App	End-to-End Encryption*	Parental Controls	Privacy Extras
Zoom	X No	X No	Meeting passwords Meeting locks Meeting registration
Google Hangouts	X No	✓ Yes	Invitation blocker
Skype	Optional	X No	Invitation blocker
WebEx	Optional	X No	Meeting locks Meeting passwords
WhatsApp	✓ Yes	X No	User blocker Turn off public view Turn off location
Snapchat	Limited	✓ Yes	Turn off Quick Add Turn off location
Messenger Kids	X No	✓ Yes	Controlled chat list 30 days of history Remote logout
Facetime	✓ Yes	✓ Yes	Limit contacts Limit screen time Remote iCloud monitoring

**End-to-end encryption means the only people who can see the communication are the participants. Your chats and information are protected from all prying eyes that lurk on the internet—from the moment you sign on until you sign off. This is the strongest form of privacy protection for online communications.*

